INFORMATION ECOSYSTEM ASSESSMENT (IEA) ON THE IMPACT OF CYBER SECURITY AND CYBERCRIME LAWS ENACTED BY SOUTHERN AFRICA GOVERNMENTS ON MEDIA FREEDOM AND DIGITAL RIGHTS

USAID
FROM THE AMERICAN PEOPLE

Internews
Local voices. Global change.

ADVANCING RIGHTS IN SOUTHERN AFRICA
ARISA

This Information Ecosystem Report (IEA) was commissioned by Advancing Rights in Southern Africa (ARISA). ARISA is a 5-year USAID-funded human rights program being undertaken by consortium partners Freedom House, Internews, PACT and American Bar Association, across the SADC region.

ARISA CONSORTIUM PARTNERS

ABOUT THE AUTHORS

Author: *Dianne Hubbard has degrees in English from the University of North Carolina-Chapel Hill and Stellenbosch University in South Africa and a law degree from Harvard Law School. She was the Coordinator of the Gender Research & Advocacy Project of the Legal Assistance Centre in Windhoek, Namibia for 30 years. She has also served on Namibia's statutory Law Reform and Development Commission and carried out consultancy work for various international agencies including the ILO, the World Bank, UNICEF and UNHCR.*

Contributors: *Frederico Links is a Namibian journalist, researcher, trainer and freedom of expression advocate. In both his journalism and research, Links has a strong focus on good governance, human rights (including digital rights), state surveillance, corruption, rule of law, and transparency and accountability. Chaacha Mwita is a consultant at Internews and compiled the IEA Summary Report.*

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of ARISA and do not necessarily reflect the views of USAID or the United States Government.

ACKNOWLEDGEMENTS

Internews and the researchers, Dianne Hubbard and Frederico Links, would like to acknowledge and thank the following individuals for their contributions and inputs, through interviews and/or reviewing of manuscripts, towards deepening and strengthening the accuracy and credibility of this report with their informed perspectives and insights.

Heartfelt thanks to Dr. Allen Munoriyarwa and Prof. Tachilisa Balule, both of the University of Botswana, for their insights on relevant political, legislative and electoral matters playing out in Zimbabwe and Botswana, respectively.

Similarly, we would like to thank Prof. Tresor Musole Maheshe, of the Catholic University of Bukavu, in the Democratic Republic of the Congo (DRC), for granting an interview to discuss unfolding events in that country; Christina Chan-Meetoo, Senior Lecturer in Media and Communication at the University of Mauritius, for her insights regarding the situation in Mauritius; Murray Hunter, Interim Director of Intelwatch and also of ALT Advisory in South Africa; Armando Nhatumbo of MISA Mozambique; Richard Mulonga, CEO of Bloggers of Zambia; and, Ndimphiwe Shabangu of the Coordinating Assembly of NGOS (CANGO) in Eswatini.

We further acknowledge and thank the following people for taking the time to review the country specific sections: Gregory Gondwe, Director of the Platform for Investigative Journalism (PIJ), and Moses Chitsulo, Program Officer at MISA Malawi, in Malawi; Prof. Rui Verde, Chief Legal Adviser at MakaAngola and researcher at Oxford University's Center for African Studies; Andrew Marawiti, Executive Director of MISA Tanzania; and Mzimkhulu Sithetho, consultant and adviser at Media Institute of Southern Africa (MISA) Lesotho. Perri Caplan, a layout consultant based in Namibia, who provided volunteer assistance with the conversion and processing of various documents in French and Portuguese to make them suitable for the application of online translation tools.

To the Internews team, Rosemary Viljoen, and Molly Hove who provided support and guidance and to Chaacha Mwita for preparing the IEA Summary Report.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS **3**
ACRONYMS AND ABBREVIATIONS **11**
EXECUTIVE SUMMARY **16**
MEDIA FREEDOM AND FREEDOM OF EXPRESSION UNDER THREAT 16
KEY OBSERVATIONS 18
CONCLUSIONS 20
RECOMMENDATIONS FOR FURTHER REGIONAL RESEARCH 22
FOR SADC GOVERNMENTS: 22
FOR FURTHER REGIONAL RESEARCH: 24
CHAPTER 1: INTRODUCTION AND METHODOLOGY **26**
THE APPROACH TO THE ANALYSIS 26
CYBERCRIME CAN BE DIVIDED INTO THREE CATEGORIES 26
WHAT IS NOT COVERED 33
THE STRUCTURE OF EACH CHAPTER 33
CHAPTER 2: INTERNATIONAL STANDARDS, MODELS AND GUIDELINES **36**
2.1 CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION), 2001 37
2.2 AFRICAN UNION CONVENTION ON CYBER SECURITY AND DATA PROTECTION (MALABO CONVENTION), 2014 41
2.3 SADC COMPUTER CRIME AND CYBERCRIME MODEL LAW, 2012 43
2.4 COMMONWEALTH COMPUTER AND COMPUTER-RELATED CRIME MODEL LAW, 2002 45
2.5 AFRICAN CHARTER ON HUMAN AND PEOPLES' RIGHTS (ACHPR) DECLARATION ON THE PRINCIPLES OF FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION, 2019 46
PRINCIPLE 9. JUSTIFIABLE LIMITATIONS 47
2.6 JOINT DECLARATIONS OF THE SPECIAL RAPPORTEURS 50
2.7 WINDHOEK DECLARATIONS 51
2.8 CRIMINAL DEFAMATION 52
2.9 PRIVACY AND FREEDOM OF EXPRESSION 53
REGISTRATION OF SUBSCRIBERS 54
MASS SURVEILLANCE AND DATA RETENTION 55
2.10 GUIDELINES ON ACCESS TO INFORMATION AND ELECTIONS IN AFRICA, 2017 56
MEDIA AND INTERNET REGULATORY BODIES 57
THE MEDIA AND ONLINE MEDIA PLATFORM PROVIDERS 57
2.11 REVISED SADC PRINCIPLES AND GUIDELINES GOVERNING DEMOCRATIC ELECTIONS, 2015 58
2.12 SADC MODEL LAW ON ELECTIONS, 2018 59
CHAPTER 3: ANGOLA **63**

3.1 CONTEXT 64
A) OVERVIEW 65
B) LAW NO. 1/17: PRESS LAW 68
C) LAW NO. 2/17: REGULATORY ENTITY OF THE ANGOLAN MEDIA (ERCA) 70
D) LAW NO. 3/17: TELEVISION ACTIVITIES 72
E) LAW NO. 4/17: RADIO BROADCASTING 73
F) LAW NO 5/17: JOURNALISTS' STATUTE 73
3.2 CONSTITUTION 74
3.3 CASE STUDIES 77
3.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 83
A) CYBERCRIME PROVISIONS IN THE PENAL CODE 83
B) CYBERCRIME PROVISIONS IN LAW NO.7/17 ON PROTECTION OF INFORMATION SYSTEMS AND NETWORKS 86
C) PENAL CODE PROVISIONS THAT COULD RESTRICT FREEDOM OF EXPRESSION 87
D) STATE SURVEILLANCE 89
E) SIM CARD REGISTRATION 90
F) TAKE-DOWN NOTIFICATIONS 91
CHAPTER 4: BOTSWANA 93
4.1 CONTEXT 94
4.2 CONSTITUTION 98
4.3 CASE STUDIES 99
4.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 102
A) CYBERCRIME AND COMPUTER RELATED CRIMES ACT 18 OF 2018 102
B) PENAL CODE 111
C) COMMUNICATIONS REGULATORY AUTHORITY ACT 19 OF 2012 117
D) STATE SURVEILLANCE: CRIMINAL PROCEDURE AND EVIDENCE (CONTROLLED INVESTIGATIONS) ACT 14 OF 2022 119
E) OTHER LAWS AND REGULATIONS 121
F) SIM CARD REGISTRATION 121
G) TAKE-DOWN NOTIFICATIONS 122
4.5 ELECTION LAW AND FREEDOM OF EXPRESSION 122
CHAPTER 5: COMOROS 130
5.1 CONTEXT 131
5.2 CONSTITUTION 135
5.3 CASE STUDIES 135
5.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 138
A) CYBERCRIMINALITY IN THE PENAL CODE 139

B) LAW ON CYBER SECURITY AND THE FIGHT AGAINST CYBERCRIME....150
C) ADDITIONAL SPEECH-RELATED OFFENCES IN THE PENAL CODE....159
D) CRIMINAL INVESTIGATIVE POWERS AND STATE SURVEILLANCE....162
E) SIM CARD REGISTRATION....163
COMOROS DOES NOT HAVE A LAW ON MANDATORY SIM CARD REGISTRATION....163
F) TAKE-DOWN NOTIFICATIONS....163
CHAPTER 6: DEMOCRATIC REPUBLIC OF CONGO (DRC)....165
6.1 CONTEXT....166
6.2 *CONSTITUTION*....173
6.3 *CASE STUDIES*....174
6.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION....181
A) CYBERCRIME PROVISIONS IN LAW NO. 20/17 ON TELECOMMUNICATIONS AND INFORMATION AND COMMUNICATION TECHNOLOGIES....181
B) CYBERCRIME PROVISIONS IN LAW NO. 23/010, DIGITAL CODE....187
C) PENAL CODE OFFENCES RELATED TO FREEDOM OF EXPRESSION....198
D) PRESS FREEDOM LAW OFFENCES RELATED TO FREEDOM OF EXPRESSION....200
E) STATE SURVEILLANCE....202
F) SIM CARD REGISTRATION....203
G) TAKE-DOWN NOTIFICATIONS....203
6.5 *ELECTION LAW AND* FREEDOM OF EXPRESSION....203
CHAPTER 7: ESWATINI....210
7.1 CONTEXT....211
7.2 CONSTITUTION....212
7.3 CASE STUDIES....214
7.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION....218
A) THE COMPUTER CRIME AND CYBER CRIME ACT, 2022....218
B) OTHER LAWS THAT MAY INHIBIT FREEDOM OF EXPRESSION....231
C) SIM CARD REGISTRATION (REGISTRATION OF ELECTRONIC COMMUNICATIONS AND MOBILE CUSTOMERS)....237
D) TAKE-DOWN NOTIFICATIONS....237
7.5 ELECTION LAW AND FREEDOM OF EXPRESSION....238
CHAPTER 8: LESOTHO....245
8.1 CONTEXT....246
8.2 CONSTITUTION....249
8.3 CASE STUDIES....250
8.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION....252
A) TECHNICAL CYBERCRIME PROVISION IN PENAL CODE....252

B) COMPUTER CRIME AND CYBER SECURITY BILL 252
C) OTHER LAWS THAT MAY LIMIT FREEDOM OF EXPRESSION 265
D) STATE SURVEILLANCE 268
E) SIM CARD REGISTRATION 268
F) ACCESS TO TRAFFIC DATA 269
G) TAKE-DOWN NOTIFICATIONS 269
CHAPTER 9: MADAGASCAR 271
9.1 CONTEXT 272
9.2 CONSTITUTION 280
9.3 CASE STUDIES 282
9.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 286
A) LAW NO. 2014-006 ON THE FIGHT AGAINST CYBERCRIME (AS AMENDED) 286
B) LAW NO. 2014-006 ON THE CODE ON MEDIA COMMUNICATIONS (AS AMENDED) 293
C) OFFENCES RELATING TO EXPRESSION IN THE PENAL CODE 298
D) INVESTIGATION TOOLS AND STATE SURVEILLANCE 298
E) SIM CARD REGISTRATION 300
F) TAKE-DOWN NOTIFICATIONS 300
9.5 ELECTION LAW AND FREEDOM OF EXPRESSION 300
CHAPTER 10: MALAWI 307
10.1 CONTEXT 308
10.2 CONSTITUTION 310
10.3 CASE STUDIES 312
10.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 316
A) ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT 33 OF 2016 316
B) OTHER LAWS THAT MAY IMPACT FREEDOM OF EXPRESSION 325
PENAL CODE 326
60. PUBLICATION OF FALSE NEWS LIKELY TO CAUSE FEAR AND ALARM TO THE PUBLIC 326
PENAL CODE 326
200. DEFINITION OF LIBEL 326
C) SIM CARD REGISTRATION 327
D) STATE SURVEILLANCE 328
E) TAKE-DOWN NOTIFICATION 328
CHAPTER 11: MAURITIUS 330
11.1 CONTEXT 331
11.2 CONSTITUTION 340
11.3 CASE STUDIES 343

11.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 345
A) CYBERSECURITY AND CYBERCRIME ACT 16 OF 2021 345
B) INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 44 OF 2001 353
C) CRIMINAL CODE 357
D) NATIONAL ASSEMBLY (PRIVILEGES, IMMUNITIES AND POWERS) ACT 22 OF 1953 359
E) SIM CARD REGISTRATION 359
F) STATE SURVEILLANCE 359
G) TAKE-DOWN NOTIFICATIONS 360
11.5 ELECTION LAW AND FREEDOM OF EXPRESSION 360
CHAPTER 12: MOZAMBIQUE 365
12.1 CONTEXT 367
12.2 CONSTITUTION 373
12.3 CASE STUDIES 375
12.4 CYBERCRIME 379
A) TECHNICAL OFFENCES 379
B) CONTENT-BASED OFFENCES 381
C) STATE SURVEILLANCE AND CRIMINAL INVESTIGATIONS 384
D) SIM CARD REGISTRATION 386
E) TAKE-DOWN NOTIFICATIONS 386
12.5 ELECTION LAW AND FREEDOM OF EXPRESSION 387
CHAPTER 13: NAMIBIA 393
13.1 CONTEXT 394
13.2 CONSTITUTION 396
13.3 CASE STUDIES 397
13.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 400
A) DRAFT COMPUTER SECURITY AND CYBERCRIME BILL, 2019 401
B) COMMUNICATIONS ACT 8 OF 2009 407
C) DATA RETENTION AND STATE SURVEILLANCE 408
D) TAKE-DOWN NOTIFICATIONS IN THE ELECTRONIC TRANSACTIONS ACT 4 OF 2019 412
13.5 ELECTION LAW AND FREEDOM OF EXPRESSION 413
CHAPTER 14: SEYCHELLES 419
14.1 CONTEXT 420
14.2 CONSTITUTION 427
14.3 CASE STUDIES 431
14.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 432
A) CYBERCRIMES AND OTHER RELATED CRIMES ACT 59 OF 2021 432
B) PENAL CODE 440

C) INVESTIGATORY POWERS AND STATE SURVEILLANCE 442
D) SIM CARD REGISTRATION AND OTHER SUBSCRIBER INFORMATION 443
CHAPTER 15: SOUTH AFRICA 445
15.1 CONTEXT 446
15.2 CONSTITUTION 452
15.3 CASE STUDIES 457
15.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 461
A) CYBERCRIMES ACT 19 OF 2020 461
B) ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 473
C) FILMS AND PUBLICATIONS ACT 65 OF 1966 474
D) HATE SPEECH 476
E) REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION 478
OF COMMUNICATION RELATED INFORMATION ACT 13 OF 2002 (RICA) 478
F) TAKE-DOWN NOTIFICATIONS 480
15.5 ELECTION LAW AND FREEDOM OF EXPRESSION 480
CHAPTER 16: TANZANIA 489
16.1 CONTEXT 490
A) TANZANIA 492
B) ZANZIBAR 495
16.2 CONSTITUTION 496
16.3 CASE STUDIES 497
16.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 501
A) CYBERCRIMES ACT, 2015 501
B) ELECTRONIC AND POSTAL COMMUNICATION ACT, 2010 510
C) ELECTRONIC AND POSTAL COMMUNICATIONS (ONLINE CONTENT) REGULATIONS, 2020 510
D) MEDIA SERVICES ACT, 2016 517
E) THE PENAL CODE [REVISED EDITION 2022] 517
F) ZANZIBAR 518
G) SIM CARD REGISTRATION 520
H) TAKE-DOWN NOTIFICATIONS 520
CHAPTER 17: ZAMBIA 522
17.1 CONTEXT 523
17.2 CONSTITUTION 526
17.3 CASE STUDIES 529
17.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 531
A) THE CYBER SECURITY AND CYBER CRIMES ACT 2 OF 2021 531

B) PENAL CODE 542
C) OTHER LAWS THAT MAY RESTRICT FREEDOM OF EXPRESSION 545
D) STATE SURVEILLANCE AND INVESTIGATORY POWERS 546
E) SIM CARD REGISTRATION 547
F) TAKE-DOWN NOTIFICATIONS 547
CHAPTER 18: ZIMBABWE 549
18.1 CONTEXT 551
18.3 CASE STUDIES 556
18.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION 559
A) CRIMINAL LAW (CODIFICATION AND REFORM) ACT [CHAPTER 9:23] AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 [CHAPTER 12:07] 559
B) INVESTIGATION TOOLS AND STATE SURVEILLANCE 570
C) SIM CARD REGISTRATION 572
18.5 ELECTION LAW AND FREEDOM OF EXPRESSION 573
REFERENCES 581

ACRONYMS AND ABBREVIATIONS

ACHPR	African Commission on Human and Peoples' Rights
AMPS	Association of Media Practitioners Seychelles
ANADEN	National Agency for Digital Development - L'Agence Nationale de Développement du Numérique
ANC	African National Congress
ANRCM	National Authority for the Regulation of Media Communication -Autorité Nationale de Régulation de la Communication Médiatisée
ANRTIC	National Regulation Authority of Information and Communications Technology
ARECOM	Communications Regulatory Authority - Autoridade Reguladora das Comunicações de Moçambique
ARPTIC	Regulatory Authority for Posts, Telecommunications and Information Technologies of Congo - L'Autorité de Régulation de la Poste et des Télécommunications du Congo
BAZ	Broadcasting Authority of Zimbabwe
BCCSA	Broadcast Complaints Commission of South Africa
BOCRA	Botswana Communications Regulatory Authority
BTI	Bertelsmann Transformation Index
CANGO	Coordinating Assembly of NGOs
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CEIR	Central Electric Identity Register
CENCO	National Episcopal Conference of Congo
CENI	Independent National Election Commission
CENI	Independent National Electoral Commission
CENI	Independent National Electoral Commission - Commission Électorale Nationale Indépendante
CERT-MU	Computer Emergency Response Team of Mauritius
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CISP	Integrated Public Security Centre
CNE	National Electoral Commission - Comissão Nacional de Eleições
CNPA	National Press and Audiovisual Council
CRAN	Communications Regulatory Authority of Namibia

CSAC	High Council for Broadcasting and Communication - Conseil Supérieur de l'Audiovisuel et de la Communication
DA	Democratic Alliance
DMCA	Digital Millennium Copyright Act
DMMA	Digital Media and Marketing Association
DPA	Data Protection Agency
EBC	Elections and Boundaries Commission
EFF	Economic Freedom Fighters
EOM	Election Observation Mission
ERCA	Regulatory Entity of the Angolan Media
ESAP	Economic Structural Adjustment Programs
ESAP	Economic Structural Adjustment Programs
FCC	Common Front for Congo
FRELIMO	Front for the Liberation of Mozambique
GABINFO	Government Press Office
GILAB	General Intelligence Laws Amendment Bill
GNU	Government of National Unity
IBA	Independent Broadcasting Authority
IBA	Independent Broadcasting Authority
IBGDH	Initiative Bonne Gouvernance et Droits Humains - Good Governance and Human Rights Initiative
ICASA	Independent Communications Authority of South Africa
ICCPR	International Covenant on Civil and Political Rights
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
IEA	Information Ecosystem Assessment
IEC	Independent Electoral Commission
ILO	International Labour Organization
INACOM	National Institute of Telecommunications
INCM	Institute of Communications of Mozambique - Instituto Nacional das Comunições de Moçambique
INTIC	National Institute of Information and Communication Technologies – Instituto Nacional de Tecnologias de Informação e Comunicação
ISPA	Internet Service Providers' Association
ISS	Institute for Security Studies
LCA	Lesotho Communications Authority

LEXOTA	Laws on Expression Online: Tracker and Analysis
LNBS	Lesotho National Broadcasting Service
MACRA	Malawi Communications Regulatory Authority
Malawi CERT	Malawi Computer Emergency Response Team
MCERT	Malawi Computer Emergency Response Team
MBC	Malawi Broadcasting Corporation
MBC	Mauritius Broadcasting Corporation
MCM	Media Council of Malawi
MDC	Movement for Democratic Change
MDDA	Media Development and Diversity Agency
MDM	Democratic Movement of Mozambique
MISA	Media Institute of Southern Africa
NAMPA	Namibian Press Agency
NBC	Namibian Broadcasting Corporation
OAS	Organization of American States
ORTC	Comoros Radio and Television Office
ORTC	Office de Radio et Télé des Comores
OSCE	Security and Co-operation in Europe
PEPUDA	Promotion of Equality and Prevention of Discrimination Act
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PUDEMO	Peoples United Democratic Movement
RENAMO	Mozambique National Resistance
RFI	*Radio France Internationale*
RICA	Regulation of Interception of Communications and Provision of Communication related Information Act
RTNVC	Radio-Télévision nationale congolaise
SABC	South African Broadcasting Corporation
SADC	Southern African Development Community
SANEF	South African National Editors' Forum
SCC	eSwatini Communications Commission
SERNIC	National Service of Criminal Investigation
SIM	Security Information Management
SLAPP	Strategic Litigation Against Public Participation
SMC	Seychelles Media Commission
SNJ	Sindicato Nacional de Jornalistas

SOLORN	La Synergie des Organizations de la Société Civile de Lualaba Œuvrant dans le secteur des Ressources Naturelles
STA	eSwatini Television Authority
STAE	Technical Secretariat for Electoral Administration - Secretariado Técnico da Administração Eleitoral
TBC	Tanzania Broadcasting Services
TCRA	Tanzania Communications Regulatory Authority
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
WASPA	Wireless Applications Service Providers' Association
ZAMEC	Zambia Media Council
ZANU-PF	Zimbabwe African National Union – Patriotic Front
ZBC	Zimbabwean Broadcasting Corporation
ZEC	Zimbabwe Electoral Commission
ZEC	Zimbabwe Electoral Commission
ZICTA	Zambia Information and Communication Technology Authority
ZNBC	Zambia National Broadcasting Corporation

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

In 2023, Advancing Rights in Southern Africa (ARISA) through its consortium partner, Internews, undertook the most comprehensive review yet of laws affecting media practice and the freedom of expression, including cyber laws, penal codes, constitutions and acts of parliament, in the sixteen Southern African Development Community (SADC) countries. The Information Ecosystem Analysis (IEA) provides an in-depth overview of the legal provisions that have been enacted or are in various stages of becoming laws in the region, and are being used by SADC governments to stifle and limit press freedom and public debate. Each of the sixteen SADC countries are included as individual country chapters in this report, providing country-specific legal analyses of the relevant Cyber security and related laws used by the respective country's governments to stifle freedom of expression. The approach used by the researchers considered the legislative environment together with literature on the relevant topics, court cases and media reports about the application of specific laws and focused on incidents of where laws were used, dating from 2020 to present. The respective country analyses have been informed by extensive virtual interviews conducted with journalists, civil society representatives and academics in the region. Attention was also given to countries holding elections in 2023 and 2024.

With the rise in Cyber Security laws being enacted by regional governments, a key area of concern are the election laws that adversely affect freedom of expression. Nine SADC countries, namely, Botswana, Democratic Republic of Congo, Eswatini, Madagascar, Mauritius, Mozambique, Namibia, South Africa, Zimbabwe have elections slated to take place during late 2023 or 2024, 1 which makes examination of the potential brakes on free discussion and debate particularly important in those jurisdictions.

MEDIA FREEDOM AND FREEDOM OF EXPRESSION UNDER THREAT

The Media freedom and journalism are under heightened threat and sharpened assault across the African continent, with developments across southern Africa over recent years becoming especially troubling, according to Amnesty International.

> *In his remarks commemorating World Press Freedom Day, May 3rd, 2023,* ***Amnesty International Director for East and Southern Africa, Tigere Chagutah, noted that****: "There has been a worrying trend of attacks, harassment, intimidation and the criminalization of journalism across East and Southern Africa demonstrating the length to which authorities are prepared to go to silence the media for exposing allegations of corruption and human rights violations."*[2]

[1] "Elections Calendar for SADC-2022-to-2026", SADC Parliamentary Forum website; "SADC Elections Calendar", GENDER & Development in SADC and Southern African Research and Documentation Centre (SARDC)

[2] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.

As this report illustrates, the latest instruments in the evolving arsenal of repressive tools being deployed to undermine media freedom and civic spaces across the Southern African Development Community (SADC) have become cyberspace-related laws and regulations, particularly cybersecurity and cybercrime laws and regulatory frameworks.

These laws and regulations in the SADC region *"that limit the freedom of the press in the digital age signal a disturbing trend"*, argued the **Institute for Security Studies (ISS)** in June 2023, because they "open up a new front in curtailing press freedom in the name of national security". It added that in "today's information environment, both digital and analogue, journalists' risk *being personally attacked, or their stories dismissed as simply 'fake news'. This means powerful elites can operate without accountability*".[3]

"My sense is that I don't think the region is doing very well in terms of dealing with the cybersecurity and digital, as well as data, issues," **stated Dr. Allen Munoriyarwa**, senior lecturer in media studies at the University of Botswana, in an interview for this study[4]. *"There seems to be a deliberate attempt across the region to use regulations around cybersecurity, around digital security, around data, to weaken civil society, to weaken the press, to weaken the media and even individual journalists. I think the trend is that regimes seem to be learning from each other."*

These sentiments and the state of media freedom, as well as the generally perceived state of freedom of expression, across the region were especially concerning against the backdrop of nine of the sixteen SADC member states having or moving towards major elections in late 2023 and through 2024, starting with Zimbabwe in August 2023, at the time that this report was being finalised. Elections across the region remain highly tense and sensitive periods, prone to political violence in some countries. In such volatility it often is the case that the media, as well as critical civil society actors, become the earliest and primary targets of vilification, harassment and intimidation by political elites championing their causes on the election trails. This increasingly plays out in both the so-called 'stable' democracies in the region and the more repressive regimes.

Evidence is mounting of how regional governments have been using newly minted cybersecurity or cybercrime laws, in conjunction with criminal procedures or penal codes, as well as media and civil society regulatory mechanisms, to clampdown on critical journalists and civil society and political activists during election times. This report sheds light on some of this ample evidence and testimony concerning these anti- and undemocratic and human rights-violating practices and occurrences.

[3] Karen Allen, "Journalism on trial in Africa: fortitude and fake news", Institute for Security Studies, 26 June 2023.
[4] Interviewed via Zoom on 25 July 2023.

KEY OBSERVATIONS

Against this backdrop, in terms of key observations to be drawn from the unfolding trends evident across the region, the following should be noted and underscored:

(i) While most SADC member states have since the early 2010s, and earlier, introduced and implemented cyberspace, cybersecurity and/or cybercrime related laws, at the time of compiling this report in mid-2023, some states – such as Namibia and Lesotho – were still in the process of finalising substantive laws and regulatory frameworks for enactment or implementation;

(ii) Aside from the democracy and human rights challenging aspects emerging from the latest regional trend to legislate for cyberspace, all SADC member states already had or have a range of problematic laws and regulatory frameworks, from colonial era laws or outdated post-colonial frameworks to more recent press laws or penal code amendments, on their statute books that can be or have been used for repressive purposes;

(iii) In this regard, over the years, the primary tools used to clampdown on the media, as well as civil society and political opposition in countries across the region, have been criminal defamation or insult provisions, as well as 'decency', 'national security' or 'public order' provisions, among others, in criminal procedures laws or penal codes, along with media registration and communications regulatory mechanisms and, of late, provisions related to the dissemination of what can broadly be labelled as 'fake news';

(iv) Concerningly, in many instances where repressive state practices have been recorded and reported, such practices have occurred as a result of law enforcement and/or state security actors having acted extrajudicially;

(v) Similarly, media freedom and free expression violations have occurred where law enforcement and/or state security overreach have been enabled by poorly developed or under-developed law or regulatory provisions;

(vi) At the same time, across the region human rights safeguards, along with public oversight guardrails, and transparency and accountability mechanisms, where such exist, are generally also poorly developed or under-developed in law and regulation, and especially so in the context of cybersecurity or cybercrime law and regulation;

(vii) The enabling of state surveillance abuse and/or overreach – especially through mass surveillance enabling legislative and regulatory measures – has become a primary concern, particularly for media freedom advocates, in the context of cybersecurity and/or cybercrime law and regulatory crafting and drafting in the SADC region.

Considering the key observations, the following are worth noting at a country-level:

ANGOLA: There are several content-based offences in the Penal Code that could inhibit freedom of expression: including some that appear to have been applied for this purpose in practice.

BOTSWANA: Certain provisions of the Penal Code that criminalise specific forms of expression seem to have been used repeatedly against media practitioners, in respect of both online and traditional media.

COMOROS: Comoros is one of the few countries in the world (and the only SADC country) that has not ratified the International Covenant on Civil and Political Rights (ICCPR). The rule of law is considered weak, and journalists are frequently arrested and intimidated over their reporting.

DEMOCRATIC REPUBLIC OF THE CONGO (DRC): The Digital Code regulates online media, and (amongst other things) provides prison sentences and heavy fines for offences related to social networks. It gives authorities power to imprison journalists for sharing information electronically.

ESWATINI: Arbitrary arrest and detention of journalists have become commonplace in eSwatini. In addition to government arrests and intimidation, there is an increasing trend of civil defamation cases against the media particularly by rich and powerful individuals.

LESOTHO: Lesotho's Penal Code and Communications Act have been used to target, arrest and prosecute journalists in recent times.

MADAGASCAR: Defamation and insult clauses in the cybercrime law have been used to arrest, charge and prosecute journalists on a number of occasions.

MALAWI: Numerous incidents since 2020 show how cybercrime offences under the Electronic Transactions and Cyber Security Act have been applied against journalists and persons who post on social media.

MAURITIUS: The Independent Broadcasting Authority Act allows a judge in Chambers to require journalists to reveal their sources without any legal safeguards, while in recent times the Information and Communication Technology Act has been used repeatedly to arrest and prosecute social media users.

MOZAMBIQUE: The Penal Code has been used to arrest and charge journalists with engaging in terrorism. Harassment, assault and intimidation of journalists, and civil society actors, have become part of the country's media and civic spaces.

NAMIBIA: At the time of publishing this report, Namibia was the only SADC country without a dedicated cybercrime law or a set of cybercrime offences in a broader law.

TANZANIA: The Cybercrimes Act and the Media Services Act have been used repeatedly to muzzle free expression and prosecute journalists over recent years.

SEYCHELLES: While journalists were generally free to do their work and were not subjected to arrests or violence, there are several aspects of the Penal Code that threaten freedom of expression and of the media.

SOUTH AFRICA: While South African courts have upheld the common law crime of defamation, the courts have also been robust defenders of freedom of expression and media freedom in the post-apartheid era.

ZAMBIA: Specific sections of Zambia's Penal Code have been used over recent years to arrest and charge journalists, while sections of the Cyber Security and Cyber Crimes Act have been used to intimidate the media.

ZIMBABWE: The Criminal Law (Codification and Reform) Act, as amended by the Cyber and Data Protection Act, has in recent times been the basis of arrests of journalists and numerous others for offences related to expression.

CONCLUSIONS

(i) Despite the clear reliance on the Malabo Convention, the SADC Model Law and in some cases the Budapest Convention, there is still a great deal of **variation across the region in both technical and content-based offences**. While local adaption is not a bad thing, one question to consider is whether the variations in national laws will affect international cooperation on cybercrimes, which often involve multiple jurisdictions.

(ii) **Content-based criminal offences** are the ones most often employed to inhibit speech, and these are most often contained in laws other than cybercrime law, such as Penal Codes. **Criminal defamation** and outdated laws on **sedition, "public order"** and **criticism of government officials** are amongst the most common culprits. Some countries (such as Madagascar, Malawi, Tanzania and Zimbabwe) include ill-defined content-based crimes aimed at "**insult**", "**harassment**", "**disturbing the peace**" or publishing **false information** in their cybercrime legislation - which are in some cases so widely and vaguely drafted that they invite subjective application. Topics such as there can be covered in clear and narrowly-defined ways that are more precisely targeted.

(iii) Cybercrime laws often have **provisions prohibiting access to or use of materials originally obtained via illegal access to computer systems**, which

could affect journalists' use of materials from whistleblowers or caches of documents such as Wikileaks or the Panama Papers. We found no evidence of this concern playing out in practice yet, but many cybercrime laws are new and perhaps not yet widely applied.

(iv) **Take-down procedures** which do not involve judicial decision-makers are of concern, although these do not seem to have not yet inspired much discussion or debate in the region to date. This is an area which warrants more-in-depth study, as such provisions can be used to remove online speech on the mere allegation of illegality without sufficient safeguards – and can be particularly dangerous when combined with vague content-based criminal provisions that provide a wide basis for alleging illegality. There is significant variation in the mechanics of such procedures across the region, which could be usefully compared and contrasted, with a view to developing detailed regional recommendations. It would also be useful to collect data on how widely used such provisions are, and in respect of what kinds of speech.

(v) **Prior restraints** on speech tended to take the form of discretionary mechanisms for suspending media activity or revoking media licences.

(vi) There is a need for attention to the **independence of regulatory bodies** – particularly where they have significant degrees of discretion (such as the discretion of suspend or cancel media licences). There also appears to be scope for more exploration of relationships between government regulatory systems and self-regulatory media bodies - an area that is already under discussion and debate in some countries, such as South Africa and Lesotho. Procedures for appointment, accountability and representation of a wide spectrum of stakeholders warrant more detailed examination – along with the question of how the bodies that administer cybercrime regulations will fit into overarching schemes for media regulation.

(vii) **Where there is political will to inhibit speech, legal tools will be found**. Some SADC countries have used mechanisms as unexpected as aviation regulations, allegations of non-payment of utility accounts and bogus charges of illegal drug trafficking to harass journalists. Legal tactics to control speech that is critical of government are likely to become even more pronounced as many crucial elections take place in the SADC region in 2023-2024.

(viii) One area that could be further explored is the **power of the government to close down internet access**, either partially or completely. This power was not typically found in cybercrime laws, but in more general laws on electronic communications.

(ix) **Cybercrime and related media laws are rapidly evolving across the region**, with many new developments. This means that even recent research in this field quickly becomes outdated and must be frequently revised and refreshed.

RECOMMENDATIONS FOR FURTHER REGIONAL RESEARCH

Against this backdrop, the following general recommendations are proffered:

FOR SADC GOVERNMENTS:

(i) Laws regulating freedom of expression and media freedom should be brought in line with best practice guidance and standards and reflective of compliance with international and continental instruments that speak to protecting and enhancing such freedoms;

(ii) SADC member states are encouraged to look to international and continental best practice guidance and examples, such as the Malabo Convention,[5] in the context of domestically legislating for cyber security and cybercrime, and to bring laws and regulatory frameworks in line with such guidance and examples;

(iii) In this regard, states are also encouraged to look to the Declaration of Principles on Freedom of Expression and Access to Information in Africa as guidance in law, policy and regulatory crafting and drafting in the context of free expression and media freedom, as well as cyber security and cybercrime related matters;[6]

(iv) In line with the above, states are explicitly encouraged to build out, where necessary in cyber security and cybercrime laws and regulatory frameworks, meaningful and effective public and judicial oversight and transparency mechanisms as necessary guardrails against executive, law enforcement and state security abuse and overreach;

(v) Similarly, in the context of elections, states are encouraged to give life to the Guidelines on Access to Information and Elections in Africa, both legislatively and practically;[7]

(vi) SADC member states are encouraged to revisit and review criminal defamation and insult provisions, that generally adversely impact media freedom, in their criminal procedure and penal codes with a view to bringing such measures in

[5] African Union Convention on Cyber Security and Personal Data Protection, African Union, 27 June 2014.
[6] The Declaration of Principles of Freedom of Expression and Access to Information in Africa, African Commission on Human and Peoples' Rights, 10 November 2019.
[7] Guidelines on Access to Information and Elections in Africa, African Commission on Human and Peoples' Rights, 15 November 2017.

line with best practice, either through repealing them or updating them, in line with domestic constitutional arrangements.

FOR JOURNALISTS AND THE MEDIA:

(vii) Journalists and the media in countries across the region are encouraged to continuously and persistently focus the glare of public scrutiny on law and regulatory crafting and implementation that threaten freedom of expression and media freedom, both domestically and regionally;

(viii) Specifically, journalists and the media in general are encouraged to proactively engage with law, policy and regulatory crafting and drafting processes – on such issues as promoting the repeal of criminal defamation provisions – that could impact media freedom and freedom of expression generally;

(ix) In the same vein, journalists and the media in countries across the region are encouraged to continuously and persistently contribute to raising public awareness and knowledge of the content and potential impacts of state-driven actions in the realm of cyberspace law and regulation;

(x) Regionally, journalists and media organizations are encouraged to form effective information and advocacy sharing networks that engage at the highest levels with regional governments and international stakeholders on media freedom issues in the digital age.

FOR CIVIL SOCIETY:

(xi) Domestic and regional civil society actors are encouraged to form alliances and collaborations with local and regional media actors to raising local and regional public awareness and knowledge of the content and potential impacts of state-driven actions in the realm of cyberspace law and regulation;

(xii) Similarly, human rights and civil society actors, both domestically and regionally, are encouraged to continuously and persistently focus the glare of public interest advocacy on law and regulatory crafting and implementation that threaten freedom of expression and media freedom, both domestically and regionally.

FOR FURTHER REGIONAL RESEARCH:

Much recent regional analysis has been more descriptive than analytic, particularly when broad topics are covered. Therefore, one useful way forward would be to contrast and compare more narrow, specific topics across the SADC region. Suggestions in this regards would be the following:

- **Criminal defamation**, and regional strategies for advocacy to repeal this crime where it survives.
- **Broad and vague laws on the content of speech**, including insult, harassment, sedition, "public order", criticism of government officials and the publication of false information
- **Take-down procedures**, which are currently found in a variety of laws, with a variety of different approaches - most of which give key decision-making powers to service providers without sufficient monitoring or supervision.

CHAPTER 1

INTRODUCTION AND METHODOLOGY

CHAPTER 1: INTRODUCTION AND METHODOLOGY

This report analyses cybercrime legislation in the SADC region, which could have negative implications for freedom of expression generally and media practitioners in particular.

THE SIXTEEN COUNTRIES IN THE SOUTHERN AFRICAN DEVELOPMENT COMMUNITY (SADC)	
ANGOLA	MAURITIUS
BOTSWANA	MOZAMBIQUE
COMOROS	NAMIBIA
DEMOCRATIC REPUBLIC OF CONGO (DRC)	SEYCHELLES
ESWATINI	SOUTH AFRICA
LESOTHO	TANZANIA
MADAGASCAR	ZAMBIA
MALAWI	ZIMBABWE

THE APPROACH TO THE ANALYSIS

CYBERCRIME CAN BE DIVIDED INTO THREE CATEGORIES:

CATEGORY ONE: Crimes where a computer or an information system is the object of the crime, such as hacking, the spread of malware or other actions that compromise the confidentiality, integrity and availability of computer data and systems (sometimes called "cyber-dependent crimes")
CATEGORY TWO: Crimes where a computer is used as a tool to facilitate the crime, such as fraud and identity theft (sometimes called "cyber-enabled crimes")
CATEGORY THREE: Specific content-related offences, such as the use of computers to spread child pornography or hate speech.[8]

IN THIS ANALYSIS, THE FIRST TWO CATEGORIES WILL BE GROUPED TOGETHER AS "TECHNICAL OFFENCES" IN CONTRAST TO "CONTENT-RELATED OFFENCES".

[8] See, for example, Assessing Cybercrime Laws from a Human Rights Perspective, Global Partners Digital, [2022], page 9; Kirsty Phillips et al, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies", 2(2) Forensic Science 2022, pages 379-398; Prof. Dr. Marco Gercke, "Understanding cybercrime: phenomena, challenges and legal response", International Telecommunications Union, 2012, Chapter 2; "Cybercrime", United Nations Office on Drugs and Crime (UNODC), undated (accessed 23 June 2023).

It is beyond dispute that cybercrime is on the rise in the SADC region, as elsewhere, and that there is a need for legal tools to combat cybercrime. However, one recent analysis asserts that there has been insufficient attention to the human rights impact of cyber legislation in most Southern African countries:

> *With regards to the human rights impact assessment in the development of cybercrime legislation and regulations, the region is at start-up stage, where there is no evidence of human rights impact assessments during the development of cybercrime legislation or cybersecurity regulations in the majority of countries. South Africa is the most advanced in this aspect; the country's cybercrime law recognises the fundamental human rights on the internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. While all countries have laws that protect human rights, due care has to be taken in the development of cybercrime legislation to ensure that the law also protects human rights online.*[9]

[9] "Southern African Development Community Cybersecurity Maturity Report 2021", Cybersecurity Capacity Centre for Southern Africa (C3SA), 2022, page 48 (footnote omitted).

This research report will focus on provisions that are drafted in a way that could allow them to be applied to inhibit freedom of expression, and provisions that have in fact been used to limit press freedom or public debate. At the same time, brief descriptions of all the offences covered in SADC cyberlaws will be included, to allow easy comparison and contrast.

SIMPLIFIED EXPLANATIONS OF TECHNICAL TERMINOLOGY USED IN CYBERCRIME LAWS

Biometrics: records of unique physical characteristics such as fingerprints, voice, and retina used to identify an individual's identity

IP address: (Internet Protocol address): a unique numeric address used by computers on the Internet

Malware: computer code with malicious intentions

Preservation order: an order directing a person with access to a computer or a computer system to preserve specified data to that it can be accessed in future by law enforcement officials

Production order: an order directing a person with access to a computer or a computer system to produce specified data to law enforcement officials

Service provider: any public or private entity that provides users with the ability to communicate by means of a computer system

Spam: unsolicited commercial email

Traffic data: information about communication via a computer or a computer system that indicates the communication's source, destination, route, format, intent, time, date, size, duration, or type - but not its content.

Unauthorized access: can include any access that violates the stated security policy for a computer system or a website.

Based in part on the *Handbook: The Language of Cybercrime*, European Judicial Training Network, 2017

Technical cybercrime offences can be applied in the journalism context in several ways. For instance, information illegally obtained from a computer system might be given to a journalist by a hacker or a whistleblower, or a journalist might obtain information from an online depository that publishes data from such sources.[10] Another example is where investigative journalism might involve posing as an ordinary customer or user on a computer system, adopting a fake identity on social media to expose a trafficker or a child pornographer, altering tracking cookies, disguising an IP address or gaining unauthorised access to a computer system to expose a security vulnerability.[11] Yet another example involves the use of automated tools to load and read information from a website in order to facilitate subsequent analysis ("scraping"), which may be prohibited by the terms of service of the targeted websites – and thus constitute unauthorised access.[12] The ethics of some such practices can be debated, but one issue to consider is whether African cybercrime laws are drafted with sufficient specificity and attention to intent to avoid catching good-faith journalism in their net.[13]

According to Human Rights Watch:

> *A core element of cybercrime laws is usually the criminalization of unauthorized or illegal access to and interference with computer systems and data. These provisions can provide important safeguards against privacy violations and generally strengthen cybersecurity. However, these laws can undermine human rights when they are overbroad, such as by criminalizing mere access to computer systems and data, regardless of intent and without allowing a public interest defence.*[14]

[10] John General, "Analysis: For Journalists, Using Hacked and Surveillance Data Creates Tough Ethical Decisions", *The Click*, 13 October 2021.
[11] See, for some examples, Caroline O'Donovan, "Hacking in the newsroom? What journalists should know about the Computer Fraud and Abuse Act", Nieman Lab, 3 March 2014 (discussing a US cybercrime statute); Katitza Rodriguez et al, "Protecting Security Researchers' Rights in the Americas", Electronic Frontier Foundation, 16 October 2018; Deborah Brown, "When Digital Rights and Cybercrime Collide: A Trial to Watch in Ecuador", *Opinio Juris*. 10 November 2021.
[12] "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021; Katitza Rodriguez et al, "Protecting Security Researchers' Rights in the Americas", Electronic Frontier Foundation, 16 October 2018. According to this article, one US court found that scraping information from a public website "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions".
[13] Rainey Reitman, "When Computer Crimes Are Used To Silence Journalists: Why EFF [Electronic Frontier Foundation] Stands Against the Prosecution of Glenn Greenwald", Electronic Frontier Foundation, 24 January 2020 (suggesting that references to malicious intent in cybercrime laws can help avoid misuse of cybercrime laws against journalists and researchers).
[14] "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.

A second category of potentially problematic legal provisions concerns **content-based crimes** such as harassment, hate speech, criminal defamation or the publication of "fake news" that may be found in laws on cybercrime, general penal codes or other legislation. Again, there is undoubtedly a legitimate need for prohibitions on online harassment and hate speech. The focus here will again be laws that are crafted in a way that violates international standards, or provisions worded in an overly-broad manner that could allow for abuse. At the moment, these appear to be the types of provisions which are being most commonly used in practice to stifle freedom of expression in the SADC region.

> "Laws – from sedition to censorship – have long been used to punish journalists and suppress media freedom. That practice has been revived by some States with a new ferocity in the digital age. The arsenal of legal weapons has broadened to include criminal cyberlibel, anti-terrorism, cybersecurity and fake news laws. In many instances, punishment for online publication is more severe than print or broadcast. Additionally, libel, income tax or other financial investigations and vexatious and frivolous lawsuits are commonly used to harass and intimidate journalists or media outlets.
>
> […]
> Arrests and prosecutions of journalists leading to heavy fines and harsh prison sentences serve not only to intimidate and punish the individuals charged but also to create a climate of fear, chilling critical reporting by other journalists."
>
> "**Reinforcing media freedom and the safety of journalists in the digital age**", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022, paragraphs 51 and 53

A third area of concern involves laws relating to **state surveillance** – such as laws on SIM card registration or other records of internet users, the retention of telecommunications and internet data and access to such data, and legal authority for interception of the content communications or the confiscation of communications devices. Again, there is undoubtedly a legitimate need for effective crime-fighting tools, but it is important that laws on these topics are appropriately targeted with sufficient safeguards against abuse – such as requirements for judicial oversight and guidelines for the exercise of judicial discretion in authorising state surveillance activities.[15] These provisions are often part of cybercrime laws, or else work hand-in-hand with them, as explained by **Human Rights Watch**:

> Cybercrime laws often establish new investigative powers, including allowing authorities to intercept, retain, and access people's data. Obtaining data from internet service providers and other online services such as social media platforms or cloud storage services can be essential for prosecuting cybercrime. But some laws require disproportionate data collection and retention without judicial oversight and basic due process protections. In some cases, law enforcement may be able to obtain stored subscriber data, traffic data, and even content data, directly and in real time. Laws also often impose harsh sanctions on companies for failure to retain data and provide access to law enforcement.

[15] See, for example, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights", A/HRC/39/29. paragraph 34: "Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted."

> […]
> The UN Office of the High Commissioner for Human Rights has criticized governments for imposing mandatory obligations on service providers to retain communications data for extended periods because such requirements limit people's ability to communicate anonymously, create the risk of abuses, and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches.[16]

As a fourth topic, each chapter will also include a brief discussion of **take-down provisions**. Many SADC countries include take-down provisions in their electronic transactions' laws, following the example in the SADC Model Law on Electronic Transactions and Electronic Commerce,[17] although some of these provisions are found elsewhere. The reason why these provisions are included in this analysis requires some explanation. The concept of take-down notifications is to allow online platforms to quickly remove content allegedly to be illegal. The alleged illegality might concern infringements of copyright law or prohibitions on child pornography, non-consensual sharing of intimate images or hate speech (amongst other things). If service providers remove offending material expeditiously in response to such notification, they avoid liability for the content. However, in practice, such provisions raise several concerns. Firstly, they push online platforms to be overly cautious, pre-emptively removing content that may not actually be illegal. Secondly, they force the person who placed the content online to bear the burden of proving that the material does not infringe any rights if they want the content to be restored to the platform – and many take-down procedures do not require any notice to the person who is the source of the removed content or provide for any appeal process. Thirdly, notice and take-down procedures have in some countries generated a need for the use of algorithms to speed up the removal process, and this can lead to inaccuracies that result in the removal of material that is not problematic. In short, these provisions are flagged because they can effectively erase legal speech in some circumstances.[18]

A fifth area of attention concerns **election laws that affect freedom of expression**. Nine SADC countries have elections slated to take place during late 2023 or 2024, [19] which makes examination of the potential brakes on free discussion and debate particularly important in those jurisdictions. For these nine countries, the paper

[16] "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.
[17] SADC Model Law on Electronic Transactions and Electronic Commerce, section 35.
[18] See, for example, Juan Londoño, "Content Moderation Using Notice and Takedown Systems: A Paradigm Shift in Internet Governance", *Insight* column, American Action Forum, 8 November 2021.
[19] "Elections Calendar for SADC-2022-to-2026", SADC Parliamentary Forum website; "SADC Elections Calendar", GENDER & Development in SADC and Southern African Research and Documentation Centre (SARDC); Dr Tabani Moyo, "States in Southern Africa cracking down on free expression online", Media Institute of Southern Africa (MISA), 22 February 2023; "IFES Election Guide: Madagascar", International Foundation for Electoral Systems. Elections for the National Assembly were set to take place in Malawi in 2024, but the Parliamentary and Presidential Elections Act (PPEA) Amendment Act, 2020 extended the term of office for Members of Parliament and ward councillors by one year so that harmonised presidential, parliamentary and local elections can take place in 2025. Enelless Nyali, "Elections May 19", *The Nation*. 25 February 2020.

considers legal provisions that apply specifically to freedom of expression, media coverage and Internet access during elections, to see if there are any particular vulnerabilities.

COUNTRY	TYPE OF ELECTION	NEXT ELECTION
Botswana	President (indirect), General Elections	October 2024
DRC	President, National Assembly	December 2023
Eswatini	Parliament	September 2023
Madagascar	President, National Assembly,	November 2023
Mauritius	General Elections	November 2024
	President (indirect)	December 2024
Mozambique	Local Government	October 2024
	President, National Assembly	October 2024
Namibia	President, National Assembly, Regional Councils	November 2024
South Africa	Provincial legislatures	May 2024
	President (indirect), Parliament	May 2024
Zimbabwe	President, Parliament, Local Government	August 2023

Additionally, there are **miscellaneous legal provisions** that might be applied to restrict freedom of expression – such as the misuse of civil defamation to silence activists, or general laws on topics such as terrorism, national security, money laundering and "foreign agents". A detailed examination of such laws is beyond the scope of this paper, but they will be mentioned in respect of countries where such laws have actually been used against journalists, civil society or opposition politicians – and particularly if they arise in tandem with cybercrime issues.

Legislation is considered along with **literature on the relevant topics, court cases and media reports about the application of specific laws** focusing on incidents dating from 2020 to the present. In fact, the case studies appear *before* the legal discussion in each analysis, to ground each discussion with information about how laws are being applied (or misapplied) in practice.

In addition, because what exists on paper does not necessarily match what takes place in practice, the analyses will be informed by virtual **interviews** with journalists, civil society representatives and academics in the region, with a focus on the countries with elections scheduled for 2023 or 2024.

Analysis of the specific wording of the various cybercrime offences has been guided in part by the **Comprehensive Study on Cybercrime** drafted by the United Nations Office on Drugs and Crime (UNODC).[20]

[20] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. Despite its designation as a draft, this appears to be the most recent version of the document. See "Open-ended intergovernmental expert group meeting on cybercrime", UNODC website, undated, (accessed 23 June 2023), which links to the 2013 draft as well as various country comments on that draft.

WHAT IS NOT COVERED

Most every cybercrime law in the region includes one or more **offences relating to investigations** – criminalising the disclosure of details about a confidential criminal investigation that is underway, obstruction of an investigation in some way, or a refusal by service providers to facilitate an investigation in accordance with the duties under the law. These provisions have not been included in the analysis.

The analysis also omits discussion of **provisions providing for extra-territorial jurisdiction** in respect of cyber offences.

Laws relating specifically to information about the Covid-19 pandemic – which in some instances included stringent curtailments of free expression – are also *not* considered in this analysis because of their specific application.

THE STRUCTURE OF EACH CHAPTER

Each SADC country is considered individually, with the country analyses presented in alphabetical order. The chapter on each country opens with a **table of "key indicators"** that quotes the country's constitutional provisions on freedom of expression and, for context, the country's ranking in the 2023 World Press Freedom Index, as well as listing the key laws that are examined.

The discussion of each country is presented as follows:

1. **Context:** This section gives a brief overview of the regulatory system that affects different forms of expression.

2. **Constitution:** This section provides a short discussion of the constitutional framework on freedom of expression, and a summary of key cases where it has been applied.

3. **Case studies:** This section considers recent examples where laws have been applied in an attempt to constrain freedom of expression.

2023 WORLD PRESS FREEDOM INDEX

This is an annual ranking conducted by Reporters Without Borders, based on a definition of press freedom as "*the ability of journalists as individuals and collectives to select, produce, and disseminate news in the public interest independent of political, economic, legal, and social interference and in the absence of threats to their physical and mental safety.*"

Each country is scored on the basis of a **quantitative count of abuses** against media and journalists in connection with their work, and a **qualitative analysis** of the situation in each country based on the responses of press freedom specialists (including journalists, researchers, academics and human rights defenders) to a questionnaire that considers each country's political, economic and socioeconomic context as well as its legal framework and the physical, psychological, emotional and professional safety of media practitioners.

Note that the regional groupings in this index group North Africa with the Middle East, ranking 48 countries in the remainder of Africa.

World Press Freedom Index, "Methodology"

4. **Cybercrime legislation and other legal provisions relevant to freedom of expression:** Although the focus of the research is cybercrime law, in practice, content-based offences in both cybercrime laws and other laws are most commonly utilised in practice to restrict freedom of expression. Thus, rather than being considered in isolation, the cybercrime laws are discussed alongside other offences which are or may be used to limit speech. This discussion includes information about relevant procedural law as well, including provisions on state investigative powers, state surveillance, SIM card registration and take-down notifications.

5. **Election law and freedom of expression:** In respect of the SADC countries where elections will take place in 2023 or 2024, specific laws and regulations relating to freedom of expression during election periods will be briefly considered.

There is no attempt to draw overarching conclusions in respect of each country's cyber laws. In virtually every case, some specific cybercrimes and related offences are well-crafted while others are overbroad or vaguely defined, which increases opportunities for subjective application. The focus is to discuss specific legal provisions, with an indication of both good and bad practice in respect of individual provisions.

CHAPTER 2

INTERNATIONAL STANDARDS, MODELS AND GUIDELINES

CHAPTER 2: INTERNATIONAL STANDARDS, MODELS AND GUIDELINES

The right to freedom of expression is a foundational right that is protected under the ***Universal Declaration of Human Rights***,[21] the ***International Covenant on Civil and Political Rights***[22] and the ***African Charter on Human and Peoples' Rights***.[23]

Significantly, the ***International Covenant on Civil and Political Rights*** provides for the restriction of freedom of expression only where this is imposed by law and necessary for the protection of the rights or reputations of others, or the protection of national security, public order or public health or morals.[24] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has elaborated this test as follows:

> *Firstly, the restriction must be provided by law in precise and clear terms, and not left to the unfettered discretion of those responsible for its execution. Secondly, it can be imposed only for the specific legitimate objective of respecting the rights or reputations of others or protecting national security, public order, public health or public morals. Thirdly, the restriction must be strictly necessary, appropriate, proportionate and directly relevant to achieving the legitimate objective. Restrictions must be construed narrowly, using the least intrusive measure possible and never going so far as to impair the essence of the right itself.*
>
> *Although the principle of necessity and proportionality deems that journalists should not be prosecuted for disseminating information that is of legitimate public interest, many Governments use laws protecting national security, public order and public morals to clamp down on reporting that is critical of their policies. The Special Rapporteur considers the weaponization of the law against journalists as a major threat to media freedom […].* [25]

[21] *Universal Declaration of Human Rights*, Article 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[22] *International Covenant on Civil and Political Rights*, Article 19: "1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

[23] *African Charter on Human and Peoples' Rights*, Article 9: "1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law."

[24] *International Covenant on Civil and Political Rights*, Article 19(3) (quoted above).

[25] "Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022. paragraphs 19-20 (footnote omitted).

In Africa, the right to freedom of expression has been elaborated in the 2019 ***African Charter on Human and Peoples' Rights (ACHPR) Declaration on the Principles of Freedom of Expression and Access to Information***,[26] which is discussed in some detail below.

The key challenge in a world where access to information is increasingly dominated by online mechanisms is that "there are no easy solutions to modern digital challenges which are both effective in addressing potential harms and yet maintain respect for freedom of expression as guaranteed under international law".[27]

With this challenge in mind, this chapter provides a brief overview of key international standards and guidelines that can be used as yardsticks for assessing laws in the SADC region which may threaten media freedoms.

2.1 CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION), 2001

The Budapest Convention [28] is aimed at improving international cooperation on cybercrime. It originated with the Council of Europe but is open to ratification by any country in the world and currently has six African countries amongst its 68 parties; with respect to SADC, it has been joined by **Mauritius** and signed but not ratified by **South Africa**.[29] It is supplemented by the ***Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003***, which has only two African parties (neither of which is part of SADC) and has additionally been signed but not ratified by South Africa.[30] A ***Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 2022*** was opened for signature in May 2022 but as of June 2023 had only one ratification (Serbia).[31] This Protocol aims at enhancing international cooperation on evidentiary issues that cross jurisdictional boundaries, to facilitate effective and efficient user of such evidence in specific criminal investigations or proceedings.[32]

---

[26] The text of the *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information* can be found here.

[27] Quotation from the Windhoek+30 Declaration, paragraph 12. The Windhoek Declaration and the Windhoek+30 Declaration are described further below.

[28] *Council of Europe Convention on Cybercrime, 2001* ("Budapest Convention").

[29] See "Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Status as of 28/07/2019". The text refers to the status as of 7 June 2023.

[30] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003*. See the "Chart of signatures and ratifications of Treaty 189". The text refers to the status as of 7 June 2023.

[31] The text of the *Second Additional Protocol* is available here, and the status list can be found here. The *Second Additional Protocol* requires five ratifications to enter into force.

[32] "Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence", CETS-224, 12 May 2022, paragraph 22.

Although the Budapest Convention has only the formal support of only a few African nations, it has reportedly influenced legislation and legislative proposals in Botswana, Lesotho, Mauritius, Tanzania and South Africa, as well as the **SADC Model Law on Computer Crime and Cyber Crime** and the **Commonwealth Computer and Computer Related Crimes Model Law**, discussed below.[33]

The Budapest Convention calls for the criminalisation of a range of cybercrimes:[34]

CYBERCRIME OFFENCES PROPOSED BY THE BUDAPEST CONVENTION	
Article 2	unauthorised access to a computer system
Article 3	unauthorised interception of non-public transmissions to, from or within a computer system
Article 4	data interference (unlawful damaging, deleting, deterioration, alteration or suppression of computer data)
Article 5	system interference (seriously hindering the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data)
Article 6	misuse of computer-related devices for criminal purposes
Article 7	computer-related forgery
Article 8	computer-related fraud
Article 9	content-based offences: *child pornography*
Article 10	content-based offences: *infringements of copyright and related rights*
Article 11	attempt, aiding or abetting
Article 12	corporate liability

It has been noted with concern that the Convention make no mention of a public interest defence for journalists or whistleblowers in the cybercrimes it enumerates.[35]

The Budapest Convention also proposes procedures for securing electronic evidence for law enforcement purposes (in respect of cybercrime or any other crimes), including orders for the search and seizure of data, interception of communications and preservation of data:[36]

PROCEDURAL POWERS PROPOSED BY THE BUDAPEST CONVENTION	
Article 16	expedited preservation of stored computer data, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure.
Article 17	expedited preservation and partial disclosure of traffic data (data identifying the service providers and the path through which a communication was transmitted)

[33] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, January-June 2018.
[34] "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.
[35] "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.
[36] "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.

Article 18	production orders (orders to submit to authorities specified computer data or subscriber information)
Article 19	search and seizure of stored computer data
Article 20	real-time collection of traffic data
Article 21	real-time interception of content data in relation to serious offences determined by domestic law

However, it has been emphasised that these powers apply only to specific data for specific criminal investigations and do not cover national security measures or bulk collection of data.[37] The Convention also requires that these procedures must be subject to conditions and safeguards enshrined in law which provide for the adequate protection of human rights and liberties – such as judicial or other independent supervision, the presentation of grounds to justify the application of these procedures, and limitations on the scope and the duration of the investigative powers and procedures.[38]

The *Additional Protocol* calls for additional content-related offences:

ADDITIONAL CYBERCRIME OFFENCES PROPOSED BY THE ADDITIONAL PROTOCOL	
Article 3	dissemination of racist and xenophobic material to the public through a computer system
Article 4	*threats* through a computer system to commit a *serious criminal offence* against a person or a group on the basis of *race, colour, descent, national or ethnic origin or religion* (where religion is used as a pretext for the other characteristics)
Article 5	*insults* made publicly through a computer system against a person or a group on the basis of *race, colour, descent, national or ethnic origin or religion* (where religion is used as a pretext for the other characteristics)
Article 6	using a computer system to distribute or otherwise make available to the public material which denies, grossly minimises, approves or justifies acts constituting *genocide or crimes against humanity*
Article 7	aiding and abetting any of these offences

The *Second Additional Protocol* calls on its State Parties to implement legislation or other measures to facilitate the sharing of information in relation to *specific* criminal investigations or proceedings:

ADDITIONAL PROCEDURES PROPOSED BY THE SECOND ADDITIONAL PROTOCOL	
Article 6	requests for domain name registration information to an entity providing domain name registration services in the territory of another State Party

[37] Id.

[38] Council of Europe Convention on Cybercrime, 2001 ("Budapest Convention"), Article 15.

Article 7	disclosure of subscriber information by service providers in the territory of another State Party
Article 8	giving effect to orders from another State Party for expedited production of subscriber information and traffic data
Article 9	procedures for expedited disclosure of stored computer data in an "emergency", defined as" a situation in which there is a significant and imminent risk to the life or safety of any natural person"
Article 10	procedures for expedited mutual assistance between State Parties in an emergency
Article 11	procedures for permitting testimony and statements to be taken from a witness or expert by remote video conference
Article 12	procedures for joint investigations

The ***Second Additional Protocol*** also calls on State Parties to ensure that the implementation of the powers and procedures provided for in the Protocol are subject to conditions and safeguards that protect human rights and liberties,[39] and includes an extensive provision on the protection of personal data received via the mechanisms set out in the Protocol.[40]

The Council of Europe has noted with concern that some African nations which have adopted cyber laws based on the Budapest Convention have included provisions "that create risks to the freedom of expression and other fundamental rights, in particular where offences are vaguely defined and conditions and safeguards are weak or missing", or where investigative powers are not prescribed precisely, do not provide safeguards against abuse, are not necessary and proportionate, or lack effective remedies.[41]

Furthermore, the Budapest Convention has been criticised by some for failing to strike an appropriate balance between fundamental rights and the prevention of cybercrime.[42]

[39] *Second Additional Protocol*, Article 13.
[40] Id, Article 14.
[41] "The state of cybercrime legislation in Africa – an overview", Council of Europe**,** Version 11, May 2015.
[41] Id.
[42] See, for example, "ARTICLE 19's briefing: The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol", May 2022.

2.2 AFRICAN UNION CONVENTION ON CYBER SECURITY AND DATA PROTECTION (MALABO CONVENTION), 2014

This Convention addresses cybercrime and related issues, including the prohibition of online child pornography and certain forms of hate speech made via computer technology. It has only recently garnered sufficient support to come into force, having achieved the necessary 15 ratifications.[43] The parties to date include only five SADC countries: Angola, Mozambique, Mauritius, Namibia and Zambia, with another two SADC countries having signed but not ratified: Comoros and South Africa.[44]

Leaving aside for the purposes of this discussion the provisions on electronic commerce, electronic contracts and other transactions and personal data protection, the Malabo Convention calls for the criminalisation of a range of cybercrimes and related evidentiary procedures:[45]

CYBERCRIME OFFENCES PROPOSED BY THE MALABO CONVENTION	
Article 29.1	attacks on computer systems, including: • unauthorised access to a computer system • system interference • fraudulent entry of data • data interference • dealing in computer-related devices designed or adapted for criminal purposes
Article 29.2	computerised data breaches (including unauthorised interception of non-public transmissions to, from or within a computer system, taking steps to produce inauthentic computer data, and knowingly using computer data fraudulently obtained)
Article 29.3	content-related offences, including: • offences related to *child pornography* and exposing children to pornographic material • using a computer system for any representation of "*ideas or theories* of a *racist or xenophobic nature*" • *threats* through a computer system to commit a criminal offence against a person or a group on the basis of *race, colour, descent, national or ethnic origin or religion* (where religion is used as a pretext for the other characteristics) • *insulting* a person or a group through a computer system on the basis of *race, colour, descent, national or ethnic origin or*

[43] "AU Convention on Cyber Security and Personal Data Protection: Malabo Convention", Michaelson's, 24 April 2023. The treaty came into force on 8 June 2023. June 15, 2023. Yohannes Eneyew Ayalew, "The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?", *EJIL: Talk!*, Blog of the European Journal of International Law, 15 June 2023.
[44] *African Union Convention on Cyber Security and Data Protection, 2014*, Article 36: Entry into Force; Status List (dated 11 April 2023). The status list as accessed on 15 July 2023 was not up-to-date.
[45] "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.

	religion (where religion is used as a pretext for the other characteristics) • denying, justifying or approving through a computer system acts of *genocide or crimes against humanity*
Article 29.4	steps to ensure that properly-verified digital evidence is admissible in criminal cases
Article 30	adapting certain crimes cover computer technologies; criminal liability of legal persons
Article 31.1-2	appropriate criminal sanctions

PROCEDURAL POWERS PROPOSED BY THE MALABO CONVENTION	
Article 31.3	search and seizure of stored computer data; preservation orders, up to a maximum of two years

Article 25.3 of the Malabo Convention specifically requires that legal measures adopted in the sphere of cybersecurity must not infringe the rights of citizens guaranteed under national constitutions and domestic laws or protected by international conventions – particularly the *African Charter on Human and Peoples' Rights*. Article 25.3 also specifically mentions the need to protect "basic rights such as freedom of expression, the right to privacy and the right to a fair hearing".

The Malabo Convention does not contain a general reference to public interest defences, but it does cite malicious intent in respect of some offences. It proposes that States should criminalise unauthorised access to a computer system where it takes place with intent to commit or facilitate another criminal offence.[46]

It also notes in respect of the offence of inputting, altering, deleting or suppressing computer data that a State Party *may* require an intent to defraud or a "similar dishonest intent" before attaching criminal liability.[47]

The Convention has been criticised by some for using vague terms such as "insult" that could give rise to problematic interpretations, and for overly-broad justifications for judicial authority for state surveillance.[48]

[46] *African Union Convention on Cyber Security and Data Protection, 2014*, Article 29.1(b).
[47] Id, Article 29.2(b).
[48] See, for example, "Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'". CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence), undated, text and footnote 1; Lukman Adebisi Abdulrauf & Charles Manga Fombad. "The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?", paper presented at the 7th International Conference on Information Law and Ethics (ICIL) at the University of Pretoria, South Africa, 22-23 February 2016.

2.3 SADC COMPUTER CRIME AND CYBERCRIME MODEL LAW, 2012

In 2012, SADC developed the "SADC Harmonised Cyber Security Legal and Regulatory Framework" which is made up of three model laws: the Computer Crime and Cybercrime Model Law, the Data Protection Model Law and the E-Commerce/E-Transaction Model Law.[49]

According to SADC, as of 2022, all SADC Member States have either adopted versions of the Cybercrime Model Law or had a pre-existing legal framework in place for cybercrime, while ten SADC Member States had data protection laws with another four working on draft legislation on this topic.[50]

The SADC Model Law includes provisions on the crimes listed in the table below. Its many overlaps with the Budapest Convention and its Additional Protocol and the Malabo Convention are obvious.

CRIMES IN THE SADC COMPUTER CRIME AND CYBERCRIME MODEL LAW, 2012	
Section 4	*illegal access*: accessing the whole or any part of a computer system without lawful excuse or justification
Section 5	*illegal remaining:* remaining logged into a computer system without lawful excuse or justification
Section 6	*illegal interception* of any non-public transmission to, from or within a computer system
Section 7	*illegal data interference*
Section 8	*data espionage:* obtaining computer data for oneself or another which is not meant to be shared in this way and which is specially protected against unauthorized access, without lawful excuse or justification
Section 9	*illegal system interference*, which includes hindering or interfering with the functioning of a computer system; or a person who is lawfully using or operating a computer system
Section 10	*dealing in devices* designed or adapted for computer crimes, or *dealing in passwords, codes etc* intended for the purpose of committing a crime
Section 11	*computer-related forgery*
Section 12	*computer-related fraud*
Section 13	*child pornography involving a computer system*
Section 14	*making pornography available to children via a computer system*
Section 15	*identity-related crimes:* transferring, possessing, or using, a means of identification of another person via a computer system for criminal purposes without lawful excuse or justification

[49] The text of the 2012 *SADC Computer Crime and Cybercrime Model Law* can be found here.
[50] SADC, "Consultancy for the Review and Modernisation of the SADC Cyber Crime Model Law", 22 September 2022.

Section 16	producing, distributing or transmitting *racist and xenophobic material* via a computer system, with this being defined as any material that "advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors"
Section 17	*insults* made publicly against a person or a group through a computer system on the basis of *race, colour, descent, national or ethnic origin or religion* (where religion is used as a pretext for the other characteristics)
Section 18	using a computer system to distribute or otherwise make available to the public material which denies, grossly minimises, approves or justifies acts constituting *genocide or crimes against humanity*
Section 19	*offences related to "spam"*
Section 20	*disclosure of a confidential order related to a criminal investigation by an Internet service provider*
Section 21	*failure to assist with an order related to a criminal investigation* (by a person other than the suspect)
Section 22	*harassment via electronic communication:* initiating an electronic communication "with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person", or "using a computer system to support severe, repeated, and hostile behavior"

The SADC Model Law also covers the procedural issues listed in the table below.

PROCEDURAL ISSUES COVERED BY THE SADC COMPUTER CRIME AND CYBERCRIME MODEL LAW, 2012	
Section 25	*search and seizure* based on a warrant issued by a judicial officer and supported by information on oath that there are reasonable grounds to suspect that a place contains a thing or computer data that may be material as evidence in proving a criminal case or that has been acquired by a person as a result of a criminal offence
Section 26	*duty of persons other than the suspect to assist with a search of computer data*
Section 27	*production orders* to a person in control of a computer system or an internet service provider
Section 28	*expedited preservation orders* by law enforcement officers in respect of computer data reasonably required for the purposes of a criminal investigation that is particularly vulnerable to loss or modification, for up to 7 days, which may be extended for a further 7 days by a judicial officer
Section 29	*partial disclosure of traffic data about specified communications* to identify the Internet service providers;

	and/or the path through which a communication was transmitted
Section 30	*collection of traffic data associated with specified communications* reasonably required for the purposes of a criminal investigation, on the authority of a judicial officer (including real-time traffic data)
Section 31	*targeted interception of content data* on the authority of a judicial officer
Section 32	*targeted use of remote forensic tools for collection of data from a computer system*

It has been asserted that this proposed legal framework prioritises the protection of 'national interests' and the prevention of 'social media abuse' at the expense of the digital security and privacy of internet users in the SADC region.[51] The SADC Model Law has been criticised for including provisions that provisions that "actively infringe on the fundamental right to privacy" and "can easily be used to justify intrusive communications surveillance", with insufficient safeguards.[52] Another assessment says that the model law is "generally fraught with failed attempts at innovation, poor language and drafting, technically and legally incorrect and overreaching provisions".[53]

In September 2022, SADC advertised for a consultant to revise and modernise the Cybercrime Model Law by incorporating international best practices, to review all existing cybercrime laws in the SADC Member States and to prepare the SADC Cybercrime Guidelines to facilitate effective implementation of the cybercrime laws.[54]

2.4 COMMONWEALTH COMPUTER AND COMPUTER-RELATED CRIME MODEL LAW, 2002

This model law was first adopted at the 2002 Commonwealth Conference of Ministers and has reportedly been utilised by at least 22 Commonwealth nations as the basis of their national cybercrime legislation[55] - although there is some evidence that its influence has waned in recent years. It is currently being reviewed with a view to the

[51] "How SADC Government Cybersecurity Laws Impact Human Rights", ICT Works, 17 November 2021.
[52] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 20.
[53] Zahid Jamil, "Cybercrime Model Laws: Discussion paper prepared for the Cybercrime Convention Committee", Council of Europe, 9 December 2014.
[54] Id.
[55] See "Commonwealth model law promises co-ordinated cybercrime response", The Commonwealth, 22 April 2016. The text of the 2002 *Commonwealth Computer and Computer-Related Crime Model Law* is available here.

adoption of an updated version.[56] This model law may be of particular relevance to the 11 SADC countries which are also members of the Commonwealth: Botswana, eSwatini, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania and Zambia. However, given the age of this model law and its apparently limited influence in the SADC region, it will not be utilised as a key reference in the ensuing analysis.

2.5 AFRICAN CHARTER ON HUMAN AND PEOPLES' RIGHTS (ACHPR) DECLARATION ON THE PRINCIPLES OF FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION, 2019

This Declaration was adopted by the African Commission on Human and Peoples' Rights in 2019 pursuant to Article 45.1 of the African Charter on Human and Peoples' Rights which requires the African Commission to promote human and peoples' rights by formulating and laying down principles and rules relating to human and peoples' rights and fundamental freedoms upon which African States may base legislation. The 2019 Declaration replaces the Declaration of Principles on Freedom of Expression in Africa adopted by the African Commission in 2002, with a view to elaborating on access to information and the interface between freedom of expression and the internet.[57]

The opening Principle of this Declaration emphasises the importance of freedom of expression and access to information "for the free development of the human person, the creation and nurturing of democratic societies and for enabling the exercise of other rights". Principle 10 states:

> *Freedom of expression, including the right to seek, receive and impart information and ideas, either orally, in writing or in print, in the form of art or through any other form of communication or medium, including across frontiers, is a fundamental and inalienable human right and an indispensable component of democracy.*

This statement of principles is discussed at some length because it emanates from Africa and because it contains a comprehensive set of progressive principles on freedom of expression and journalistic freedom.

[56] See, for example, Zahid Jamil, "Cybercrime Model Laws", discussion paper prepared for the Cybercrime Convention Committee, 9 December 2014.
[57] *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, "Introduction".

Principle 9 is particularly important for this discussion, so it is quoted here in full:

PRINCIPLE 9. JUSTIFIABLE LIMITATIONS

1. States may only limit the exercise of the rights to freedom of expression and access to information, if the limitation:

    a. is prescribed by law;
    b. serves a legitimate aim; and
    c. is a necessary and proportionate means to achieve the stated aim in a democratic society.

2. States shall ensure that any law limiting the rights to freedom of expression and access to information:

    a. is clear, precise, accessible and foreseeable;
    b. is overseen by an independent body in a manner that is not arbitrary or discriminatory; and
    c. effectively safeguards against abuse including through the provision of a right of appeal to independent and impartial courts.

3. A limitation shall serve a legitimate aim where the objective of the limitation is:

    a. to preserve respect for the rights or reputations of others; or
    b. to protect national security, public order or public health.

4. To be necessary and proportionate, the limitation shall:

    a. originate from a pressing and substantial need that is relevant and sufficient;
    b. have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; and
    c. be such that the benefit of protecting the stated interest outweighs the harm to the expression and disclosure of information, including with respect to the sanctions authorised.

The first three criteria in **Principle 9.1** appear in numerous global guidelines and declarations,[58] yet some of the laws discussed here do not appear to satisfy the criteria of being necessary and proportionate.

[58] Article 19(3) of the *International Covenant on Civil and Political Rights* requires restrictions on the freedom of expression only if they are "provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (*ordre public*), or of public health or morals."
See also, for example, the Special Rapporteurs' Joint Declaration on Media Freedom and Democracy, 2023 and Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, 2017. The Joint Declarations are discussed further below.

There are several other principles with particular relevance to the current analysis.

Principle 20 calls on states to guarantee the safety of journalists and other media practitioners, including the adoption of measures to prevent attacks, murder, torture, other forms of ill-treatment, arbitrary arrest and detention, enforced disappearance, kidnapping, intimidation, threats and unlawful surveillance by or non-State actors. It also says that States must be held liable for the conduct of law enforcement, security, intelligence, military and other personnel which threatens, undermines or violates the safety of journalists and other media practitioners. States are enjoined to pay particular attention to the safety of female journalists and media practitioners, and to respect the non-combatant status of journalists in times of armed conflict.

Principle 21 calls on States to incorporate the following standards into their defamation laws:

a. No one shall be found liable for true statements, expressions of opinions or statements which are reasonable to make in the circumstances.
b. Public figures shall be required to tolerate a greater degree of criticism.
c. Sanctions shall never be so severe as to inhibit the right to freedom of expression.

Principle 21 also directs that privacy and secrecy laws must not inhibit the dissemination of information of public interest.

In respect of criminal offences, **Principle 22** requires states to review all content-based crimes to ensure that they are "justifiable and compatible with international human rights law and standards", and to repeal laws that criminalise sedition, insult and publication of false news. While it does not explicitly demand the repeal of criminal laws on defamation, it proposes that all custodial sentences for defamation should be substituted with necessary and proportionate civil sanctions. It states further that freedom of expression shall be restricted on public order or national security grounds only if there is a real risk of harm to a legitimate interest as well as "a close causal link" between the risk of harm and the speech in question.

Real risk of harm to a legitimate interest as well as "a close causal link" between the risk of harm and the speech in question.

Principle 23 supports the prohibition of speech that advocates "national, racial, religious or other forms of discriminatory hatred which constitutes incitement to discrimination, hostility or violence". However, it urges States to criminalise prohibited speech only as a last resort and only for the most severe cases. In determining the threshold of severity that may warrant criminal sanctions, it proposes that States shall take the following factors into account:

a. prevailing social and political context;
b. status of the speaker in relation to the audience;
c. existence of a clear intent to incite;
d. content and form of the speech;

e. extent of the speech, including its public nature, size of audience and means of dissemination;
f. real likelihood and imminence of harm.

Principle 23 also calls upon States not to prohibit speech "that merely lacks civility, or which offends or disturbs".

Another principle that warrants highlighting here is **Principle 25** on the protection of sources and other journalistic material. It states that media practitioners must not be required to reveal confidential sources of information or other material held for journalistic purposes except where a court has ordered disclosure after a full and fair public hearing.

Furthermore, it states that a court should only order disclosure in the following limited circumstances:

a. the identity of the source is necessary for the investigation or prosecution of a serious crime or the defence of a person accused of a criminal offence;
b. the information or similar information leading to the same result cannot be obtained elsewhere; and
c. the public interest in disclosure outweighs the harm to freedom of expression.

Significantly, **Principle 25** also requires that "States shall not circumvent the protection of confidential sources of information or journalistic material through the conduct of communication surveillance except where such surveillance is ordered by an impartial and independent court and is subject to appropriate safeguards."

On the topic of Internet access, **Principle 38** emphasises that States must not interfere with the right of individuals to seek, receive and impart information through any communication and digital technologies by removing, blocking or filtering content, except in cases where the interference is justifiable and compatible with international human rights law and standards. It also enjoins States not to engage in or condone any disruption of public access to the Internet or other digital technologies.

State-mandated removal of online content is covered in **Principle 39**, which requires that this should take place only on the basis of a request that is:

a. clear and unambiguous;
b. imposed by an independent and impartial judicial authority…
c. subject to due process safeguards;
d. justifiable and compatible with international human rights law and standards; and
e. implemented through a transparent process that allows a right of appeal.

The only exception is where law-enforcement agencies request expedited or immediate removal of online content that poses an imminent danger or a real risk of

death or serious harm to a person, provided that such removal is subject to review by a judicial authority.

On the topic of privacy and communication surveillance, **Principle 40** states that everyone has the right to communicate anonymously or use pseudonyms on the internet, and to use digital technologies to secure the confidentiality of their communications and personal information against access by third parties – with States being directed to adopt laws or other measures that penetrate encryption only where this is justifiable and compatible with international human rights standards.

Principle 41 says that States must not engage in or condone "acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications". Targeted surveillance is permissible only where authorised by a law that conforms with international human rights law and standards, and where it is based on a specific and reasonable suspicion that a serious crime has been or is being carried out, or on the basis of some other legitimate aim.

2.6 JOINT DECLARATIONS OF THE SPECIAL RAPPORTEURS

This is a series of declarations issued annually since 1999 jointly by the United Nations Special Rapporteur on Freedom of Opinion and Expression and three **regional Special Rapporteurs** concerned with freedom of expression:

- the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media
- the Organization of American States (OAS) Special Rapporteur on Freedom of Expression
- the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information.[59]

These **Joint Declarations** will be referenced in respect of individual countries as relevant. The specific topics covered in recent years by these declarations are as follows:

- 2023-media freedom and democracy
- 2022-freedom of expression and gender justice
- 2021-politicians and public officials and freedom of expression
- 2020-freedom of expression and elections in the digital age
- 2019-challenges to freedom of expression in the next decade
- 2018-media independence and diversity in the digital age
- 2017-freedom of expression and "fake news", disinformation and propaganda
- 2016-freedom of expression and countering violent extremism

[59] The complete set of Joint Declarations can be accessed here.

- 2015-freedom of expression and responses to conflict situations
- 2014-universality and the right to freedom of expression
- 2013-the protection of freedom of expression and diversity in the digital terrestrial transition
- 2012-crimes against freedom of expression
- 2011-freedom of expression and the Internet
- 2010-key challenges to media freedom
- 2009-media and elections
- 2008-defamation of religions, and anti-terrorism and anti-extremism legislation.

2.7 WINDHOEK DECLARATIONS

The original ***Windhoek Declaration for the Development of a Free, Independent and Pluralistic Press*** is a statement of key principles relating to press freedom developed by African newspaper journalists emanating from a 1991 conference in Windhoek, Namibia, which inspired similar declarations in other regions of the world. This initiative also gave birth to World Press Freedom Day, now celebrated worldwide on May 3 – the date when the Windhoek Declaration was adopted.[60] The key problems affecting journalism in Africa in 1991 were set out as follows:

> In Africa today, despite the positive developments in some countries, in many countries journalists, editors and publishers are victims of repression - they are murdered, arrested, detained and censored, and are restricted by economic and political pressures such as restrictions on newsprint, licensing systems which restrict the opportunity to publish, visa restrictions which prevent the free movement of journalists, restrictions on the exchange of news and information, and limitations on the circulation of newspapers within countries and across national borders. In some countries, one-party States control the totality of information.[61]

Thirty years later, in 2021, the ***Windhoek+30 Declaration*** agreed upon at another international meeting of media professionals in Windhoek emphasised the new opportunities and challenges presented by the digital transformation that has both facilitated access to information and amplified disinformation and hate speech, as well as expressing concern about the "enduring and new threats to the safety of

[60] See "30th Anniversary of the Windhoek Declaration", UNESCO website. The text of the 1991 Windhoek Declaration is available here.
[61] *Windhoek Declaration, 1991*, paragraph 6.

journalists and the free exercise of journalism".[62] This 2021 Declaration cited the following threats:

> Killings, harassment of women, offline and online attacks, intimidation and the promotion of fear, and arbitrary detentions, as well as the adoption of laws which unduly restrict freedom of expression and access to information in the name, among other things, of prohibiting false information, protecting national security and combating violent extremism; and also deeply concerned at the increasing numbers of Internet disruptions, including Internet shutdowns, particularly during elections and protests.[63]

It called on States to take the following steps:

- to create a positive enabling environment for freedom of expression, online and offline;
- to adopt appropriate legal measures in a transparent manner after adequate public consultation;
- to guarantee the exercise of journalism free of formal or informal governmental interference;
- to promote universal access to the Internet; and
- to take measures to reinforce the safety of journalists, with a specific focus on women journalists.[64]

2.8 CRIMINAL DEFAMATION

In 2010, the African Commission on Human and Peoples Rights issued ***Resolution 169 on Repealing Criminal Defamation Laws in Africa***, which calls on States Parties to the African Charter to repeal criminal defamation laws, because such laws impede freedom of speech and hamper the role of the media as a watchdog.[65]

The African Court on Human and People's Rights ruled in 2014, in ***Konaté v Burkina Faso***, that long imprisonment for the crimes of criminal defamation, public insult and contempt was a "disproportionate interference" with the right of freedom of expression[66] - with four of the ten judges on the Court asserting that criminal defamation laws are *never* permissible regardless of the type of sanction imposed.[67]

---

[62] *Windhoek+30 Declaration*, paragraphs 9, 11, and 13; quote from paragraph 13.
[63] Id, paragraph 13.
[64] Id, paragraph 16.
[65] African Commission on Human and Peoples Rights, "Resolution 169 on Repealing Criminal Defamation Laws in Africa", 2010.
[66] *Konaté v Burkina Faso*, African Court on Human and People's Rights, Application No. 004/2013, 5 December 2014.
[67] Id, "Separate Opinion".

As noted above, the ***African Charter on Human and Peoples' Rights (ACHPR) Declaration on the Principles of Freedom of Expression and Access to Information, 2019*** recommends that all custodial sentences for defamation should be substituted with necessary and proportionate civil sanctions.[68]

Courts in several African countries (including Lesotho, Kenya and Zimbabwe) have ruled that criminal defamation punishable by imprisonment is a violation of the principle of free speech[69] – but this crime was upheld as being constitutionally acceptable in South Africa by the Supreme Court of Appeal in 2008.[70]

According to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> *Criminal defamation and lese-majesty laws are frequently used against journalists who criticize government officials or members of royal families. Not only are criminal penalties, especially imprisonment, inherently disproportionate when used against journalists who are simply doing their job, they are an abuse of power by public officials. Those who serve in public office should expect a higher degree of public scrutiny and be open to criticism.*[71]

The UN Special Rapporteur recently reiterated her previous call for a global ban on the criminalization of defamation and seditious libel online and offline.[72]

2.9 PRIVACY AND FREEDOM OF EXPRESSION

Both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights protect against "arbitrary or unlawful interference" with privacy, family, home or correspondence.

---

[68] *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 22.

[69] **Lesotho:** *Peta v Minister of Law, Constitutional Affairs and Human Rights* (CC 11/2016) [2018] LSHC 3 (18 May 2018); **Kenya:** *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR. An appeal is reportedly pending. Carmel Rickard, "Pen Report: Criminal Defamation is Used to Stifle Dissent in Africa", *AfricanLII,* 20 April 2018. **Zimbabwe:** *Madanhire & Another v AG* (CCZ 2/14 Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); "Concourt outlaws Criminal Defamation", *The Herald*, 4 February 2016; *MISA-Zimbabwe v Minister of Justice* (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.

[70] *Hoho v The State* 2009 (1) SACR 276 (SCA) at paras 27-36, citing a similar conclusion in Granada: *Worme and another v Commissioner of Police of Grenada* [2004] UKPC 8 at 455E-F para 42 and *R v Lucas* [1998] SCR 439 at para 55. The Supreme Court of India also upheld the constitutionality of criminal defamation in 2016, finding that this law constitutes a reasonable restriction on the right to freedom of expression *Subramanian Swamy v Union of India* (2016) 7 SCC 221.

[71] Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022, paragraph 57 (footnotes omitted).

[72] Id, paragraph 58.

Unlawful interference with privacy, or even the possibility that this might take place, can have a serious chilling effect on the right to free expression as well as other fundamental rights.[73]

The digital age has introduced new possibilities for State violations of individual privacy. In order to pass muster under international standards as a restriction on privacy that is neither arbitrary nor unlawful, the interference must be authorised by a national law that does not conflict with the provisions of the International Covenant on Civil and Political Rights, as well as being proportional and necessary to a legitimate aim.[74]

REGISTRATION OF SUBSCRIBERS

One problematic issue often associated with cybercrime is the enactment of laws requiring internet and telecommunications service providers to record and retain data about the activity of all of its clients or subscribers in case this is needed in future by law enforcement officials.

A 2015 Report on encryption, anonymity, and the human rights framework by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression considered encryption and anonymity in communications in light of the rights to privacy and freedom of opinion and expression, noting that these options "provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".[75] The Report also notes that laws requiring SIM card registration directly undermine anonymity and "may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest".[76]

The Special Rapporteur also observed that restrictions on encryption and anonymity, because they restrict right to freedom of expression, must meet the well-established test for justification of restrictions on that freedom.[77] The Special Rapporteur recommended that "… States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users".[78]

Similarly, the 2018 report on The Right to Privacy in the Digital Age by the Office of the UN High Commissioner for Human Rights states:

[73] "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, paragraph 20.
[74] Id, paragraph 21, citing General Comment No. 16 of the Human Rights Committee that monitors compliance with the International Covenant on Civil and Political Rights.
[75] "Report on encryption, anonymity, and the human rights framework", Special Rapporteur on freedom of opinion and expression, A/HRC/29/32, 22 May 2015, paragraph 16.
[76] Id, paragraph 51.
[77] Id, paragraphs 31-35.
[78] Id, paragraph 60.

> *Encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks.*[79]

As noted above, the ***(ACHPR) Declaration on the Principles of Freedom of Expression and Access to Information, 2019*** has endorsed similar principles, stating that everyone has the right to communicate anonymously or via pseudonyms on the internet, and to have encrypted communications penetrated only where this is justifiable under international human rights standards.[80]

MASS SURVEILLANCE AND DATA RETENTION

A 2014 report on ***The Right to Privacy in the Digital Age*** **by the Office of the UN High Commissioner for Human Rights** expressed concern about "the increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes":

> *Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.*[81]

This report notes that a legitimate aim is not sufficient to justify mass or "bulk" surveillance programmes, because "it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate".[82]

Concerns about mass surveillance were reiterated in the 2016 report on ***The Right to Privacy in the Digital Age*** **by the Office of the UN High Commissioner for Human Rights**, which noted that indiscriminate mass surveillance cannot be justified on national

[79] "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/39/29, 3 August 2018, paragraph 20.
[80] *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 40.
[81] "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, paragraph 26. On this point, the report references the Addendum to General Comment No. 27, Human Rights Committee, CCPR/C/21/Rev.1/Add.9, 1 November 1999, paras 11-16, https://undocs.org/CCPR/C/21/Rev.1/Add.9.
[82] Id, paragraph 25.

security grounds, since an individualized necessity and proportionality analysis would not be possible in these circumstances.[83]

The ***(ACHPR) Declaration on the Principles of Freedom of Expression and Access to Information, 2019*** also disapproves of the indiscriminate and untargeted collection of data about a person's communications, as opposed to situations where the data collection is authorised by law and based on a specific and reasonable suspicion relating to a serious crime, or to advance some other legitimate aim. This Declaration also recommends that any law that authorises targeted communication surveillance must provide adequate safeguards for the right to privacy, including the following:

a. the prior authorisation of an independent and impartial judicial authority;
b. due process safeguards;
c. specific limitation on the time, manner, place and scope of the surveillance;
d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
e. proactive transparency on the nature and scope of its use; and
f. effective monitoring and regular review by an independent oversight mechanism.

The Declaration does not discuss any exceptions for urgent collection of evidence which is in danger of being removed or destroyed, nor does it discuss the use of preservation orders (where a service provider is required to preserve data that may be required as evidence).[84]

THE FOLLOWING INTERNATIONAL DOCUMENTS RELATE TO ELECTIONS AND ARE CONSIDERED HERE ONLY IN RESPECT OF THEIR RELEVANT TO THE ROLE OF THE MEDIA DURING ELECTIONS IN THE SADC REGION.

2.10 GUIDELINES ON ACCESS TO INFORMATION AND ELECTIONS IN AFRICA, 2017

The African Commission on Human and Peoples' Rights adopted these Guidelines in 2017, on the basis of a draft prepared by the Special Rapporteur on Freedom of Expression and Access to Information in Africa, after consultations with African experts in the fields of access to information and elections.[85]

The Guidelines contain two sections on elections and the media which focus on ensuring fair and balanced coverage of the electoral process as well as transparency. The Guidelines discourage Internet shutdowns during election periods but

[83] Id, paragraph 27.
[84] *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 41.
[85] A link to the text of the Guidelines is available here; the Guidelines can also be found here. The background to their adoption is set out in the introduction.

contemplate "exceptional cases" where such shutdowns may be permissible under international law.

MEDIA AND INTERNET REGULATORY BODIES

25. Media and internet regulatory bodies shall adopt regulations on media coverage during elections that ensure fair and balanced coverage of the electoral process and transparency about political advertising policy on media and online media platforms. Such regulations shall proactively disclose to the public:

(a) The complaints procedure against media organizations that violate the regulations;
(b) The enforcement mechanism for ensuring compliance with the decisions taken and sanctions imposed;
(c) The code of conduct for online media; and
(d) Details of all complaints or petitions received during the electoral period and how these were addressed.

26. The body responsible for regulating the broadcast media and any other relevant national security, public or private body involved in the provision of telecommunication services shall refrain from shutting down the internet, or any other form of media, during the electoral process.

27. In exceptional cases in which a shutdown may be permissible under international law, the reasons for any shutdown shall be proactively disclosed. Such limitation shall:

(a) Be authorised by law;
(b) Serve a legitimate aim; and
(c) Be necessary and proportional in a democratic society.

28. Any decision of the Media or Internet Regulatory Body shall be subject to judicial review, which shall be undertaken on an expedited basis.

THE MEDIA AND ONLINE MEDIA PLATFORM PROVIDERS

29. Print, broadcast and online media, whether publicly or privately owned, shall proactively disclose the following:

(a) Editorial and ethical codes or guidelines utilised in undertaking election coverage, including provisions prohibiting incitement to discrimination, hostility or violence, if any;
(b) Sanctions for transgressions of these codes or guidelines;
(c) Complaints procedures for handling breaches of these codes or guidelines;
(d) Number of complaints received and how these were addressed;
(e) Code of conduct for staff on procedural matters;

(f) Criteria for the allocation of airtime or news coverage for political campaign advertisements and activities;
(g) Polling methodologies and margins of error;
(h) Actual allocation of airtime or news coverage for political campaign advertisements and activities;
(i) Plan for transparent repository of all political advertisements, including those targeted at individuals or specific groups on online media;
(j) Coverage plan for election day;
(k) Criteria for the selection of election commentators, political analysts or other experts;
(l) Guidelines on responsible use of online media; and
(m) Conflict of interest media ownership information, political affiliations or party support arrangements, if any.

2.11 REVISED SADC PRINCIPLES AND GUIDELINES GOVERNING DEMOCRATIC ELECTIONS, 2015

These Guidelines were adopted by SADC's Ministerial Committee of the Organ on Politics, Defence and Security Cooperation in 2015 after broad consultation with stakeholders and regional experts. They replace the previous 2008 Guidelines.[86]

Like the 2008 Guidelines, the 2015 revised Guidelines pay scant attention to the role of the media in democratic elections, although the concept of free elections set out in the document includes references to freedom of speech and expression as well as freedom of access to information:

> *"Free (elections)" means 'Fundamental human rights and freedoms are adhered to during electoral processes, including freedom of speech and expression of the electoral stakeholders; and freedom of assembly and association; and that freedom of access to information and right to transmit and receive political messages by citizens is upheld; that the principles of equal and universal adult suffrage are observed, in addition to the voter's right to exercise their franchise in secret and register their complaints without undue restrictions or repercussions.'*[87] *[emphasis added]*

The revised Guidelines further emphasise this by identifying as one of the key principles for conducting democratic elections that all citizens must enjoy fundamental

[86] The text of the Revised 2015 Guidelines can be found here (the text could not be accessed on the SADC website at the time of writing). The background to their adoption is set out in the introduction. (The text of the previous 2008 Guidelines can be found here, as a point of comparison.)
[87] *Revised SADC Principles and Guidelines Governing Democratic Elections, 2015*, Definitions of Concepts and Acronyms.

freedoms and human rights "including freedom of association, assembly and expression".[88]

Another fundamental principle is the promotion of "necessary conditions to foster transparency, freedom of the media; access to information by all citizens; and equal opportunities for all candidates and political parties to use the state media".[89]

The revised Guidelines also require States to take "reasonable measures to guarantee political parties and other electoral stakeholders, unhindered access to, and to communicate freely with, the media".[90]

But there is no additional discussion of the role of the press in general, and no reference to the internet or online media.

2.12 SADC MODEL LAW ON ELECTIONS, 2018

The Plenary Assembly Session of the SADC Parliamentary Forum unanimously adopted the SADC Model Law on Elections in 2018, and urged SADC States to incorporate its provisions into their domestic election laws.[91]

The Model Law emphasises the importance of freedom of expression and access to information as critical components of the electoral process:

> **16. Freedom of opinion and expression**
> Free communication of information and ideas by voters and candidates is essential to genuine elections and shall be protected by the State. It may only be restricted under circumstances prescribed by law, as necessary in an open and democratic society, and for the protection of the rights of others as per the law.
>
> **17. Access to information**
> It is the duty of the State to guarantee citizens' right to request and receive information as a critical means of ensuring transparency and accountability throughout the electoral process.

Moreover, it contains an entire chapter with details about the role of the media in elections, reproduced below.

[88] Id, paragraph 4.1.2.
[89] Id, paragraph 4.1.6.
[90] Id, paragraph 5.1.10
[91] "SADC Model Law on Elections adopted", SADC Parliamentary Forum website, undated. The text of the model law is available here. The introduction to the model law gives more background information on its adoption.

SADC MODEL LAW ON ELECTIONS, 2018

PART XIII: MEDIA

61. Access to media

All political parties and candidates shall be afforded equal opportunity to access to the public media to disseminate their ideas, manifestos for free.

62. Impartiality of media

(1) In covering the electoral process, the media should maintain impartiality.

(2) Every candidate and political party shall respect the impartiality of the public media by undertaking to refrain from any act which may constrain or limit their electoral adversaries from using the facilities and resources of the public media to air their campaign messages.

63. Public media

(1) Election contestants shall have equitable and unimpeded access to public media for purposes of advertising and spreading their messages to the electorate before and during the campaign period.

(2) Political Party Broadcasts (PPBs) on public media shall be free to all competing political parties and candidates. Such broadcasts shall be made in equal coverage and at same time slots.

(3) Free airtime in (2) applies to PPBs only and the public media may still charge political parties for additional airtime required for adverts and propaganda.

64. Private media

(1) The State shall enact a law that affirms the existence of private media and regulates its operations in line with regional and international best practices.

(2) Candidates shall have unimpeded access to private radio, television and print media houses for purposes of advertising and spreading their messages to the electorate before and during the campaign period.

65. Prohibition of hate speech, bias and propaganda

(1) *Private and public media*

Private and public media shall not broadcast and publish abusive language, incitement of hate, and other forms of provocative language that may lead to bias,
discrimination or violence before, during and post-elections.

(2) *Social Media*

The use of social media to broadcast and publish hate speech and abusive language
that may lead to bias, discrimination or violence before, during and post-elections shall be prohibited.

66. Accreditation of media covering elections

(1) Media personnel covering elections and requiring access to election centres, polling stations and other facilities shall be accredited by the EMB as stipulated in the electoral law.

(2) Accreditation for access to polling and other election centres shall not be denied on the basis of perceived bias or any other discriminatory factor, provided that individuals and entities seeking such accreditation conform to a legally enforceable Code of Conduct.
(3) The Media Commission or an equivalent body responsible for accreditation of the media for operation in the country shall work together with the EMB, but the EMB may not override the decisions of the Media Commission or its equivalent on the status of a concerned media house or individual journalists.

67. Code of Conduct for media
(1) The Media Commission shall through a consultative process involving all stakeholders in elections:
(a) develop a Code of Conduct for the media, to which all media covering elections shall adhere to;
(b) be responsible for the enforcement of the Code of Conduct for media and shall work together with the EMB to enforce compliance with the Electoral Code of Conduct;
(c) develop means to monitor behaviour of public and private media during electoral campaigns.
(2) Both public and private media shall be subject to the Electoral Code of Conduct and the Code of Conduct developed and enforced by the body responsible for media regulation and monitoring in the country.
(3) The media Code of Conduct shall encourage fair reporting and prevention of hate speech.
(4) Codes of Conduct shall be compiled in a consultative and representative process.

However, one concern regarding this chapter is that hate speech, bias and propaganda are not defined – and, if the meaning of these broad terms is left open-ended in national laws, their prohibition could become an avenue for silencing views critical of the ruling party.

Additional provisions in this model law on security agents at polling stations give them a duty to protect the safety of members of the media as well as voters and election officials and observers. Security agents are also expected to act impartially and professionally, without bias or malice towards the media as well as candidates, political parties and voters, and must not "harass, intimidate or otherwise seek to control or influence" members of the media along with voters and election officials and observers.[92]

Another provision aims to secure media access to polling stations, with no restrictions on video and audio recording anywhere except in the voting booths.[93]

[92] *SADC Model Law on Elections, 2018*, section 76.
[93] Id, section 81.

CHAPTER 3

ANGOLA

CHAPTER 3: ANGOLA

ANGOLA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **125th globally; 38th out of 48 African countries** "Censorship and control of information still weigh heavily on Angolan journalists."
MALABO CONVENTION: party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Angola's 2010 Constitution (in English)

ARTICLE 40. FREEDOM OF EXPRESSION AND INFORMATION

1. Everyone shall have the right to freely express, publicise and share their ideas and opinions through words, images or any other medium, as well as the right and the freedom to inform others, to inform themselves and to be informed, without hindrance or discrimination.
2. The exercise of the rights and freedoms described in the previous point may not be obstructed or limited by any type or form of censorship.
3. Freedom of expression and information shall be restricted by the rights enjoyed by all to their good name, honour, reputation and likeness, the privacy of personal and family life, the protection afforded to children and young people, state secrecy, legal secrecy, professional secrecy and any other guarantees of these rights, under the terms regulated by law.
4. Anyone committing an infraction during the course of exercising freedom of expression and information shall be held liable for their actions, in disciplinary, civil and criminal terms, under the terms of the law.
5. Under the terms of the law, every individual and corporate body shall be assured the equal and effective right of reply, the right to make corrections, and the right to compensation for damages suffered.

ARTICLE 44. FREEDOM OF THE PRESS

1. Freedom of the press shall be guaranteed, and may not be subject to prior censorship, namely of a political, ideological or artistic nature.
2. The state shall ensure plural expression, imposing different ownerships and editorial diversity in the media.
3. The state shall ensure the existence and the independent and qualitatively competitive functioning of a public radio and television service.
4. The law shall establish the forms by which freedom of the press shall be exercised.

ARTICLE 57. RESTRICTION OF RIGHTS, FREEDOMS AND GUARANTEES
1. The law may only restrict rights, freedoms and guarantees in cases expressly prescribed in the Constitution and these restrictions must be limited to what is necessary, proportional and reasonable in a free and democratic society in order to safeguard other constitutionally protected rights and interests. 2. Laws restricting rights, freedoms and guarantees must be of a general and abstract nature and may not have a retroactive effect nor reduce the extent or scope of the essential content of constitutional precepts.
KEY LAWS: • Lei n.º 38/20: Código Penal Angolano • Lei n.º 7/17: Protecção das Redes e Sistemas Informáticos • Lei n.º 1/17: Lei de Imprensa • Lei n.º 5/17: Lei sobre o Estatuto do Jornalista
CRIMINAL DEFAMATION: Yes; frequently applied against journalists
DATA PROTECTION: Angola has a law on data protection, enacted in 2011.[94]
ACCESS TO INFORMATION: Angola has a law on access to information held by public authorities,[95] which has been criticised for being inadequate and not well-implemented in practice.[96]

3.1 CONTEXT

The Angolan media does not provide sufficient access to free, diverse, and impartial information. One problem is that Angola is reportedly the only southern African country without community radio stations, due to the prohibitively high license fees for local and community stations – although this issue was addressed by 2022 law reforms.[97] Another problem is that the state-sponsored media is allegedly biased toward the ruling party. For example, a representative of the Media Institute of Southern Africa (MISA) in Angola, stated that 90% of the airtime during the election campaign was dedicated to the ruling party.[98]

[94] **Lei n.º 22/11 de 17 de Junho**: Data Protection Law. A short overview is available in English here. In addition, **Lei n.º 23/11 de 20 de Junho**: Electronic Communications and Information Society Services Law contains specific data protection rules for personal data generated from electronic communications. See also **Decreto Presidencial n.º 214/2016 de 10 de Outubro**: Organic Statute of the Angolan Data Protection Agency. João Robles, "Doing Business in Angola: Overview", section 14, Thompson Reuters Practical Law, discussing law in force as of 1 October 2021.

[95] **Lei n.º 11/02 de 16 de Agosto**: Access to Documents held by Public Authorities, available in English here.

[96] "Africa Freedom of Information Centre Submission to the UN Universal Periodic Review", undated.

[97] "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022; **Lei n.º 17/22 de 6 de Julho** – Alteração da Lei de Imprensa (amends the Press Law (Law no. 1/17) and adds articles 2.ºA and 25.ºA); **Lei n.º 16/22 de 6 de Julho** – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão (amends the Law on the Exercise of Broadcasting Activity (**Law no. 4/17**), and adds Chapter IV-A with Articles 46A-46F).

[98] "Angola: Events of 2022", Human Rights Watch World Report 2023.

A) OVERVIEW

Five new media laws were promulgated in January 2017, six months prior to the presidential and parliamentary elections that took place that year, "introducing a regulating body and stringent controls on journalists, the internet, the press, radio and television broadcasting".[99] Observers asserted that the laws were very broad and ambiguous, which resulted in giving government officials broad discretion in their application.[100] One prominent Angola journalist stated that the aim of the laws was to "control and censor any attempt by political activists to use social media and the internet to blow the whistle on the most egregious examples of corruption, nepotism and the abuse of power". [101]

The five media-related laws contained in this "Social Communication Legislative Package of 2017" were the following: [102]

(1) Law no.1/17: **Press Law**[103]
This law establishes the general guiding principles of social communication and regulates the forms of exercise of freedom of the press.

(2) Law no. 2/17: Regulatory Entity of the Angolan Media[104]
This law establishes the attributions, competencies, composition, organization and operation of the Regulatory Entity of the Angolan Media **(ERCA**).

(3) Law no. 3/17: Exercise of Television Activity[105]
This law regulates television activity as well as audiovisual social communication.

(4) Law no. 4/17: Exercise of Broadcasting Activity[106]
This law regulates radio broadcasting.

(5) Law no. 5/17: Journalists' Statute.[107]

---

[99] Rui Verde, "The Death Knell for Freedom of the Press in Angola", Maka Angola, 8 February 2017.
[100] Id.
[101] D Quaresma Dos Santos, "Angola passes laws to crack down on press and social media", *The Guardian* via *Maka Angola,* part of the Guardian Africa Network, 19 August 2016.
[102] The text of all five laws in Portuguese can be found here. See also "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 24 and footnote 99.
[103] Lei n.º 1/17 de 23 de Janeiro: Lei de Imprensa, que estabelece os Princípios Gerais Orientadores da Comunicação Social e regula as Formas do Exercício da Liberdade de Imprensa. (Press Law, which establishes the General Guiding Principles of Social Communication and regulates the Forms of Exercise of Freedom of Press). This law repeals the 2006 Press Law (**Lei n.º 7/06**: Lei de Imprensa).
[104] Lei n.º 2/17 de 23 de Janeiro**:** Lei Orgânica da Entidade Reguladora da Comunicação Social Angolana, que estabelece as Atribuições, as Competências, a Composição, a Organização e o Funcionamento da Entidade Reguladora da Comunicação Social Angolana.
[105] Lei n.º 3/17 de 23 de Janeiro**:** Lei sobre o Exercício da Actividade de Televisão, que regula o Acesso e o Exercício da Actividade de Televisão, a Gestão e Exploração de Redes de Transporte e Difusão do Sinal Televisivo e a Prestação de Serviços de Comunicação Social Audiovisual em todo o Território Nacional.
[106] Lei n.º 4/17 de 23 de Janeiro**:** Lei sobre o Exercício da Actividade de Radiodifusão, que regula o Exercício da Actividade de Radiodifusão no Território.
[107] Lei n.º 5/17 de 23 de Janeiro**:** Lei sobre o Estatuto do Jornalista. This law revokes Decree no. 56/97.

Additional laws relevant to the communications sector include these: [108]

- **Law no. 23/11**: **Electronic Communications and Information Services**[109]
  This law provides foundational regulations for electronic communications and establishes the ***Autoridade das' Comunicações Electrónicas*** **(Electronic Communications Authority)**, a State body responsible for regulating and supervising the operation of electronic communications. It also aims to safeguard the right to security of information by enhancing the integrity, reliability and quality of information systems.[110] It also addresses critical infrastructure.[111]

- **Presidential Decree no. 202/11**: **Regulation on Information Technologies and Services** [112]

- **Presidential Decree no. 243/14**: **National Institute of Telecommunications INACOM**
  This law is the most recent authority for the establishment of the National Institute of Telecommunications (INACOM), the country's telecommunications regulator. Freedom House describes its roles as follows: "The MTTICS [Ministry of Telecommunications, Information Technologies, and Social Communication] is responsible for oversight of the ICT sector. INACOM, established in 1999, serves as the sector's regulatory body. In this capacity, it determines industry policies, sets prices for telecommunications services, and issues licenses. INACOM is, on paper, an independent public institution with both financial and administrative autonomy from the ministry. In practice, its autonomy is fairly limited. Its director general is appointed by the government and can be dismissed for any reason. In addition, the MTTICS can influence staff appointments. Other ministries often involve themselves in sector policy, leading to politically influenced regulatory decisions."[113]

[108] See "Data Protection and Cybersecurity Laws in Angola", CMS law firm, undated; An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-24.

[109] Lei n.º 23/11 de 20 de Junho: Das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (Electronic Communications and Information Society Services Law), described in "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-23.

[110] An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-23/

[111] Ferreira Manuel, "Angola precisa reforçar a aplicação das leis sobre cibersegurança nas instituições públicas", 14 de Abril, 2023: "De acordo com Alcides Miguel, que falava em representação do Banco Millennium Atlântico, há já em Angola leis importantes que regulam as principais preocupações relactivas à cibersegurança, entre as quais a Lei 7/17, relactiva à protecção e segurança das redes e a Lei 23/11, relactiva às infra-estruturas críticas. Entretanto, o observa, a aplicabilidade destas normas nos organismos públicos e a sua supervisão não é visível."
Translation: "According to Alcides Miguel, who was speaking on behalf of Banco Millennium Atlântico, there are already important laws in Angola that regulate the main concerns relating to cybersecurity, including Law 7/17, relating to the protection and security of networks, and Law 23 /11, concerning critical infrastructures. However, he observes, the applicability of these norms in public bodies and their supervision is not visible."

[112] Decreto Presidencial n.º 202/11 de 22 de Julho: Aprova o Regulamento das Tecnologias e dos Serviços da Sociedade da Informação.

[113] "Freedom on the Net 2022: Angola ", Freedom House, section A5 (footnotes omitted).

- **Presidential Decree no. 108/16**: **General Electronic Communications Regulation**[114]

- **Law no. 7/17**: **Protection of Networks and Information Systems**[115]
  This law aims to promote a safe and secure online environment, improve the provision of digital services, and promote citizens' access to information and knowledge. It also provides for international cooperation in preventing, investigating and prosecuting cybercrimes.[116] Some of its other procedural provisions on cybercrime are discussed below.

- **Law no. 27/17**: **Electronic Communications**
  This law establishes measures to secure electronic communications and transactions.[117] Ostensibly, the law aims to ensure that ICTs in Angola are developed to play a fundamental role in ensuring citizens' universal access to information, transparency in the public sector and participatory democracy. The law also sets broader goals of poverty alleviation, competitiveness, productivity, employment, and consumer rights. However, it is asserted this law enhances the government's ability to control the country's ICT sector; it contains a broadly worded clause allowing the head of government to "intervene" if internet service providers jeopardize "social functions" or "gravely compromise the rights of subscribers or users" (Article 26(2)).[118]

- **Law no. 38/20**: **Angolan Penal Code.**
  This law has a chapter on cybercrime, as well as several provisions that could restrict freedom of expression over-broadly These are discussed in more detail below.

In May 2022, the Angolan National Assembly (the only House in the country's unicameral Parliament) approved a **Law on Amendments to the Press Law,** a **Law on Radio Broadcast Activity** and a **Law on Opinion Polls and Surveys**. These laws made provision for community radio and provides for the inclusion of opinion polls in the Angolan legal system but prohibited the disclosure of opinion polls during the electoral campaign.[119]

---

[114] Decreto Presidencial nº 108/16 de 2 de Maio: Regulamento Geral das Comunicações Electrónicas (General Electronic Communications Regulation).
[115] Lei nº 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
[116] An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 23, which refers to this law as the "Computer Networks and Systems Protection Act, 2016"; "Freedom on the Net 2022: Angola ", Freedom House, section C6, which refers to the law as the "2017 Law on Protection of Information Networks and Systems".
[117] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 23.
[118] "Freedom on the Net 2022: Angola ", Freedom House, section A4.
[119] "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022. The three laws are:
- **Lei n.º 17/22 de 6 de Julho** – Alteração da Lei de Imprensa (amends the Press Law (**Law no. 1/17**) and adds articles 2A and 25A);

B) LAW NO. 1/17: PRESS LAW

This law[120] applies to various media, including newspapers, magazines, radio and television and online media.

Many things about this law look good on paper. It states that freedom of the press translates into the right to inform, and to be informed and must not be subject to any prior censorship of a political, ideological or artistic nature.[121] After noting that freedom of the press is guaranteed under the terms of the Constitution and the law, it also says that the exercise of freedom of the press must ensure broad and unbiased information, democratic pluralism, non-discrimination and respect for the public interest. It states furthermore that no citizen should be prejudiced in his private, social and professional life due to the legitimate exercise of the right to freedom of expression through the media.[122]

However, Article 7 provides for some broad limits on the exercise of freedom of the press:

- the need to safeguard the objectivity, accuracy and impartiality of information;
- protection for the right to a good name, honour and reputation, privacy of private and family life, the protection of children and youth, state secrecy, judicial secrecy and professional secrecy;
- defence of the public interest and democratic order;
- protection of public health and morality.

Article 7(2) states that freedom of the press does not cover the illicit production of information, explaining that this means that journalists cannot obtain information through illicit or unfair means. One analyst states that this "creates a grey area for Angolan journalists and allows the powers-that-be to go after both whistle-blowers and the journalists to whom they take any stories of malfeasance".[123]

Article 10 states that "All social communication media have the responsibility of assuring citizens' rights to inform and be informed in accordance with the public interest." [124]

- **Lei n.º 16/22 de 6 de Julho** – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão (amends the Law on the Exercise of Broadcasting Activity (**Law no. 4/17**), and adds Chapter IV-A with Articles 46A-46F);
- **Lei n.º 15/22 de 6 de Julho** – Aprovação da Lei das Sondagens e Inquéritos de Opinião (Opinion Polls and Surveys).

"Newsletter Julho-Agosto 2022", LegisPalop+TL. The texts of these laws are available on LEXLINK, which is a subscription service.

[120] Law no. 1/17, which establishes the General Guiding Principles of Social Communication and regulates the Forms of Exercise of Freedom of Press. It has been amended by **Lei n.º 17/22 de 6 de Julho.** "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022; "Newsletter Julho-Agosto 2022", LegisPalop+TL.

[121] Id, Article 5.

[122] Id, Article 6.

[123] Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017.

[124] Translation of this provision as in Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017. "Social communication" includes printed materials and telecommunications disseminated to the public (Article 2: definitions).

Article 11 lists what is in the public interest:

- contributing to consolidating the Angolan State, reinforcing national unity and identity and preserving territorial integrity
- informing the public truthfully, independently, objectively and impartially about all national and international events, ensuring the right of citizens to correct, impartial and impartial information;
- ensuring the free expression of public opinion
- contributing to the promotion of national and regional culture and the defence and dissemination of national languages
- promoting respect for the ethical and social values of the person and the family;
- Promoting good governance and the correct administration of public affairs
- Contributing to raising the population's socioeconomic level and awareness of citizenship.

The following topics of news and information are also in the public interest, according to Article 11:

- crimes, misdemeanours and other antisocial conduct
- issues concerning the protection of public health and the safety of citizens
- events in public spaces
- information provided or disclosed by the public authorities;
- information about administrative and judicial proceedings not subject to secrecy.

The limitations on the basis of public interest set a vague standard, despite the lists of what this entails. According to one source:

> *Article 11 goes on to make it clear that the public interest is whatever the organs of power define it to be. Article 84 defines the organs of power as the Ministerial Department responsible for Social Communication and in the final analysis, that department's boss, the President of the Republic. In effect, this grants the President and his appointee the legal powers to limit press freedoms, because he, or the Minister he appoints, has the power to determine what is, and what isn't, in the public interest. Would the President or his Minister consider it in the public interest to allow publication of a report on the alleged financial improprieties of senior figures in the MPLA [ruling party] regime? Doubtful."* [125]

Other critics also say these provisions effectively enable the government to control and censor critical information posted on social media or elsewhere online.[126]

The Press Law requires all journalists to operate in accordance with a Journalist Statute

[125] Rui Verde, "The Death Knell for Freedom of the Press in Angola", Maka Angola, 8 February 2017.
[126] "Freedom on the Net 2022: Angola ", Freedom House, section B3 (footnote omitted)

and Code of Ethics adopted by a national assembly of journalists convened by ERCA for this purpose. This Statute must provide a system for licensing journalists and issuing press cards.[127] The Journalism Statute was issued as **Law no. 5/17**, discussed below. The Press Law also requires foreign media and foreign press correspondents to request authorization and registration from the ministry responsible for social communication for activities in Angola.[128]

In addition to providing for the licensing of individual journalists, the Press Law provides requirements for the establishment and licensing of different forms of media outlets, including broadcasting, radio, social communication companies and news agencies, and sets out detailed rules regarding the right to reply.

News publications and television and radio broadcasters are required to publish with the utmost urgency and due emphasis, official statements from the President, the National Assembly and the Courts. Television and radio broadcasters are also obliged to broadcast live messages addressed to the Nation by the President.[129]

One positive point in this law is explicit protection for the confidentiality of sources. Article 20(1) states that it is lawful for journalists to refuse to reveal their sources of information and that their silence is not subject to any sanction.

C) LAW NO. 2/17: REGULATORY ENTITY OF THE ANGOLAN MEDIA (ERCA)

The Press Law states that the Angolan Media Regulatory Entity is an independent body whose mission is to ensure objectivity and impartiality of information and safeguard freedom of expression and thought in the press, in accordance with the rights enshrined in the Constitution and the law.[130] This companion law, which actually establishes ERCA, emphasises its "activities of regulation and supervision of the media in accordance with the provisions of the Constitution and the law".[131] Its jurisdiction includes television, radio, producers of periodical publications distributed by any means, news agencies and online media that distribute editorial content.[132]

The objectives of its regulation and supervision activities are to promote pluralism and diversity in the media; to guarantee free dissemination and free access to media content; to protect the most vulnerable social groups, such as children, against information content that may harm their development as citizens or jeopardize the preservation of socio-economic values, ethics and patriotism; to ensure that the content disseminated by the media is guided by strict criteria that correspond to good journalism practices; to guarantee effective editorial responsibility in case of violation

[127] Law no. 1/17, Article 21.
[128] Id, Article 22.
[129] Id, Article 16.
[130] Id, Article 8(1).
[131] Law no. 2/17, Article 2(2).
[132] Id, Article 7

of the law or media guidelines; and to ensure the protection of individual personality rights.[133]

The Board of ERCA is made up of 11 members who are elected by the National Assembly. The membership must be made up of five members of the ruling party, three members drawn from other political parties with representation in Parliament, one member of the executive branch of government and two members appointed by bodies representing the media profession.[134]

ERCA has broad investigatory powers. It can carry out investigations in any entity or place where activities in the field of Social Communication are carried out, and all public or private entities must provide access to information and documents requested by ERCA within 30 days. A court becomes involved only where an entity invokes commercial confidentiality as a basis for refusing to provide any documentation. ERCA is permitted to disclose the identity of companies or media bodies under investigation and the reason for the investigation whenever this is relevant for the regulation of the sector.[135]

ERCA also handles complaints about the media,[136] and administers the right to reply.[137]

Journalists and opposition political parties have criticized ERCA for being controlled by the ruling party and for issuing regulations that favour the government. [138] In 2021, one journalist views ERCA as window-dressing for a system where the relevant ministry continues to exercise the real regulatory power. This journalist, Reginaldo Silva, cited as an example the suspension of three television channels (ZAP Viva, Vida TV and Record TV Africa) by the ministry without ERCA involvement in April 2021.[139]

Observers have emphasised the potential intrusiveness of this law in respect of **persons who use the internet to criticise government, asserting that one of its purposes was to** ensure that web content would come under state control:

> *The new law creates a Regulatory Body with powers to regulate and supervise Angolan web content. It has the power to revoke, annul or suspend those websites whose content fails to obey the rigorous criteria of "good journalism", as determined by the Regulatory Body itself, which simultaneously has the power to "guarantee" editorial responsibility in the event that there is a violation of the law, or its self-defined "principles that inform social communication".*
>
> **[…]**
>
> *The law confers police-like powers on the Regulatory Body to pursue investigations in any place where (social) media activity may take place – that includes workplaces,*

[133] Id, Article 3.
[134] Id, Article 13.
[135] Id, Article 45.
[136] Id, Articles 48-50.
[137] Id, Article 51.
[138] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
[139] "Media regulation is 'undemocratic' and should be shared", *Lusa/Verangola*, 1 October 2021.

schools, peoples' own homes and any public spaces where a journalist may happen to be.
For example, Rafael Marques, the editor of Maka Angola, works from home with a laptop set up in his kitchen. Under the new law, anyone working for the Regulatory Body would have the right, without a warrant, to enter his home, go through his personal effects and seize or confiscate any item they might consider related to the production of his website.
In effect, the MPLA [Angola's ruling party] has created its own digital media police, governed by a Council of Directors chosen by MPLA deputies and the MPLA government. There can be no mistaking the intent of Angola's ruling party. With the departure of José Eduardo dos Santos from the Presidency after 38 years, the party cannot afford anything but a seamless transition of power to the next in line. Any information that might disrupt this can now, conveniently, be banned. It will be no surprise that the only information deemed to be legitimate and in the public interest will be information that serves the MPLA's interest first and foremost.[140]

D) LAW NO. 3/17: TELEVISION ACTIVITIES

This law regulates television and audiovisual social communication services,[141] with audiovisual works being defined to include films, documentaries, television series, television reports, educational, musical, artistic and cultural programs.[142] Generally, it provides more detail about licencing and the different categories of services that can be licenced.

Of particular interest to this discussion are the limits on television and audiovisual programming freedom. Programming cannot violate the dignity of the human person or any of the fundamental rights and freedoms. It must also not incite the commission of crimes, incite racial, religious, political, ethnic or xenophobic hatred, or discriminate on the grounds of gender, sexual orientation or disability. Other rules that apply to channels with unrestricted public access are to set limits (such as times of transmission, age classifications and warnings) in respect of pornography, gratuitous violence and other material that might negatively influence certain audience segments. [143] Audiovisual media services are also prohibited from assigning spaces for political propaganda (which is not defined in the law), without prejudice to the provisions of specific legislation on the right to broadcast, reply and political rebuttal.[144]

Licences can be suspended or revoked for infractions of the law and this power is explicitly given to "the Holder of Executive Power".[145]

[140] Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017.
[141] Law no. 3/17, Article 1.
[142] Id, Article 2(i).
[143] Id, Article 34. See also Article 35.
[144] Id, Article 36.
[145] Id, Article 82.

E) LAW NO. 4/17: RADIO BROADCASTING

This law[146] follows a similar approach to that of Law no. 3/17 on television activities. Here, limits on programming freedom restrict any material that violates the dignity of the human person, violates the fundamental rights, freedoms and guarantees of citizens or incites the commission of crimes, civil disobedience and social disorder as well as political propaganda.[147]

F) LAW NO 5/17: JOURNALISTS' STATUTE

This law[148] defines a "journalist" as someone who, as a permanent and remunerated occupation, carries out research, collection, selection and treatment of facts, news or opinions, through text, image or sound, intended for the dissemination of information by the Press, news agency, radio, television or electronic dissemination.[149] Journalists must have a degree in Journalism, Communication Sciences or Social Communication, or otherwise receive at least one semester of specialized training in journalism techniques at an institution accredited for this purpose.[150] A professional journalist must also complete a mandatory internship that lasts from six to twelve months.[151]

The authority to license and delicense journalists lies with the Portfolio and Ethics Commission, which also issues Certificates of Recognition to foreign journalists who wish to operate in Angola.[152] This Commission is composed entirely of journalists who are elected at a general meeting of journalists convened by ERCA.[153] As of October 2021, any media outlets that allowed a journalist to work without credentials faced a fine.[154]

Journalists' rights and duties are set out in this Statute, echoing the Press Law to a large extent. Some interesting additions to journalists' rights here are the right "not to be detained in the exercise of their professional activity, except under the terms of the law",[155] and "the right to access public places for the purpose of news coverage".[156] Journalists' duties are listed in Article 16:

---

[146] Law no. 4/17, as amended by **Lei n.º 16/22 de 6 de Julho** – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão.
[147] Id, Article 36.
[148] Law no. 5/17.
[149] Id, Article 2. Persons who carry out these activities without falling under the definition of journalists are termed "specialised collaborators". (The term translated as "specialised collaborator" in Portuguese is "colaborador especializado".)
[150] Id, Article 4. Specialised collaborators who work for media outlets are not subject to licensing, but must have an identification card issued by the media outlet. Id, Article 25.
[151] Id, Article 20.
[152] Id, Chapter III read with Article 30. This body has also been referred to in English as the "Ethics and Credentialing Commission". "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A. In Portuguese, it is the "Comissão da Carteira e Ética".
[153] Id, Article 31.
[154] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
[155] Id, Article 10(2)(a).
[156] Id, Article 11(1).

- to respect for professional ethics, and to report accurately, objectively, impartially and with respect for the adversarial principle
- to respect the editorial statute of the media organization which employs the journalist;
- to refrain from making accusations without evidence and to respect the presumption of innocence;
- not to identify, directly or indirectly, victims of crimes against freedom and sexual self-determination, or minors who have been subject to sanctioning guardianship measures; [157]
- not to discriminate against people on grounds of colour, race, religion, nationality, gender, sexual orientation or any other similar ground;
- to refrain from collecting statements or images that affect people's dignity;
- to respect privacy according to the nature of the situation;
- not to falsify or stage situations with the intention of abusing the good faith of the public;
- not to collect images and sounds using unauthorized means, unless the safety of the people involved and a relevant public interest justifies it.[158]

It is a professional disciplinary offence to violate any of these duties. Disciplinary proceedings are handled by the Portfolio and Ethics Commission. Possible sanctions include a warning, a fine, suspension or de-registration.[159]

The Portfolio and Ethics Commission also handles complaints from interested parties.[160]

As of June 2023, amendments to this law were under discussion which would allow individuals to serve as highly-placed political party officials and practice journalism at the same. The Union of Angolan Journalists (SJA) and MISA-Angola asserted that the amendments would undermine the impartiality of journalists, while the SJA alleged that this move would open doors to "promiscuity between journalism and party politics".[161] The proposed amendments have been withdrawn for the time being.[162]

3.2 CONSTITUTION

One key case in respect of freedom of expression concerned multiple charges against two journalists, **Rafael Marques de Morais and** Mariano Bras Lourenço for an article about the Attorney-General.[163] The news article at issue was published by

[157] This is, in Portuguese, "menores que tenham sido objecto de medidas tutelares sancionatórias".
[158] Law no. 5/17, Article 16.
[159] Id, Articles 42-43.
[160] Id, Article 39.
[161] Coque Mukuta, "Angola: Organizações de classe criticam propostas de alteração ao estatuto dos jornalistas e da ERCA", VOA, junho 15, 2023.
[162] Personal communication with Rui Verde, July 2023.
[163] "Angola: Judicial harassment of the award-winning investigative journalist, Mr. Rafael Marques de Morais", International Federation for Human Rights 12 July 2017. The charges were (1) "**outrage towards a sovereign body**" ("*ultraje ao órgão de*

Rafael Marques on the news website *Maka Angola* in 2016 and then republished with some alterations by Mariano Bras in the newspaper *O Crime*. Under the headline "Attorney-General involved in corruption", the article alleged that it was illegal for the Attorney General to act as a real estate developer in addition to his official duties and suggested that he had relied on the patronage of then-President dos Santos in respect of certain deals. On the charge of **defamation**, after a detailed examination of the articles, the Court concluded that "there is truth" in the matter that was reported upon, and that the two journalists had respected all the journalistic rules imposed on them, including seeking comment from the offended party prior to publication. The Court also found that the defendants had no intent to defame the victim, but only to publicize a situation that is in the public interest. It also considered that defamation involves the collision of two constitutional rights: the right to freedom of expression and information and the right to good name and honour, and that public figures expect to be exposed to more criticism than private figures. In this case, the topic was of obvious public interest, so the freedom of expression tipped the scales and the Court found no defamation.

> **In conclusion:** Freedom of expression constitutes one of the fundamental pillars of the democratic State and one of the fundamental conditions for its progress and, as well, for the development of each person. Politicians and other public figures, either because of their exposure, or because of the debatability ("*discutibilidade*") of the ideas they profess, or even because of the control to which they must be subject, either by the media or by the common citizen [...], must be more tolerant to criticisms than private individuals, including criticism of a greater degree of intensity.

In respect of **insult against public authority** and **abuse of press freedom**, the Court noted that insults must not be confused with impoliteness, lack of politeness or rudeness. On abuse of the freedom of the press, the Court noted that the press plays an important public function of providing information to the public on social, political, economic and cultural matters. It found the two journalists did not exceed the duty to inform the public objectively, remaining within the admissible limits of the right to information, and not fulfilling the criteria for insult or abuse of press freedom. On the charge of **outrage against the organ of sovereignty,** the Court found that objective criticism of the office does not equate to an injury to the personal honour of the President.[164]

Two cases involving freedom of expression in Angola have been taken to international forums to assert violations of the International Covenant on Civil and Political Rights (ICCPR), including violations of Article 19 on freedom of expression.

---

soberania" under Article 25(1) of the Law on Crimes against State Security and Article 105(1) of the Angola Constitution); (2) "**insult towards public authority** ("*injúrias contra autoridade pública*"), Article 181 of the previous Penal Code); (3) "**abuse of press freedom**" (Article 74(2) of the Press Law, Law No. 7/06); (5) **slander** (Article 7 of the previous Penal Code) and (6) **defamation** (Article 410 of the previous Penal Code). The Penal Code was revised in 2020, and Law No. 7/06 has been repealed.

[164] Processo n.592/17-B, Repûblica de Angola, Tribunal Provincial de Luanda, 6ª Seccâo da Sala dos Crimes Comuns.

In 1999, journalist **Rafael Marques de Morais** wrote several articles critical of Angolan President dos Santos in an independent Angolan newspaper, the *Agora,* alleging that the President was responsible for the destruction of the country and the calamitous situation of State institutions and was accountable for the promotion of incompetence, embezzlement and corruption as political and social values. He was arrested and initially detained without being informed of the reason, then charged with "materially and continuously committ[ing] the crimes characteristic of defamation and slander against His Excellency the President of the Republic and the Attorney General of the Republic". After a trial marked by several irregularities, he was convicted by the Provincial Court of **"abuse of the press"** under Law no 22/91 of June 15 (a previous Press Law)[165] and **criminal defamation** under a previous version of the Penal Code,[166] and sentenced to six months imprisonment along with a hefty fine and an order to pay compensatory damages to the offended persons. On appeal to the Supreme Court, the defamation conviction was overturned, but the Supreme Court upheld the conviction for abuse of the press on the basis of injury to the President. The Court found that the speech in question was not covered by the constitutional right to freedom of speech, since the exercise of that right was limited by other constitutionally recognized rights, such as honour and reputation, and "the respect that is due to the organs of sovereignty and to the symbols of the state, in this case the President of the Republic". The prison sentence was suspended, but the journalist was still required to pay a fine and compensatory damages.

Marques de Morais then submitted a **communication to the UN Human Rights Committee** alleging that the State had violated several provisions of the International Covenant on Civil and Political Rights (ICCPR), including Article 19 on freedom of expression. The Committee noted that any restriction on the freedom of expression must be proportional to the value which the restriction serves to protect. It found that, given the paramount importance of the right to freedom of expression and a free and uncensored press in a democratic society, the severity of the sanctions imposed could not be considered a proportionate measure to protect public order or the honour and the reputation of the President – who, as a public figure, is subject to criticism. The Committee thus found a violation of Article 19 of the ICCPR, amongst other articles. It found that Marques de Morais was entitled to an effective remedy, including compensation for his arbitrary arrest and detention, as well as for the violations of his rights under the ICCPR, and directed the State to take measures to prevent similar violations in the future [167]

The second case stemmed from an incident in 2015. In June 2015, **15 youth activists were arrested** without a warrant at a gathering in Luanda where they were discussing a book by Gene Sharp entitled "From Dictatorship to Democracy," and peaceful

[165] The crime of abuse of the press is defined in article 43 of the Press Law as "any act or behaviour that injures the juridical values and interests protected by the criminal code, effected by publication of texts or images through the press, radio broadcasts or television".

[166] Article 407 of the Penal Code describes the crime of defamation as publicly imputing to another person "something offensive to his honour and dignity".

[167] *Rafael Marques de Morais v Angola*, Communication No. 1128/2002, U.N. Doc. CCPR/C/83/D/1128/2002 (2005). This case is also summarised in the Malawi case of *Mbele v R*, Misc. Criminal Case No. 04 of 2022, High Court of Malawi, 20 June 2022.

ways to protest against President Dos Santos's 37-year reign. The meeting was led by **Domingos da Cruz**, an Angolan author, journalist and human rights activist. The 15 persons arrested included da Cruz and **Luaty Beirão**, a local rapper and political activist also known as "Ikonoklasta". Two other activists who did not attend the gathering were arrested later on, which led to the incident being referred to in the media as the "**15+2 case**".

All were charged with planning a rebellion and plotting a coup to overthrow the government. The public prosecutor later added a third charge of criminal association under Article 273 of the Penal Code In September 2015, a number of the activists went on hunger strike for a few days to protest their arrest; Luaty Beirão continued his hunger strike for 36 days and was admitted to the prison hospital in serious condition. Most were held in solitary confinement. While they were in custody, the case was considered by the **Working Group on Arbitrary Detention of the UN Human Rights Council**. This Group found that their situation violated a number of international human rights, including the rights to freedom of expression and peaceful assembly under the ICCPR, and called upon the government to release them, accord them an enforceable right to compensation and put an end to the unlawful criminal proceedings against them. The **U.N. Special Rapporteur on the situation of human rights defenders** urged the Angolan government to release the activists, to no avail.

The Provincial Court of Luanda found the activists guilty of **planning a rebellion** and **criminal association**. The criminal sanctions varied for the different defendants, ranging from two to eight years imprisonment. While their appeal to the Supreme Court was pending, they were released under a general amnesty law that had just been enacted.[168]

3.3 CASE STUDIES

According to Reporters without Borders in its 2023 World Press Freedom assessment, "Investigative reporting on subjects involving governance and the judicial system still often lead to prosecutions and sometimes heavy sentences". and "several journalists have been physically attacked or briefly arrested in recent years".[169]

The US State Department's 2022 Report on Human Rights Practices in Angola found "serious restrictions on free expression and the press, including violence, threats of violence or unjustified arrests against journalists, censorship, and enforcement or

[168] This account is based on the case summary of the Provincial court case, *Public Prosecutor v. Beirão, et al.* (15+2), by Global Freedom of Expression *here*; Ricardo Miguel Vieira, "Angolan Awakening: Ikonoklasta Doubles Down in his Fight for Change", *okayafrica*, [2017]; "'In Angola nobody is free,' activist Luaty Beirao tells DW", *Deutsche Welle,* 13 September 2016; "Opinion No. 21/2016 concerning Henrique Luaty da Silva Beirão, Manuel Chivonde, Nuno Álvaro Dala, Nelson Dibango Mendes dos Santos, Hitler Jessy Chivonde, Albano Evaristo Bingobingo, Sedrick Domingos de Carvalho, Fernando António Tomás, Arante Kivuvu Italiano Lopes, Benedito Jeremias, Inocêncio Antônio de Brito, José Gomes Hata, Osvaldo Sérgio Correia Caholo, and Domingos da Cruz (Angola)", Opinions adopted by the Working Group on Arbitrary Detention at its seventy-fifth session, 18-27 April 2016, UN Human Rights Council Working Group on Arbitrary Detention, A/HRC/WGAD/2016, 31 May 2016; "UN expert urges Angola to release fourteen rights activists detained for criticizing the Government", Press Release, UN Office of the High Commissioner on Human Rights, 23 October 2015.

[169] "2023 World Press Freedom Index: Angola", Freedom House, "Safety".

threat to enforce criminal libel laws".[170] It identified the main reasons for attacks against journalists to be reporting on corruption, poor governance, and human rights abuses, although some journalists reported being harassed by government authorities while covering peaceful demonstrations and election rallies. According to this report, civil society groups and individual political activists and journalists reported that Government monitored their activities and their social media, and used spyware to monitor their telephone conversations.[171] The report also states that journalists reported more incidents of violence, harassment, and intimidation in 2022 than in 2021, and that journalists practiced self-censorship for political and financial reasons.[172]

Freedom House gave this overview of Internet freedom in 2020-2021:

> *Internet freedom in Angola improved in the first years of the administration of President João Lourenço. A greater political focus on transparency and the fight against corruption has emboldened free speech. However, violence against protestors and journalists have recently contributed to self-censorship, reinstating an environment of fear that in the past limited public discussion of governance issues. Angolans are likelier to use social media platforms for the purposes of activism and community building than in the past. An ongoing economic crisis has affected the viability of some online media outlets. The government's perceived ability to monitor and intercept the data and communications of Angolan citizens is a major concern.*[173]
>
> *[…]*
>
> *While occasional arrests of protesters and online activists have muted digital activism and mobilization in the past, use of social media to mobilize support for various causes has become more common in recent years. Mobilization platforms are freely available to users, and citizens criticize the government and react to alleged wrongdoings within Angola's lively social media environment. Youth groups in particular have increasingly flocked to Facebook to call out government corruption, reflecting a gradual weakening of the environment of fear within civil society.*
>
> *Social media and messaging apps, like Facebook, Twitter, and WhatsApp, are frequently used to mobilize protests. Activists consider livestreaming and messaging as effective tools to record evidence of police brutality, as security forces often repress demonstrations with disproportionate force.* [174]

Reports of individual incidents provide some idea of what laws and other tactics are being applied against journalists in practice. Criminal defamation and laws against

[170] "2022 Country Reports on Human Rights Practices: Angola", US State Department, Executive Summary.
[171] Id, section 1F.
[172] Id, section 2A.
[173] "Freedom on the Net 2021: Angola", Freedom House, "Overview".
[174] "Freedom on the Net 2021: Angola", Freedom House, excerpt from section B8 (footnotes omitted),

insult appear to be the ones most commonly applied against the media.[175] Referring to criminal defamation, the US State Department's 2022 report on human rights practices in Angola stated:

> Several journalists in print media, radio, and political blogs faced libel and defamation lawsuits. Journalists complained the government used libel laws to limit their ability to report on corruption and nepotistic practices, while the government stated that some journalists abused their positions and published inaccurate stories regarding government officials without verifying the facts or providing the accused with the right of reply.[176]

A 2022 report discussed **criminal defamation** and **insult** charges filed by political figures against journalists Escrivão José, Óscar Constantino, and Fernando Caetano – with José reporting that 24 criminal defamation suits have been filed against him in relation to his work, most of which were unresolved and some of which had been closed without a formal prosecution.[177]

In another 2022 incident, a police official filed **criminal defamation** charges against *Rádio Ecclésia* reporters, José Kalembe and Diamantino Sangueve following a report about the official's alleged dealings in arms trafficking.[178]

In 2022, Nelson Dembo, a political activist who is also the co-host of a weekly current affairs show that airs on the YouTube and Facebook channels of *Camunda News*, was charged with various criminal offences, including **incitement to rebellion** and **outrage against the President.** Several staff members of *Camunda News* have been questioned by law enforcement officials since then, and state officials have demanded proof that the outlet is operating legally even though they maintain that there is no regulatory framework that applies to their online content. As a result of the intimidation, it was reported in March 2023 that the site has suspended its operations indefinitely.[179]

In January 2022, a political activist named Tanaice Neutro was arrested in Luanda for streaming a live video outside the prison hospital which protested the recent arrest of another activist at a political demonstration and the poor prison conditions in which he was being held. Neutro was convicted of "**insulting the state and its symbols**" and punished with a 15-month suspended sentence.[180]

---

[175] In addition to the examples summarised below, see "Angola charges 2 more journalists with criminal defamation over corruption reporting", Committee to Protect Journalists, 1 July 2021 and "Angolan editors questioned in separate criminal defamation investigations", Committee to Protect Journalists, 4 June 2021.
[176] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
[177] "Angolan journalists continue to face criminal insult and defamation proceedings", Committee to Protect Journalists, 30 June 2022.
[178] "Angolan journalists questioned in criminal defamation complaint over gun trafficking report", Committee to Protect Journalists, 16 March 2022.
[179] "Angolan outlet Camunda News suspends operations indefinitely after police harassment", Committee to Protect Journalists", 17 March 2023.
[180] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.

In April 2022 in Luanda, police arrested 22 people who were peacefully protesting the detention of political prisoners and calling for free and fair elections. Those detained included Laurinda Gouveia and her 6-month-old baby. Both mother and son were kept in a crowded cell without food or water for more than 48 hours. A judge in Luanda Provincial Court ordered the release of 20 of the 22 protesters for lack of evidence, but the other two were convicted of **civil disobedience** and ordered to pay the equivalent of $135 in fines.[181]

Carlos Alberto, editor of an investigative journalism website, *A Denúncia*, was convicted on charges of **criminal defamation** and "**abuse of press freedom**" in 2021, and sentenced to a fine of 110 million kwanzas (US$176,000) as well as two years in prison in connection with a story about a questionable land purchase by the deputy attorney general. He was told that the fine and the prison sentence would both be suspended if he published an apology every five days over a period of 45 days on his Facebook page and on *A Denúncia*. He refused to apologise and was reportedly appealing the case outcome, alleging that the charges were aimed at closing down the website because of its role in exposing corruption by top government officials.[182]

In February 2021, the editor of an independent paper, Mariano Brás, was questioned by police and **threatened with charges for writing an article critical of the President's performance**.[183]

Many other incidents involve police harassment of journalists rather than formal legal charges, or assaults and intimidation by members of the public:

- In October 2022, *Deutsche Welle* correspondent Borralho Ndomba was **detained** by police while covering a student demonstration in Luanda, after he refused to comply with a demand to stop filming and erase his footage. Police reportedly loaded him into a police van and **confiscated his cell phone and wallet**. He was released without charge after spending about an hour at a police station.[184]
- In August 2022, a correspondent for *Voice of America,* Coque Mukuta, was **detained by police** while filming a peaceful public demonstration in Luanda. He alleged that he was driven around in a police vehicle for three hours before being released without charge, and that **police confiscated his cell phone and professional credentials** (but later returned them).[185]
- In August 2022, *Deutsche Welle* submitted an official complaint to the Ministry of Social Communications, after one of its reporters was arbitrarily arrested and

[181] "Angola: Events of 2022", Human Rights Watch World Report 2023.
[182] "Angolan editor Carlos Alberto sentenced to fine, 2 years in prison over coverage of land deal", Committee to Protect Journalists, 17 September 2021.
"2023 World Press Freedom Index: Angola", Freedom House, "Safety".
[183] "Freedom on the Net 2021: Angola", Freedom House, section B4.
[184] "DW correspondent Borralho Ndomba harassed, briefly detained while covering student protest in Angola", Committee to Protect Journalists, 17 October 2022.
[185] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A; "VOA correspondent briefly detained covering attempted election protest in Angola", Committee to Protect Journalists, 17 August 2022; "Angola: Events of 2022", Human Rights Watch World Report 2023.

questioned for an hour by police officers in Malange, for filming proceedings at a voting station during elections.[186]

- In July 2022, **police used batons and sticks to break up a group of peaceful activists** protesting the detention of political prisoners in Luanda. Police also **detained** at least 10 persons, but released them without charge.[187]
- In April 2022, military and police officers reportedly surrounded journalists who were covering evictions and home demolitions in Luanda, allegedly **shoving them, hitting them with a baton and confiscating their equipment**.[188]
- In February 2022, a correspondent for *Deutsche Welle* in Cuanza Norte was brutally **assaulted by private security guards** of a major regional supermarket while investigating a case of food poisoning. The security guards also seized his equipment and that of two other journalists from *Rádio Ecclésia*.[189]
- In January 2022, six journalists working for news outlets *TV Zimbo* and *TV Palanca* were **assaulted by unidentified people** and forced to flee to safety while reporting on a nationwide strike by taxi drivers in Luanda. The secretary-general of the Journalists Union, Teixeira Cândido, told the Committee to Protect Journalists that public media journalists in Angola are increasingly becoming the targets of people's anger because of a perceived bias against the government and ruling party.[190]
- Reporters Without Borders reported in 2021 that an Angolan reporter for *Rádio Ecclésia*, Alfredo Kuito, was **badly bitten by a police dog** while covering a small civil society protest against the government in Ondjiva. The police had reportedly let loose dogs to disperse the protesters. The journalist required medical treatment for his injuries. [191]
- Reporters Without Borders also reported that at least seven journalists were harassed by police during a demonstration against corruption, unemployment and the postponement of local elections in Luanda, on 24 October 2020. Several persons were **detained without charge** and held for about 48 hours before being released – including Suely de Melo and Carlos Tomé of *Rádio Essencial;* and Santos Samuesseca, a photographer for the newspaper *Valor Económico*, along with driver Leonardo Faustino. Other journalists covering the demonstration were detained more briefly: Domingos Caiombo and Octávio Zoba of *TV Zimbo* and *AFP* photographer Osvaldo Silva were held for several hours, being released only after **being forced to delete photos and video footage** of the demonstration. Silva alleged that was **slapped, kicked and hit with batons by the police**. Another *AFP* photographer, Georges Nsimba, was briefly detained and also forced to delete his photos to secure his release. [192]
- Reporters Without Borders was also informed that an independent news website, Correio Angolense was the target of a **"cyber-attack"** in 2020, after

[186] Angola: Events of 2022", Human Rights Watch World Report 2023.
[187] "Angola: Events of 2022", Human Rights Watch World Report 2023.
[188] "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A; "Angolan security forces attack journalists covering evictions in Luanda", Committee to Protect Journalists, 3 May 2022.
[189] "Angola: Events of 2022", Human Rights Watch World Report 2023.
[190] "Angolan public media journalists assaulted, branded 'sellouts' while covering nationwide strike", Committee to Protect Journalists, 18 January 2022; Angola: Events of 2022", Human Rights Watch World Report 2023.
[191] "Angolan police unleash dog on reporter covering protest", Reporters Without Borders, 17 February 2021.
[192] "Crackdown on reporters covering Luanda demonstration", Reporters Without Borders, 28 October 2020; "Angolan police detain, harass, and beat journalists covering protests", Committee to Protect Journalists, 27 October 2020.

reporting on alleged embezzlement of public funds by the president's chief of staff. The *Correio Angolense* website was crashed by thousands of simultaneous connection attempts, which is not normal. Freelance journalist Siona Casimiro also reported a "cyber-attack" after working on the same story, but Reporters Without Borders provided no details as to what this attack entailed.[193]

- Four journalists were briefly **detained** during a protest against inflation and poor living conditions in November 2020.[194]

One investigative journalist who has been targeted repeatedly by the state is **Rafael Marques de Morais**, who is known for his articles denouncing corruption. **One case where he was acquitted of multiple criminal charges has already been discussed in the section above. He is**, moreover, the same journalist involved in the Human Rights Commission case discussed in the previous section of this chapter.

In 2011, the same journalist found himself in complex legal trouble following his publication of a book entitled *Blood Diamonds: Corruption and Torture in Angola,* which included details of human rights by security guards and soldiers in the diamond fields. He was sued for **civil defamation** by eight Angolan generals and two private mining companies, both in Angola and in Portugal, where the book was originally published. The case filed in Portugal was dismissed for lack of evidence. In Angola, Marques de Morais was then criminally charged with "**slanderous denunciation" under Article 245 of the Penal Code** in respect of the allegations in the book. He reached a settlement agreement with the generals, who agreed to dismiss the criminal complaint if he agreed not to republish the book and also stated in court that he did not intend to offend the generals by writing the book. Although Marques de Morais complied with the settlement agreement, the public prosecutors asserted that his statement before court was an admission of guilt that warranted a suspended prison sentence at the very least. In May 2015, he was convicted of **malicious prosecution** for intentionally submitting false evidence against the army generals, and given a sentenced to a six-month suspended sentence. The court also found him guilty of **criminal defamation** for filing criminal charges against these generals on the basis of the information contained in the book, and imposed a two-year suspended sentence for this crime.[195]

Another journalist who has been targeted repeatedly is **Felisberto da Grâça Campos**, a well-known independent journalist and editor of the weekly *Semanario Angolense*. He has reportedly been sued repeatedly by politicians. In 2007, he was fined 18.7 million kwanza (US$250,000) for **criminal defamation** as well as being sentenced to eight months in prison for allegedly **insulting a former minister**. This charge stemmed from articles published in April 2001 and March 2004 on alleged trafficking of

[193] "Cyber-attacks against Angolan news site and reporter", Reporters Without Borders, 9 October 2020.
[194] "Angolan police unleash dog on reporter covering protest", Reporters Without Borders, 17 February 2021. No further details about this incident were reported.
[195] "Angola: Judicial harassment of the award-winning investigative journalist, Mr. Rafael Marques de Morais", International Federation for Human Rights 12 July 2017; Kerry A Dolan, "Journalist Rafael Marques Given Two Year Suspended Sentence In Angolan Defamation Trial", *Forbes*, 28 May 2015; "The Case of Rafael Marques de Morais", Global Freedom of Expression, Columbia University, reporting on court decision of 28 May 2015.

influence. He also ran into legal troubles under press laws which are now no longer in force, after his 2003 publication of a list of "Angola's ten richest people" fuelled accusations of wrongdoing against some of the political figures on the list.[196]

3.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

Angola's legislation on cybercrime was previously concentrated in **Law no 7/17** on **Protection of Networks and Information Systems**, which deals primarily with procedural issues.[197] However, in 2020, this law was supplemented by provisions on cybercrime in Angola's 2020 **Penal Code**[198] and 2020 **Criminal Procedure Code**[199] covering both substantive and procedural issues. These recent provisions are based on the Budapest Convention.[200] It has been noted that there is still no culture of cybersecurity in organizations and government bodies in Angola, no cybersecurity regulatory authority and no dedicated legislation on this topic.[201]

A) CYBERCRIME PROVISIONS IN THE PENAL CODE

Cybercrimes are covered in Chapter III of the current Penal Code, entitled "Computer Crimes".[202] Note that this section was drafted with the assistance of online translation tools, as well as summaries of some provisions in English published by a law firm.[203] Also note that fines in the Penal Code are expressed as days, with each day corresponding to somewhere between 75 and 750 "Procedural Reference Units", as decided by the court on the basis of the convicted person's economic and financial situation.[204] Due to the difficulties of translation, what follows is a simple summary without attempts to analyse the precise wording or coverage of any of the provisions – but none of the technical provisions raise any immediate red flags.

[196] "Cyber-attacks against Angolan news site and reporter", Reporters Without Borders, 9 October 2020; "Newspaper editor freed provisionally pending outcome of appeal", Reporters Without Borders, 13 November 2007; "Angola: Prominent journalist sent to jail in libel case", Committee to Protect Journalists, 5 October 2007.
[197] Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
[198] Lei n.º 38/20 de 11 de Novembro: Código Penal Angolano (Angolan Penal Code).
[199] Lei n.º 39/20 de 11 de Novembro: Código do Processo Penal Angolano (Code of Criminal Procedure).
[200] "Angola: Cybercrime policies/strategies", Council of Europe, undated.
[201] "Data Protection and Cybersecurity Laws in Angola", CMS law firm, undated, section 4.
[202] See id, sections 3 and 6.
[203] Id.
[204] Article 47 of the Penal Code.

Penal Code

TITLE VIII
Computer Crimes

CHAPTER I
General Provisions

Article 437: Definitions. Definitions are provided for access code, traffic data, computer data. device, service provider, interception, semiconductor product, computer programme, electronic communications network, information system, and topography.

CHAPTER II
Crimes Against Computer Data

Article 438: Illegitimate access to information system and raid through information system
Unauthorized access to all or part of an information system is punishable by imprisonment for up to 2 years or a fine up to 240 days. If access is achieved by a breach of security rules or if it has been carried out in respect of a protected service, the penalty is from two to eight years' imprisonment. The same elevated penalty applies where the unauthorized access was used to procure industrial secrets, confidential data protected by law, or financial benefits. It is also an offence, without being duly authorized, to -

- carry out the computer processing of individually identifiable data or information;
- transmit data or information to third parties. for purposes other than those authorized; or
- create, maintain or use a computer file of personally identifiable data relating to political, religious, or philosophical convictions, party or trade union affiliation or the private life of others.

Article 439: Illegitimate interception in an information system. Whoever, by technical means, intercepts or records non-public transmissions of data processed within an information system, shall be punished by a prison sentence from two to eight years, or a fine up to 240 days.

Prison sentence from two years up to eight years, or the application of a fine up to 240 days.

Article 440: Damage to computer data. Whoever, with intent to cause damage to a third party or to obtain benefit for himself or for a third party, alters, deteriorates, renders useless, deletes, suppresses or destroys, in whole or in part, or in any way renders other people's data inaccessible, shall be punished by a prison sentence from one year up to 12 years, or the application of a fine up to 360 days, depending on the damage caused. "Data" for this purpose is any representation

of facts, information or concepts, including programs for computer, which is stored, transmitted or processed in an information system (Article 250(d)).

The same penalties apply to anyone who, with the intention of causing damage to a third party or obtaining benefit for himself or a third party, destroys, in whole or in part, renders useless, impedes, erases, alters, damages, hinders, impedes, interrupts or seriously disturbs the functioning of an information system or the ability to use an information system. The definition of an information system is not limited to computer systems, but also encompasses electronic communications and broadcasting, amongst other things (Article 250(d)).

CHAPTER III
Crimes Against Communications and IT Systems

Article 441: Computer sabotage. The following crimes against communications and information systems are punishable with prison sentence from two years to 240 days, or imprisonment for 2-8 years depending on the severity of damage and the nature of the system that was sabotaged:

- altering, damaging, interrupting or destroying, in whole or in part, an electronic communications network or computer system;
- seriously disrupting the functioning of an electronic communications network or IT system;
- affecting usability by introducing transmissions, damaging, altering, hindering, or preventing access or deletion of computer data, or in any other way interfering in an electronic communications network or computer system.

Article 442: Computer fraud. Whoever, with intent to deceive or harm, introduces, changes, deletes or suppresses data in an information system or, generally interferes with the processing of such data, in such a way as to produce false data that may be considered true and used as evidence commits an offence punishable with a prison sentence of up to two years or a fine of up to 240 days. It is also a crime for a person to use such false data with intent to cause harm to another or to obtain benefit for himself or for a third party, even if this person was not involved in creating the false data.

Article 443: Computer and communications fraud. The same penalties as for the crime of theft apply where someone causes material damage that causes a financial loss by certain forms of data interference, or by using programs, devices or other means to interfere with the normal operation or operation of telecommunications services, for the purpose of obtaining financial advantage for themselves or a third parties.

Article 444: Illegitimate reproduction of a computer program, databases and topography of semiconductor products. It is an offence to illegitimately reproduce or distribute a protected computer program, or make it available to the public – or to do the same actions, for commercial purposes, in respect of a creative database. It is an offence, without authorization, to extract or reuse a protected database, or to illegitimately reproduce, distribute, disseminate or make available to the public a topography of a semiconductor product. The Article also provides

COUNTRY CHAPTER: ANGOLA

for the seizure of items connected with these offences. Prison sentence from two years up to three years or the application of a fine from 240 days up to 360 days.

Angola President João Lourenço recently announced plans to open a cybersecurity academy to better secure the nation's telecommunications and IT networks. According to the Angolan Press Agency, the President added that efforts are underway to guarantee the security of the country's networks, with a focus on the protection and defence of critical infrastructure and vital information services. The academy is meant to support this effort.[205]

B) CYBERCRIME PROVISIONS IN LAW NO.7/17 ON PROTECTION OF INFORMATION SYSTEMS AND NETWORKS

This summary of the relevant provisions comes from a secondary source:

> *Law no. 7/17 of 16 February, the Legal Framework on Measures to Protect IT Networks and Systems, came into force on its publication date. As the name itself indicates, the aim of this legislation is to introduce rules to safeguard the cyberspace of the Republic of Angola by establishing sanctions for IT theft, cyber-attacks and IT incidents.*
>
> *The new legislation also governs measures to protect the cyberspace accessible to the public. These measures include security in cyberspace networks, critical infrastructures, encryption of electronic communications networks, response to incidents in cyberspace networks, electronic communication network security emergencies and security management in electronic communications networks. Security in cyberspace networks must ensure the integrity, confidentiality and privacy of communications by implementing the logical and physical security services established under the new rules.*
>
> *The legislation introduces measures to protect traffic and location data. These measures include expedited data retention, expedited retention of traffic and location data, and preservation of evidence.*[206]

Article 31 of this law provides that only telecommunications providers are free to import and use **encryption**. Article 32 provides that operators of publicly available electronic communications networks must retain **data where communications are not initiated or terminated on national territory**.[207]

[205] "Angola Marks Technology Advancements With Cybersecurity Academy Plans", *Dark Reading*, 15 June 2023.
[206] "Angola now has an IT Networks and Systems Protection Law", Gabinete Legal Angola, *News Lextter*, March 2017.
[207] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12; Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).

C) PENAL CODE PROVISIONS THAT COULD RESTRICT FREEDOM OF EXPRESSION

There are a number of content-based offences in the Penal Code that could inhibit freedom of expression – including some that appear to have been applied for this purpose in practice.

Note also that this section was drafted with the assistance of online translation tools, referenced against an English version of a preliminary draft of a previous version of the Penal Code[208] and a discussion of provisions of concern in the draft Penal Code by Amnesty International.[209] There may be additional problematic provisions in the Penal Code beyond the ones discussed here.

According to a secondary source, Angola's Penal Code contains two provisions that prohibit the **publication of false information**.[210]

Article 224, entitled "**abuse of press freedom**", prohibits the dissemination of information that incites secession, organised crime or racial, tribal, ethnic or religious hatred. It also criminalises engaging in a campaign to persecute or defame through the systematic and continuous dissemination of false information about the facts, attitudes, or professional, administrative or commercial performance of any person. In addition, it criminalises the intentional publication of false news in general. This provision has been applied against journalists in the last few years.

Article 322, which prohibits **propaganda against national defence and the armed forces.** This covers the dissemination of false or "distorted" true statements that might disturb the actions of the armed forces. Such publications are punishable whether they were published with the intention to hinder the armed forces or not, with different sanctions for intentional and unintentional acts. There is also provision for an enhanced penalty in a time of war.

ARTIGO 224.º
(Crime de abuso de liberdade de imprensa)

1. Comete o crime de abuso de liberdade de imprensa, punido com pena de prisão até 6 meses ou multa até 60 dias quem, por meio da comunicação social, proceder:
   - *a)* Ao incitamento à prática de crime ou a apologia de facto criminoso;
   - *b)* À divulgação de informações que incitem a secessão do país, a criação de grupos organizados de crime, ódio racial, tribal, étnico e religioso e a apologia às ideologias fascistas e racistas;
   - *c)* À promoção dolosa de campanha de perseguição e difamação, através da divulgação sistemática e contínua de informação falsa sobre factos, atitudes, desempenho profissional, admnistrativo, ou comercial de qualquer pessoa;
   - *d)* À divulgação de textos, imagens ou som, obtidos por meio fraudulento;
   - *e)* À publicação intencional de notícias falsas.
2. A retractação ou a publicação de resposta, se aceite pelo ofendido, isenta de pena o autor ou autores do escrito, som ou imagem.

[208] Preliminary Draft of the Penal Code, undated.
[209] "Angola: Provisions of the 'Draft Criminal Code' are Incompatible with Angola's Human Rights Obligations", Amnesty International, 2012.
[210] "LEXOTA Country Analysis: Angola", last updated July 2022.

It has been observed that both provisions are vague, with no direction on how to determine truth or falsity. It is also stated that these offences can be punished by sanctions that could be disproportionate. Thus, there is a concern that these provisions could unreasonably inhibit freedom of expression.[211]

Another article of concern, Article 333, prohibits **"outrage to the State, its symbols and organs"**. This provision makes it an offence to outrage, by words, images, writings, drawings or sounds, the Republic of Angola, the President of the Republic or any other Organ of Sovereignty publicly, with intent to offend. The punishment is imprisonment from 6 months to 3 years or a fine of 60 to 360 days. Where the object of the outrage is the flag, the insignia or the anthem of the Republic, the penalty is imprisonment for up to 2 years or a fine of up to 240 days. It has been pointed out that this provision could be used, for instance, against political cartoonists.[212] It has been utilised in recent years, as the case studies in this chapter illustrate.

ARTIGO 333.º
(Ultraje ao Estado, seus símbolos e órgãos)

1. Quem, publicamente, e com intuito de ofender, ultrajar por palavras, imagens, escritos, desenhos ou sons, a República de Angola, o Presidente da República ou qualquer outro Órgão de Soberania é punido com pena de prisão de 6 meses a 3 anos ou multa de 60 a 360 dias.
2. Se o ultraje tiver por objecto a bandeira, a insignia ou o hino da República, a pena é de prisão até 2 anos ou de multa até 240 dias.

Article 380 covers **incitement to discrimination**. It is an offence, in a meeting or a public place or through any means of dissemination or communication with the public, to incite hatred against a person or group of people on the grounds of race, color, ethnicity, place of birth, gender, sexual orientation, physical or mental disability, religious belief, political or ideological convictions, social status or origin or other basis, for the purpose of discrimination against such persons or groups. The punishment is imprisonment from 6 months to 6 years. It is also an offence to incite violence on these grounds, subject to the same penalty. Doing these acts through an information system attracts a penalty of imprisonment for 1 to 6 years. It is an even more serious offence to found, direct, join, finance, support or participate in the activities of an organization established to incite discrimination on such grounds, or one that reiterates and publicly incites discrimination, hatred and violence on such grounds. Article 381 prohibits incitement to **genocide**.

There is an entire chapter of the Penal Code on crimes against the dignity of the person, which includes injuria, defamation, slander and offence to the memory of a deceased person – which are all different shades of **criminal defamation**.

[211] Id.
[212] "Article of the new Penal Code threatens freedom of expression, lawyers consider", *Lusa/Verangola*, 17 November 2020.

D) STATE SURVEILLANCE

This topic is summarised by Freedom House as follows:

> *The government's ability to monitor and intercept the data and communications of Angolan citizens without adequate oversight is a major concern, particularly among human rights activists and journalists. The full extent of the government's surveillance capabilities and practices is unknown, though developments in the coverage period suggest that the government plans to expand its surveillance capacity.*
> *[…]*
> *In June 2020, reports emerged that Angolan intelligence services had purchased Pegasus spyware, which allows users to compromise devices and monitor communications, from the Israeli technology company NSO Group. Pegasus was known to have abused vulnerabilities in WhatsApp, the dominant messaging app in Angola that is widely used by journalists, activists and opposition politicians. A 2018 Haaretz investigation found that an unnamed Israeli company had sold social media monitoring software to the Angolan government.*

> *In December 2019, the government opened the Integrated Center for Public Security (CISP), a surveillance data integration center operated by state security forces, in Luanda. That facility is the first of 16 planned centers to be built around the country. The initiative is backed by Chinese funding along with technology from Huawei. In November 2020, the head of the External Intelligence Services and Military Information Services informed members of Parliament that the government intends to construct centers to detect cybercrimes.*

> *A law that permits law enforcement to conduct electronic surveillance and location tracking with minimal oversight came into force in May 2020. [Law no. 11/20 of the 23rd of April] The law authorizes the public prosecutor's office, the National Police, and judges to order and deploy surveillance technology, including spyware and telecommunications interception, in a broad range of circumstances. It prohibits surveillance on political grounds or on the basis of a discriminatory motivation. Though it is not yet clear how the law has been applied, Angolans worry it provides legal coverage for existing surveillance practices, with little or no competent oversight of security forces' use of invasive technology.*[213]

"In Angola, the law on video surveillance No. 2 of 22 January 2020 provides for the installation of *video surveillance* systems by state security forces to maintain public safety. Article 29 obliges all persons with CCTV systems to provide recordings when requested by the **Data Protection Agency (DPA)**, and mandates the Agency to impose sanctions and penalties, including for infractions related to the operation of CCTV systems. According to Freedom House:

[213] "Freedom on the Net 2022: Angola", Freedom House, section C5 (footnotes omitted).

A law that came into effect in January 2020 allows for the installation of surveillance cameras by state security forces without prior authorization. Security agencies are exempted from many of the law's safeguards, raising concerns that the law will expand the government's surveillance authority, including its capacity to integrate offline and online surveillance through the CISP. The CISP in Luanda, which is reportedly connected to over 700 cameras installed around the city, is equipped with facial recognition technology.[214]

Law no. 2/20 on Video Surveillance[215] allows for the installation of surveillance cameras by state security forces without prior authorization. Article 29 obliges all persons with CCTV systems to provide recordings when requested by the Data Protection Agency (DPA). "Security agencies are exempted from many of the law's safeguards, raising concerns that the law will expand the government's surveillance authority, including its capacity to integrate offline and online surveillance through the CISP. The CISP in Luanda, which is reportedly connected to over 700 cameras installed around the city, is equipped with facial recognition technology." [216]

Law no. 7/17 on Protection of Networks and Information Systems[217] mandates that telecommunications operators store traffic and location data for the "investigation, detection and repression of crimes". Article 37 requires the approval of a magistrate for the interception of communications by Angola's security services. Article 22 requires service providers to allow the Prosecutor General or a magistrate to access data, including location data, where this is considered "evidence." Article 23 requires telecommunications operators to store all data for at least one year.[218]

E) SIM CARD REGISTRATION

SIM card registration is mandatory, which hampers the ability of mobile phone users to communicate anonymously. SIM cards must be registered directly with the National Institute of Telecommunications (INACOM), which is the country's ICT regulator that operates under government oversight. The process requires an identity card or driver's license and tax card for national citizens, or a passport with a valid visa for visitors.[219]

The authorising law – **Law no. 11/20 (Identification and Location of Cellular Phones and Electronic Surveillance carried out by Police Authorities)** – justifies this with objectives that include prevention and prosecution of crime; location of a cellular signal of a device owned or presumed to be owned by a missing person who is a victim or a

[214] Id.
[215] Lei n.º 2/20 de 22 de Janeiro: Da Videovigilância (Videosurveillance).
[216] "Freedom on the Net 2022: Angola ", Freedom House, section C5 (footnotes omitted); see also "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12; "Angola: Regulation of the Video-Surveillance Law", PLMJ, 4 January 2022.
[217] Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
[218] "Freedom on the Net 2022: Angola ", Freedom House, section C6.
[219] Id, section C4.

perpetrator of crime; and obtaining relevant data or information for criminal investigation of perpetrators of crime through their surveillance.[220]

> *Article 8 provides that interception, monitoring or surveillance through the deployment of surveillance technology, including spyware and telecommunications interception, can be carried out by the National Police, and is authorised by the Public Prosecutor's Office or judges through a written surveillance order (article 20). The law does not stipulate the duration of the surveillance order. However, the law requires that investigators report to judicial authorities the results of the surveillance once it is over. Also, the law prohibits surveillance on political grounds or based on discriminatory motivation, which terms are not defined. Further, surveillance must be done in coordination with the DPA [Data Protection Agency] which must submit an annual report on its overall activities to the National Assembly. However, this has not happened since the Authority's establishment in 2016. Under article 12, cellular identification or tracking and electronic surveillance may be carried out by the following means: software for locating and accessing telephone and telematics registration and signals, computer applications and platforms for monitoring cellular signals; video surveillance cameras and audio surveillance equipment, installed in fixed locations; equipment for locating and intercepting telephone communication; and radio listening equipment.*

There are concerns that, given insufficient safeguards against misuse of surveillance powers by state agents, the law will expand state surveillance activity, even as offline and online surveillance are integrated through the Integrated Public Security Centre (CISP). The CISP in the capital Luanda is reportedly connected to over 719 cameras in the city, whose capabilities include vehicle tracking, facial recognition, and infrastructure monitoring.

F) TAKE-DOWN NOTIFICATIONS

Angola has a take-down notification procedure in its **Digital Millennium Copyright Act**. Freedom House reports:

> *In August 202, an article by the anticorruption website Maka Angola was targeted by a fraudulent content-removal request. The article in question covered corruption in the dos Santos family and had been published by Maka Angola in 2018. The digital media foundation Qurium, which provides web-hosting services to Maka Angola, reported receiving a notice under the Digital Millennium Copyright Act (DMCA) that purported to be from the Portuguese news portal Esquerda.net, which had re-posted the Maka Angola article; the impersonator claimed that Maka Angola had copied the article from its site and was thus committing a copyright violation. Qurium did not comply with the notice.*[221]

[220] Lei n.º 11/20 de 23 de Abril: Da Identifição ou Localização Celular e da Vigilância Electrónica (Cellular Identification or Location and Electronic Surveillance), Article 3; "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12.
[221] "Freedom on the Net 2022: Angola ", Freedom House, section B2.

CHAPTER 4

BOTSWANA

CHAPTER 4: BOTSWANA

BOTSWANA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **65th globally; 11th out of 48 African countries** "Botswana has seen a decline in the most serious abuses against journalists in recent years but many obstacles still hinder their work."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Botswana's 1966 Constitution with amendments through 2016 **ARTICLE 12. PROTECTION OF FREEDOM OF EXPRESSION** 1. Except with his or her own consent, no person shall be hindered in the enjoyment of his or her freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his or her correspondence. 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision — a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; or b. that is reasonably required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, regulating educational institutions in the interests of persons receiving instruction therein, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless, broadcasting or television; or c. that imposes restrictions upon public officers, employees of local government bodies, or teachers, d. and except so far as that provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society.
KEY LAWS: • Cybercrime and Computer Related Crimes Act 18 of 2018 • Penal Code [*Chapter 08:01*] (selected provisions), as amended by the Penal Code (Amendment) Act 21 of 2018 • Communications Regulatory Authority Act 19 of 2012

• Criminal Procedure and Evidence (Controlled Investigations) Act, 2022
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: Botswana has a data protection law[222] which has not yet come into force.[223]
ACCESS TO INFORMATION: Botswana has no access to information law.

4.1 CONTEXT

Botswana will be having general and presidential elections in October 2024. The country has a relatively vibrant media landscape, populated by a variety of print, broadcast and online media.

However, based on what sources have said, the media landscape has deteriorated, and the mainstream media and journalists have largely lost credibility and public trust over especially the last decade or so, as media capture by politically associated interests and political bias have increasingly become notable features of the landscape.

Newspapers are required to register under the Printed Publications Act 15 of 1968. The definition of "newspaper" is very broad, covering "any publication containing news, intelligence, reports of occurrences, or any remarks, observations or comments on such news or on any other matters of public interest or of a political nature in relation to Botswana, which is printed or published for sale or free distribution at regular or irregular intervals within Botswana". The relevant minister has the power to extend the registration requirement to newspapers printed outside Botswana which are intended primarily for circulation inside Botswana – or are, in fact, so circulated. It is an offence to publish an unregistered newspaper. In addition, all "publications" (any document produced by any means of reproduction) must display the names and addresses of the printer and publisher and the year of publication. Violation of this rule is also an offence. Newspapers or publications that do not comply with the Act can be seized by police without a warrant (although a warrant issued by a magistrate is required to search premises for such documents) [224] It appears that this law is not vigorously enforced.[225]

[222] Data Protection Act 32 of 2018.
[223] Sarah Buerger, "Botswana's Data Protection Act grace period extended", Michaelson's, 30 October 2022. Amendments are being considered. Andrew Maramwidze, "Back to the drawing board … glaring gaps in Botswana's Data Protection Act", IT web, 24 June 2022.
[224] Printed Publications Act 15 of 1968. This is the original law; there may have been amendments since 1968 that are not reflected here. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 121-123.
[225] See, for example, Thapelo Ndlovu and Jacqueline Kabeta, "Media Sustainability Index 2008: Botswana", IREX, page 16.

Films are regulated by the Cinematograph Act 73 of 1970, which is currently under review.[226] Under the current law, it is an offence to make a film in Botswana without a filming permit issued by the relevant minister, unless the minister has provided an exemption for a particular film or class of films. The law also places some restrictions on the exhibition of films.[227]

Broadcasting is subject to the Broadcasting Act 6 of 1999, which establishes a National Broadcasting Board appointed by the relevant minister.[228] The Board, amongst other things, issues radio and television broadcasting licences and controls and supervises broadcasting activities.[229] The Broadcasting Regulations, 2004 issued this Act cover issues such as adhering to community standards; the duty of accurate, fair and impartial reporting; correction of broadcast errors and guidelines for reporting on "controversial issues".[230] There is also a Broadcasters' Code of Practice (2018) that reiterates some of the issues in the Broadcasting Regulations, 2004 and provides additional detail on broadcasting during election periods.[231]

The telecommunication, broadcasting and postal sectors are regulated under the **Communications Regulatory Authority Act 19 of 2012** which establishes the **Botswana Communications Regulatory Authority (BOCRA)**.[232] The long title of the Act states that it creates an "independent regulatory authority", but there is no reference to the authority's independence in the law's text, and the relevant minister appoints members of BOCRA and has a general power to issue regulations under the law.[233] Although radio and television broadcasting licences continue to be issued under the Broadcasting Act 6 of 1999 by the National Broadcasting Board, BOCRA is responsible for issuing licences for service providers in the other sectors it covers as well as the administration of domain names.[234]

The media in Botswana are soon to be regulated by the **Media Practitioners Association Act, 2022** (passed by Parliament but still to be brought into force as of mid-2023).[235] This law is generally considered to be an improvement on its predecessor, the Media Practitioners' Act, 2008,[236] which was never fully implemented

[226] Cedric Swanka, "Botswana Reviews Cinematography Act to Boost Creative Economy", *Sunday Standard*, 2 September 2019; Esther Mmolai, "Collaborations Boost Film Production", *Daily News*, 13 June 2023.
[227] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 123-124. The text of the law is available here, but only to subscribers.
[228] Broadcasting Act [*Chapter 72:04*], section 5.
[229] Id, section 10(1).
[230] Broadcasting Regulations, 2004
[231] Broadcasters' Code of Practice.
[232] Communications Regulatory Authority Act 19 of 2012.
[233] Id, sections 4 and 94. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 138-139.
[234] The Act defines the "regulated sector" as "any sphere of activity within the telecommunications, broadcasting and postal service sectors which includes the installation of telecommunications networks; the installation and operation of radiocommunication equipment; the provision of postal services; the converging of electronic technologies and *the provision of internet services*" (emphasis added). "Regulated supplier" is accordingly defined as any supplier of goods or services in the regulated sectors whose activities fall within the scope to be regulated by the Authority". Communications Regulatory Authority Act 19 of 2012, section 2.
[235] Media Practitioners Association Act, 2022, on file with authors.
[236] Media Practitioners Act 29 of 2008.

in practice.[237] According to the statement of the Minister for the State President in Parliament, the operation of the 2008 Act was -

> *frustrated by the resistance from the media fraternity, who view the law as draconian and counter [to] the democratic values of Botswana. The contention being that the law interferes with media freedom. A decision was made to repeal and re-enact, with amendments, the Act with a view to improve media's relations with Government and Botswana's standing in the global press freedom index. To that end, extensive consultations were done with the media fraternity and educational institutions to come up with a law best suited for Botswana.*[238]

The new law provides for an independent Media Practitioners' Association made up of media representatives, The law explicitly makes the Association independent and separate from the government and mandates it to operate without any "political interference, bias or influence".[239] The affairs of the Association are to be governed by an Executive Director and a Media Practitioners' Board chosen by the Association and structured so as to be representative of the key media stakeholders.[240] The Association also selects an Ethics and Conduct Committee to develop a Code of Ethics for the media profession, upon approval by the Association,[241] and a Complaints and Disciplinary Committee responsible for mediating and adjudicating disputes between government and media enterprises, between the public media enterprises, between a journalist and the public or any other person, or between different media enterprises.

The law provides three requirements for registration as a journalist by a professional body operating in the media sector: (1) the journalist must be an employee of a media enterprise which is recognised by the relevant professional body as "furnishing a sufficient guarantee of the required academic knowledge of, and practical experience in, journalism"; (2) the journalist must have taken an oath to uphold the Code of Ethics; and (3) the journalist must be, in the opinion of the professional body, a "fit and proper person to be registered as a journalist".[242] There are also provisions for removal of names from the register of journalists.[243] The law requires that a media enterprise that publishes news in newspapers or magazines, via radio and television broadcasts, or by "any other electronic means" must indicate the full names of the responsible journalist.[244]

---

[237] "Press Freedom in Botswana 2022", International Press Institute, February 2023 (based on information gathered during a mission to Botswana in August 2022), page 8; "US State Department Human Rights Reports, Custom Report Excerpts: Botswana", section 2A, 2020.
[238] "Statement for Second Reading Media Practitioners' Association Bill, 2002, Bill No 8 of 2022 before Parliament by Honourable Minister for State President Kabo N.S. Morwaeng", paragraph 3.
[239] Media Practitioners Association Act, 2022, sections 6-7.
[240] Id, Parts III and IV.
[241] Id, Part IX.
[242] Id, section 37(1).
[243] Id, section 38.
[244] Id, section 44.

The government describes this Act as being aimed at promoting the freedom and independence of the media by minimising government involvement.[245] According to the International Press Institute, the new law establishes a regulatory body with members from the media community and civil society which, although "not purely self-regulatory", does appear to reduce the scope for government interference.[246]

The Media Institute of Southern Africa (MISA) has welcomed the independence of the Media Practitioners' Association, but cautions that safeguards might be needed for the realisation of this objective in practice and particularly to ensure that the Executive does not play any role in the appointment or dismissal of persons from any of the Association's structures and committees.247 MISA objects to the fact that the law gives the Association a duty to ensure that national security, public order and public health are safeguarded in accordance with the applicable laws – noting that this task could lead to conflicts of interest since the listed issues are sometimes used as a basis for restricting access to information and media freedom.[248]

Concerns have also been raised regarding the law's approach to the registration of journalists, which appears to be unduly limited. The law is unclear on the implications arising from being unregistered, but concerns have been raised that government and others might refuse to deal with those who are unregistered, which could mitigate against non-traditional journalists, community media, bloggers and others working outside major media outlets.[249]

Making a counter argument, University of Botswana law professor, Tachilisa Balule, noted that there has been a marked decline in journalistic ethics and professional standards across the media landscape, and that this was what contributed to the government coming forward with a statutorily imposed registration system. Balule is of the opinion that the mainstream media had an opportunity before 2008, and even after, to come up with an effective self-regulatory system but had failed to do so.[250]

A 2022 report by the UN Special Rapporteur notes that the practice of journalism is no longer limited to those employed by news publishers, but is shared by a wide range of actors, including those who engage in self-publication on the Internet, recommending that while it is permissible for limited accreditation and registration schemes to facilitate privileged access for journalists to certain places or events, "general State systems of registration or licensing of journalists are incompatible with international human rights law".[251]

[245] Memorandum to the Media Practitioners' Association Bill, Bill No. 8 of 2022 (on file with the authors).
[246] "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 8.
[247] "Analysis of the Botswana Media Practitioners' Association Bill, 2022", MISA, page 3.
[248] Id.
[249] Id, pages 3-4; "Press Freedom in Botswana 2022", International Press Institute, February 2023, pages 8-9; Anton Harber, "Botswana Media Practitioner Act is a threat to freedom of the media", *Daily Maverick*, 28 September 2022.
[250] Professor Tachilisa Balule was interviewed via Zoom on 13 July 2023.
[251] "Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022, paragraph 15.

Another criticism of the new law is its rule that all articles must identify the responsible journalist, thus prohibiting anonymity that could protect persons who fear threats on the basis of their articles.[252]

4.2 CONSTITUTION

It has been noted that section 12(2) of the Botswana Constitution authorises broad grounds for restrictions to freedom of expression on the basis of defence, public security, public order, public morality and public health. It is consistent with international human rights standards to provide for limitations to freedom of expression as long as these are necessary, proportionate and established by law. However, concerns have been raised that restrictions based on "public order" might be interpreted in a broad way that inhibits media freedom and whistleblowing.[253] On the other hand, the Botswana Constitution also requires that any limitations imposed must be "reasonably justifiable in a democratic society", which provides scope for courts to ensure that the government does not abuse the opportunity for limiting the right to freedom of expression.[254]

In 2001, in the *Media Publishing* case, the High Court relied on the constitutional guarantees of freedom of expression in a **case where the government withdrew advertising from media outlets that had published unfavourable commentary**. The Court found that it was not permissible for Government to take away benefits in response to the exercise of a constitutional right.[255]

In a 2006 **civil defamation case**, the High Court emphasised that "freedom of expression is not only applicable to dissemination of information and ideas that are favourably received, but to those that offend, shock or disturb the state or any sector of the population. Such, it has been said are the dictates of pluralism, tolerance and broad-mindedness, without which there is no democratic society".[256]

Legitimate restrictions on freedom of expression were discussed in a 2010 decision of the African Commission on Human and People's Rights, *Good v Republic of Botswana*.[257] This case was decided with reference to the African Charter rather than the Constitution of Botswana, but the principles are the same. In this case, an Australian academic teaching at the University of Botswana co-authored a newspaper article that criticised political succession in Botswana – and soon found himself expelled from the country. The Government cited national security concerns in its submission to the Commission,[258] but the Commission disagreed:

---

[252] Anton Harber, "Botswana Media Practitioner Act is a threat to freedom of the media", *Daily Maverick*, 28 September 2022
[253] "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 7.
[254] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 109-110.
[255] *Media Publishing (Pty) Ltd v The Attorney-General and Another* 2001 (2) BLR 485 (HC), summarised and analysed by Global Freedom of Expression here.
[256] *Odong Ocaya v Francistowner (Pty) Ltd t/a The Voice Newspaper and Others* (2464 OF 2004) [2008] BWHC 268 (21 August 2008), paragraph 89.
[257] *Good v Republic of Botswana* (2010) AHRLR 43 (ACHPR 2010), summarised and analysed by Global Freedom of Expression here.
[258] Id, paragraphs 59, 118, 120 and 146.

> *In the opinion of the Commission the article that was published by the victim is a purely academic work which criticises the political system, particularly presidential succession in Botswana. There is nothing in the article that has the potential to cause instability, unrest or any kind of violence in the country. It is not defamatory, disparaging or inflammatory. The opinions and views expressed in the article are just critical comments that are expected from an academician of the field; but even if the government, for one reason or another, considers the comments to be offensive, they are the type that can and should be tolerated. In an open and democratic society like Botswana, dissenting views must be allowed to flourish, even if they emanate from non-nationals.*[259]

The Commission concluded on this point that the article in question posed no national security threat and that the punitive expulsion of the author for his expression of views was "unnecessary, disproportionate and incompatible with the practices of democratic societies".[260] The Commission also noted that a higher degree of tolerance is expected for political speech and an even higher threshold is required for speech directed towards the government and government officials – noting that politicians are expected to endure stronger public criticisms than private citizens.[261]

4.3 CASE STUDIES

According to the 2023 World Press Freedom report, journalists in Botswana are rarely detained or arrested, but they sometimes suffer police violence, especially during protests. This assessment also reports that state intelligence services use spyware to monitor journalists' communications. It also reports that journalists are often subjected to social media smear campaigns and that essential equipment such as mobile phones, cameras and laptops is "often seized without judicial justification or a warrant".[262]

Stakeholders reported in late 2022 that private journalists suffer numerous forms of harassment – including the seizure of equipment such as mobile phones, cameras, and laptops without a warrant or any valid legal justification. It was also reported that vexatious civil lawsuits are brought against the media.[263]

In July 2023, members of the Directorate of Intelligence and Security invaded the offices of a leading newspaper, *Mmegi* and took editor Ryder Gabathuse and reporter Innocent Selatlhwa to an unknown location. instead of producing a warrant, one of the security agents reportedly stated: "I am a warrant myself." The two journalists were taken to an unknown destination.[264]

---

[259] Id, paragraph 199.
[260] Id, paragraph 200.
[261] Id, paragraph 198.
[262] "2023 World Press Freedom: Botswana", Reporters Without Borders.
[263] "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 6.
[264] "'I am a warrant myself': State security agents detain journalists in Botswana", *news24*, 21 July 2023.

Journalist Tshepo Sethibe, director of an online news site, was arrested in 2022 and charged with making **alarming publications** in violation of **section 59(1) of the Penal Code** after reporting misinformation regarding the disappearance of a child and thereby allegedly inciting persons to riot. The police seized two laptops, three mobile phones, a desktop computer, and passwords from the offices of the news site, *Moeladilotlhoko News Boiler*. The journalist was released on bail after one night in detention.[265] The case was due for trial at the High Court of Botswana in Maun on 19 May 2023, with Sethibe planning to challenge the constitutionality of the relevant section of the Penal Code,[266] but the case has been postponed until 5 October 2023.[267]

The same journalist was arrested in January 2021, along with fellow journalist Michelle Teise, and three other employees of the *Moeladilotlhoko News Boiler*. The five were charged with **criminal trespass** after entering the house of a man named Obakeng Badubi who had apparently disappeared earlier that month. They were held in custody for 10 days before being released. Sethibe, Teise and three other employees of the news outlet were again arrested in March 2021, in connection with the same journalistic investigation, on charges of **criminal trespass** as well as **seditious offences** – with the latter charge being based on their creation of t-shirts bearing the slogan "Bring back Obakeng". Police seized their computers and mobile phones and demanded the passwords. The five were granted bail after some 10 days in custody. The charges stemming from the March arrests were later dropped, but the outcome of the charges in the January arrests could not be ascertained.[268]

In 2020, it was reported that three men were arrested for stating on a Facebook page that the President had declared a State of Emergency ostensibly to address Covid, but actually "so that he could deal with his political rivals and business competitors". They were charged with making **alarming publications** under the Penal Code and **"offensive electronic communication"** under the Cybercrime and Computer Related Crimes Act, as well as for publishing "with intention to deceive" in violation of the Covid Emergency Regulations. The three accused were Justice Motlhabane (spokesperson of the opposition party Botswana Patriotic Front), Oratile Dikologang (co-founder and digital editor of the online *Botswana People's Daily News*) and Letsogile Barupi (a university student who administered a Facebook page called "Botswana Trending News"). The police characterised the publication as an offensive statement against the government" that was "degrading and maligning the leadership of the country". Motlhabane alleged that he was shocked with a Taser while being interrogated in custody, while Dikologang alleged that police physically abused him while interrogating him about his sources by stripping him naked and placing black plastic over his head to restrict his breathing. Police reportedly took cell phones and computer equipment from Motlhabani and used digital forensics

[265] "Botswana journalist Tshepo Sethibe criminally charged over 'alarming publications'", Committee to Protect Journalists, 19 July 2022; "2022 Country Reports on Human Rights Practices: Botswana", US State Department, section 2A.
[266] Melusi Simelane, "False news or free speech: Protecting freedom of expression in Botswana", Southern Africa Litigation Centre, 3 May 2023; "Challenging Criminal Code on Alarming Publications in Botswana", Southern Africa Litigation Centre, 22 March 2023.
[267] Southern Africa Litigation Centre, Facebook message, 19 May 2023.
[268] "Botswana police charge Moeladilotlhoko News Boiler staff with criminal trespass", Committee to Protect Journalists, 2 June 2021.

equipment to search his phone and computer. Barapi did not report any physical mistreatment, but said that police seized his phone, requested his password, reviewed his messages and contacts, and retrieved some information from the phone relating to the content on his Facebook page. Police confirmed ownership of mobile phone numbers the men used with their telecommunications service provider, which also provided an "activity log" in respect of an account owned by Dikologang. Dikologang gave police the password to his phone, and they extracted and analysed thousands of the journalist's messages, contacts, images, audio files and videos.[269]

In June 2020, journalists David Baaitse and Kenneth Mosekiemang, were arrested and charged with **common nuisance** under the Penal Code after they photographed a building linked to the Directorate of Intelligence and Security. They alleged that they were interrogated over a period of about seven hours, about why they were investigating the agency and how they conducted their reporting. They were held in police custody overnight, and their phones and camera were confiscated.[270]

Another 2020 incident involved the conviction of a Zimbabwean, Victor Moyo, in Botswana for violating section 18 of the Cybercrime and Computer Related Crimes Act, which prohibits **offensive electronic communication**. The offence was based on the circulation of a false report on social media that Batswana police had raped a Zimbabwean woman who was an illegal immigrant and subsequently killed her husband. It was reported that Moyo was sentenced by a Village Magistrate Court to a fine of P2000 or two months imprisonment in default of payment. The magistrate noted that such false communications have the potential to tarnish the image of the police, and that misleading information on social media can cause panic, fear and alarm.[271]

In 2017, Outsa Mokone, editor of the *Sunday Standard*, was tried for the crime of **sedition** on the basis of a 2014 news article about a car accident involving then-President Ian Khama and alleging that he failed to report the incident. The State dropped the case in 2018 after an appeal court ruled that the journalist's original arrest was unlawful (without considering the constitutionality of the crime of sedition). Media practitioners told the International Press Institute in 2022 that this case "had a significant chilling effect on the media in Botswana" despite the fact that the journalist was not ultimately sanctioned.[272]

A 2020 analysis of cybercrime laws in SADC alleged, without details, that efforts to combat cybercrime and safeguard public order in Botswana have resulted in

[269] "News editor in Botswana faces jail time over Facebook posts, alleges suffocation by police", Committee to Protect Journalists, 5 May 2021; Jonathan Rozen, "Equipped by US, Israeli firms, police in Botswana search phones for sources", Committee to Protect Journalists, 5 May 2021; "Coronavirus: Censorship is not the cure", Ink Centre for Investigative Journalism, 23 April 2020.
[270] "Journalists arrested, charged with 'nuisance' in Botswana", Committee to Protect Journalists, 29 June 2020; "President Masisi and the illusion of change", Ink Centre for Investigative Journalism, 19 June 2020
[271] "A Zimbabwean Man Arrested in Botswana for Publishing False Information On Social Media", *Afrinews 247*, 4 July 2020.
[272] "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 11. The appellate case could not be located online.

increased state surveillance, including the interception of communications, which has infringed rights such as the right to privacy and freedom of expression.[273]

4.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) CYBERCRIME AND COMPUTER RELATED CRIMES ACT 18 OF 2018

Botswana's 2018 Cybercrime and Computer Related Crimes Act replaced a 2007 law of the same name. It is based on the Budapest Convention even though Botswana is not a party.[274] The Act does not create any new implementing bodies but is rather concerned solely with offences and investigatory tools in respect of such offences.

This law establishes 12 new technical cyber offences. A positive element of the definitions of many of these technical cybercrimes is the requirement that they be committed intentionally and "without lawful excuse or justification". This phrase is not defined or elaborated in the statute, but it is a useful limiting factor that could in theory be applied to cases where the actions described in the law were carried out in the public interest.

CYBERCRIME AND COMPUTER RELATED CRIMES ACT, 2018 – TECHNICAL OFFENCES	
Section4: Unauthorised access to a computer or computer system	It is an offence to - • intentionally access or attempt to access the whole or any part of a computer or computer system knowing that the access he or she intends to secure is unauthorised; or • cause a computer or computer system to perform any function as a result of unauthorized access. o Both categories of actions are offences, regardless of the purpose of the unauthorized access, meaning that this offence could in theory apply to a journalist or a security researcher who accessed a computer system to test its vulnerabilities, for instance. o "Access" is broadly defined to cover instructing, communicating with, storing data in, retrieving data from, or otherwise making use of any of the resources of the computer or computer system (definition in section 2). It has been pointed out that this wide definition is wide means that the offence covers not just the initial entering of a computer system but also subsequent acts involving its data; this could mean a person who has authorisation to *enter* a computer system may still commit an offence by *storing or retrieving data* from a computer system without authorization. It also means that merely

[273] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 24.
[274] Seth Sarefo, Banyatsang Mphago & Maurice Dawson, "An analysis of Botswana's cybercrime legislation", *Procedia Computer Science*, Volume 219, 2023, pages 1023-1033, Section 1, Introduction.

	communicating with a computer system, without actual entry into the system, qualifies as an offence.[275] o "Unauthorised access" is broadly defined, covering situations where the person accessing the computer, computer system or computer service * is not themselves entitled to the access; * does not have the consent of a person who is entitled to the access; or * exceeds the access for which he or she is authorised (definition in section 2). o While some assert that criminalisation of "mere access" without more is justified given that it compromises data confidentiality, there is no universal consensus on whether criminalization of mere access to non-protected systems is warranted, or whether this crime should be narrowed by additional conditions.[276] The *SADC Model Law on Computer Crime and Cybercrime* qualifies the offence of illegal access by requiring that it take place "intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification".[277] On the other hand, Global Partners Digital cites this formulation as an example of good practice that is closely modelled on the offence of illegal access in the Budapest Convention. This group recommends a broad approach without any additional intent requirements that might allow infringement of privacy.[278]
Section5: Unauthorized access to a computer service	It is an offence to knowingly and by any means, without authorisation or exceeding the authorisation that was given, to - • secure access *or intend to secure access* to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; • intercept, cause interception (directly or indirectly) or *intend to access* any function of, or any data within, a computer or computer system. There is no criminal liability where a person - • is acting with the express or implied consent of both the person who sent the data and its intended recipient; or • is acting in reliance on powers conferred by law (which would presumably cover access by law enforcement officials conducting a lawful criminal investigation, amongst other things) o A "computer service" is defined as including "data processing or the storage or retrieval of data" (definition in section 2). o The purpose of the unauthorised access is immaterial. Note also that the mere *intention* to secure such access is an offence, even if this is not accompanied by any attempt to secure the access, or any action at all.

[275] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 14.
[276] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
[277] SADC Model Law on Computer Crime and Cybercrime, section 4.
[278] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], pages 14 and 30.

	○ It has been noted that aspects of this offence overlap unnecessarily with the offence of unlawful interception of data in section 9.[279]
Section 6: Access with intent to commit or facilitate commission of an offence	It is an offence to cause a computer or computer system to perform any function for the purpose of securing access to any programme or data held in a computer or computer system or a computer service, *with intent to commit an offence.* ○ The requisite criminal intent narrows the offence here. ○ This offence has been described as "a subspecies of the offence of illegal access to a computer system as provided for under section 4, with the difference that the offence under section 6 is committed with a distinct motivation or intention to commit another offence."[280]
Section 7: Unauthorised interference with data	It is an offence to carry out or attempt any of the following acts *intentionally and without lawful excuse or justification*- • to damage, deteriorate, delete, alter or modify computer data • to render computer data meaningless, useless or ineffective • to obstruct, interrupt or interfere with the lawful use of computer data • to deny access to computer data to any person entitled to it. There is an additional penalty where the offence results in impairment, suppression, alteration or modification of the operation of a computer or computer system, access to any programme or data held in a computer or computer system, the operation of any programme or the reliability of any data. ○ "The section covers the basic elements of the offence as prescribed by the Budapest Convention."[281]
Section 8: Unauthorized interference with a computer or computer system	It is an offence, *intentionally and without lawful excuse or justification*, to - • hinder or interfere with the functioning of a computer or computer system; • hinder or interfere with a person who is lawfully using or operating a computer or computer system. . It is a more serious offence, *intentionally and without lawful excuse or justification*, to commit an act that causes (directly or indirectly) • a denial or partial denial of access to a computer or computer system; or • an impairment of any programme or data stored in a computer or computer system.
Section 9: Unlawful interception of data	It is an offence, *intentionally and without lawful excuse or justification*, to intercept by technical means - • any non-public transmission to, from or within a computer or computer system; or • any electromagnetic emissions that are carrying data from a computer or computer system.

[279] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 23.
[280] Id.
[281] Id, page 17.

	○ "The definition incorporates all the key definitional elements of the offence of data interception as prescribed by the Budapest Convention."[282] ○ It has been noted that this offence overlaps with aspects of section 5.[283]
Section 10: Unlawful possession of devices or data	It is an offence *intentionally and without lawful excuse or justification*, to manufacture, sell, procure for use, import, export, distribute or otherwise make available a computer, computer system or any other device designed or adapted *for the purpose of committing an offence* – as well as *intentionally and without lawful excuse or justification* to receive or possess such a device. It is an offence to possess any data or programme *with the intention that the data or programme will be used to commit or facilitate the commission of an offence under the Act.* ○ "The wording of the section gives one the impression that the devise need not be designed or adapted primarily for the purposes of committing cybercrimes, and that dual-use devices are covered. However, the requirement that the person must act 'without lawful excuse or justification' saves the day, as dealing in such dual-use devices for non-criminal and legitimate purposes would not be 'without lawful excuse or justification'."[284]
Section 11: Unauthorized disclosure of password or access code	It is an offence, *intentionally and without lawful excuse or justification,* to disclose, sell, procure for use, distribute or otherwise make available, any password, access code or other means of gaining access to a computer or computer system • for wrongful gain; • for any unlawful purpose; • to overcome security measures for the protection of data; or • with the knowledge that it is likely to cause prejudice to any person. ○ The requisite list of purposes, combined with the requirement that the action be taken without lawful excuse or justification, appears to make this offence suitably narrow.
Section 12: Damage to a computer or computer system [by means of "computer contaminants"]	It is an offence to intentionally introduce, or cause to be introduced, a "computer contaminant" into a computer or computer system if this contaminant causes, or is capable of causing, any of the following effects: • modifies, destroys, records or transmits any data or programme residing within a computer or computer system • usurps the normal operation of a computer or computer system • destroys, damages, degrades or adversely affects the performance of a computer or computer system

[282] Id, page 16.
[283] Id, page 23.
[284] Id, page 21.

	• attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer or computer system. o This provision covers what laypersons might refer to as computer viruses and malware. The requirement of intentionality protects persons who innocently spread such things by accident, such as by innocently sharing an infected file.
Section 13: Critical national infrastructure	It is an additional offence if a person obtains access to critical national infrastructure in the course of the commission of another offence under the Act. "Critical national infrastructure" means "computer systems, devices, networks, programmes or data, including those of national emergency organizations, so vital to Botswana that the incapacity or destruction of, or the interference with, such systems and assets would have a debilitating impact on national security, national economic security, public health and safety or a combination of any of these". There is a presumption, without proof to the contrary, that the accused knew that the computer in question formed part of critical national infrastructure. o This presumption could be problematic as it essentially shifts the burden of proof of a key element of the crime to the accused.
Section 14: Cyber extortion	It is an offence to perform or threaten to perform any of the acts described under Part 2 of the law (which contains all of the offences, including the content-based ones), for the purposes of obtaining any unlawful advantage from undertaking to cease or desist from such actions, or to restore any damage caused as a result of those actions.
Section 15: Cyber fraud	It is an offence to perform any of the acts described under Part 2 of the law (which contains all of the offences) for purposes of obtaining any unlawful advantage by causing forged data to be produced, *with the intent that it be considered or acted upon as if it were authentic*. It is an offence, *with intent to procure any advantage for oneself or another person*, to fraudulently cause loss of property to another person by any input, alteration, deletion, delaying transmission or suppression of data, or any interference with the functioning of a computer or a computer. system. o The required intent helps to ensure that these offences are properly targeted.

The statute also includes seven categories of content-based offences including cyber harassment, cyber stalking, "offensive electronic communication", a group of offences relating to "child pornography or obscene material relating to children", revenge pornography and two types of offences relating to hate speech. It is these

content-based offences that involve the greatest cause for concern.[285] There is no crime relating to speech concerning genocide and crimes against humanity, as is found in some other SADC cyber laws.

CYBERCRIME AND COMPUTER RELATED CRIMES ACT, 2018 – CONTENT-BASED OFFENSES	
Section 16: Cyber harassment	A person who uses a computer or computer system, or who knowingly permits a device to be used, for any of the following purposes - (a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or (b) threatening to inflict injury or physical harm to the person or property of any person, commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both. o The terms "obscene", "lewd", "lascivious" and "indecent" are not defined in the Act. o In the phrase "injury or physical harm" the term injury appears to include injuries other than physical harm, such as psychological or reputational damage. This would make the provision very wide. It is also important for the definition of a crime to be very clear about what is prohibited. o The potential dangers of this vague approach are illustrated by the prosecution of a journalist for distributing "obscene" material under the previous 2007 Act in connection with social media posts implicating a government minister in a sex scandal – which showed his sexual partner half-naked.[286] On the other hand, it is possible that the relevant information could have been reported without any invasion of privacy.[287] o There is no provision for restraining orders to protect the victim in cases where the harassment does not warrant imprisonment.
Section 17: Cyberstalking	A person who willfully, maliciously or repeatedly uses electronic communication to harass another person, or makes a threat with the intent to place that person in reasonable fear for his or her safety or for the safety of his or her immediate family, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. o Note that this offence involves two different situations: (1) using electronic communication to "harass" another person; or (2) using electronic communication to make a threat with the intent to place a person in reasonable fear for his or her safety or for the safety of his or her immediate family. The second situation is a sensible prohibition, but the first is wide and vague – particularly since the meaning of "harass" is not defined.

[285] For a brief overview, see "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], pages 21-23.
[286] "Misa Botswana Press Release on Mr Daniel Kenosi", *The Patriot on Sunday*, 5 April 2015; "Daniel Kenosi sued for 25000", *Razi 24*, 26 February 2019; "Kenosi to swallow P250K bitter pill", *Mmegi online*, 27 February 2019.
[287] In a case involving a report of an extramarital affair, a newspaper published a photo of a partially unclothed woman, alleging that the public has a right to be informed of current news and events. The person pictured won damages against the newspaper for invasion of privacy. The High Court pointed out that the story could have been told without the photograph. *Esterhuizen v Francistowner (Pty) Ltd T/A Voice Newspaper* (CVHFT-000621-11) [2012] BWHC 61 (12 October 2012).

	○ The offence applies where a person "willfully, maliciously or repeatedly" uses electronic communication to produce the indicated results. The use of the word "or" means that there need not be either malicious intent or repeated actions. ○ Note that there is no requirement that there be an intent to harass. ○ Note that there is no exception for actions done in good faith - meaning that could in theory be applied, for example, to a journalist who repeatedly uses electronic communication to seek information or comment for a news article or to reasonable efforts by a creditor to secure payment from a debtor. ○ There is no provision for restraining orders to protect the victim in cases where the cyber stalking does not warrant imprisonment.
Section 18: Offensive electronic communication	A person who willfully, maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. ○ The offence applies where a person "willfully, maliciously or repeatedly" uses electronic communication to produce the indicated results. The use of the word "or" means that there need not be either malicious intent or repeated actions. ○ The wording of this provision does not suggest that it was enacted with a view to restricting freedom of expression unreasonably; in fact, one example of inappropriate online content cited by the government in connection with the new law was posting distasteful pictures of accident scenes on social media before the next of kin of the accident victims have been notified.[288] However, regardless of the legislative intent, the case studies cited above show that this offence has been used against journalists on several occasions – even if those charges did not ultimately stick. ○ "It is not clear what could fall under 'offensive electronic communications' or 'legitimate communication'. There should be clarity on these terms otherwise statements that criticize the government could easily fall under "offensive communication" and this would curtail freedom of expression."[289]
Section 19: Pornographic or obscene material	There is an extensive set of offences relating to "child pornography" or "obscene material relating to children". Most of the actions in this section are offences only if they involve a computer or a computer system. The exception is publishing an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children, which is an offence without reference to the medium used for the advertisement. This section also covers various kinds of grooming, although the section does not use that term but rather refers to "facilitating the commission" of

[288] "Cyber bullying must be dealt with thoroughly", *Weekend Post*, 10 October 2017.
[289] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 25. A similar point is made in "LEXOTA Country Analysis: Botswana", last updated July 2022.

	certain crimes. It is an offence to use a computer or computer system to communicate with a person who is (or is believed by the accused to be) – • under age 18, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code; • under age 16, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or • under age 16, for the purpose of facilitating the commission of the offence of defilement or any sexual offence of that person under the Penal Code. o "Child pornography" is defined in this section to include "material that visually or otherwise depicts - * a child (meaning a person under age 18) engaged in sexually explicit conduct, * a person who appears to be a child engaged in sexually explicit conduct, or * realistic images representing a child engaged in sexually explicit conduct. o "Sexually explicit conduct" is defined in this section to mean "any conduct, whether real or simulated, which involves - * sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex, * bestiality, * masturbation, * sadistic or masochistic sexual abuse, or * the exhibition of the genitals or pubic area of a child. o There is no definition of "obscene material relating to children", making it unclear what is covered by this term. o There is no defence for images that are produced or communicated for genuine artistic, educational, legal, medical, scientific or public benefit purposes.
Section 20: Revenge pornography	It is an offence by means of a computer or computer system, to disclose or publish a private sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress.
Section 21: Racist or xenophobic material	It is an offence by means of a computer or computer system to produce, offer or make available, distribute or transmit "racist or xenophobic material". o Section 2 defines "racist or xenophobic material" as "any material which advocates, promotes or incites hatred, discrimination or violence against any person or group of persons based on race, colour, descent, nationality, ethnic origin, tribe or religion". o Unlike some other SADC countries, here the reference to "religion" is not limited to instances where religion is used as a pretext for one of the other listed grounds.

	○ Note that this offence overlaps with section 92 of the Penal Code, which is discussed below.[290]
Section 21: Racist and xenophobic motivated insult	It is an offence by means of a computer or computer system, to insult another person on the basis of race, color, descent, nationality, ethnic origin, tribe or religion. ○ There is no definition or qualification of the term "insult". ○ Although this provision is based on the Malabo Convention, criminalising "insult" seems extremely vague and overbroad ○ Note that there is no requirement of an intention to insult another person, meaning that it could be possible for the crime to be inadvertently committed (based on a statement intentionally made, but made without the aim of insulting another). ○ Note that the aspect of this offence concerning religion overlaps with section 140 of the Penal Code, which is discussed below.[291]

A police officer or any person authorised by the Commissioner of Police or the Director-General of the Directorate on Corruption and Economic Crime (described in this discussion as "another authorised person") has the power to issue a **preservation order** for electronic data "where there are reasonable grounds to believe that such data is vulnerable to loss or modification", but such an order requires confirmation by a court as soon as reasonably practicable.[292]

However, **certain actions relating to the preservation and disclosure of data do *not* require judicial involvement**. A police officer or another authorised person may issue a written notice to a person in control of a computer or computer system requiring that person to **ensure that the data specified in the notice is preserved** for the period specified in the notice. Such a notice can also require that person to "disclose sufficient **traffic data** about a specified communication to identify the service provider or the path through which the data was transmitted". [293]

A police officer or another authorised person may apply to a judicial officer for a **production order relating to other stored data or subscriber information**.[294]

Ordinarily, warrants issued by a judicial officer, on application by a police officer or another authorised person are required for **searches and seizures** in terms of the Act, as well as for the collection of **real-time traffic data** associated with specific communications.[295]

However, a police officer of the rank of sergeant or above is empowered to do any of these things ***without applying for an order* from a judicial authority**, if such an application would result in an **undue delay** in the investigation of any offence under

[290] Penal Code [*Chapter 08:01*], section 92.
[291] Id, section 140.
[292] Cybercrime and Computer Related Crimes Act, 2018, section 24.
[293] Id, section 25.
[294] Id, section 26.
[295] Id, sections 27-28.

the Act.[296] This seems to be a weak basis for dispensing with such an important safeguard.

The Director of Public Prosecutions, or his or her delegate, may apply to a judicial officer for an order that **pornography, obscene material or child pornography in a computer or a computer system** be removed, deleted or destroyed.[297]

There is a curious set of qualifications to the principle that data obtained under this Act by a police officer or any person authorised by the Commissioner or by the Director-General may be used only for the purpose for which the data was originally sought. This principle does *not* apply in cases where the data was sought in accordance with any other enactment, in compliance with a court order, for the prevention of injury or other damage to the health of a person, for the prevention of serious loss of or damage to property, or in the public interest.[298] The exceptions seem so wide as to virtually nullify the underlying principle.

B) PENAL CODE

Certain provisions of the Penal Code that criminalise specific forms of expression seem to have been used repeatedly against media practitioners, in respect of both online and traditional media.

PENAL CODE

59. Alarming publications

1) Any person who publishes any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace is guilty of an offence.

2) It shall be a defence to a charge under section (1) if the accused proves that, prior to publication, he took such measures to verify the accuracy of such statement, rumour or report as to lead him reasonably to believe that it was true.

One such crime that has been used in practice is the crime of "**alarming publications**" in section 59, which prohibits the publication of "any false statement rumour or report" that is likely to cause fear or alarm to the public, or to disturb the public peace. This office appears to be very overbroad. Although it is a defence to this charge to show that reasonable steps were taken to verify the content of the publication, which led the author to believe the information to be true, this essentially places the onus on the journalist to prove his or her innocence.[299] As one commentary notes: "It is not clear how to determine whether a statement, rumour or report is 'false' or the scope of something that is 'likely to cause fear and alarm to the public or to disturb the public peace'.

Section 59(1) therefore does not provide sufficient guidance for individuals to conform their behaviour and gives an overly wide degree of discretion to those charged with the enforcement of this law."[300]

---

[296] Id, section 30.
[297] Id, section 29.
[298] Botswana Cybercrime and Computer Related Crimes Act, 2018, section 31(1).
[299] Penal Code [*Chapter 08:01*], section 59.
[300] "LEXOTA Country Analysis: Botswana", last updated July 2022.

Another broadly–worded offence that has been applied to journalists is "**common nuisance**" in section 176, which can include any action undertaken without legal authority that is annoying, obstructive or inconvenient to the public.[301]

PENAL CODE

176. Common nuisance

1) Any person who does an act not authorized by law or omits to discharge a legal duty and thereby causes any common injury, or danger or annoyance, or obstructs or causes inconvenience to the public in the exercise of common rights, commits the offence termed a common nuisance and is liable to a fine not exceeding P5.000 or imprisonment for a term not exceeding two years, or to both.

2) It is immaterial that the act or omission complained of is convenient to a larger number of the public than it inconveniences, but the fact that it facilitates the lawful exercise of their rights by a part of the public may show that it is not a nuisance to any of the public.

More broadly, the Penal Code contains extensive provisions on **criminal defamation**, with defamatory matter being defined as "matter likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule, or likely to damage any person in his profession or trade by an injury to his reputation". There are exceptions for publications that are true and for the public benefit as well as various expressions of opinion made in good faith, including amongst other exceptions good faith comments about the conduct or personal character of a person in a judicial, official, or other public capacity or good faith comments about the conduct or personal character of any person "in relation to any public question or matter". Good faith is presumed as a starting point. [302] The penalty for the crime of criminal defamation can be an unspecified fine or imprisonment for up to two years, or both.[303]

The crime of **sedition** in section 51 is not commonly applied to journalists, but it is an extremely concerning restriction on freedom of expression. (The key provisions of this crime are quoted in the box below.) Publications have a seditious intention if they inspire hatred, contempt or "disaffection" against the President or the Government of Botswana or the administration of justice, or if they "raise discontent or disaffection amongst the inhabitants of Botswana" - amongst other things – and the exceptions are so narrowly-cast that threading the line between seditious intent and acceptable comment would be tantamount to walking a tightrope.[304] For instance, it could be nerve-wracking to find the line between pointing out that the President has been "mistaken" in any of his or her measures, without "exciting disaffection" against the President. Both producing and possessing a seditious publication are punishable by up to three years imprisonment. [305] The consequences of sedition for print media could be particularly devastating since the law allows police to confiscate a printing machine used to print or reproduce the material in question on the strength of an arrest alone.[306] In the case of a conviction, the printing machine can be confiscated

[301] Penal Code [*Chapter 08:01*], section 176, as amended by the Penal Code (Amendment) Act 21 of 2018.
[302] Id, sections 192-199.
[303] Id, section 33 (which applies when no penalty is otherwise specified in the law).
[304] Id, sections 50-51.
[305] Id, section 51(1)-(2).
[306] Id, section 51(4).

for a year or forfeited to the State entirely. If the convicted person is a proprietor, publisher, printer or editor of a newspaper, the court has the authority to order that the newspaper must cease publication for up to one year.[307] The International Press Institute reported in 2022 that, although charges of sedition against journalists are rare, "stakeholders said that existence of these provisions has a strong chilling effect on the media in Botswana and limits critical reporting on government officials and about government actions".[308]

PENAL CODE

51. Seditious offences

(1) Any person who-

(a) does or attempts to do, or makes any preparation to do, or conspires with any person to do, any act with a seditious intention;

(b) utters any words with a seditious intention;

(c) **prints, publishes, sells, offers for sale, distributes or reproduces any seditious publication**;

(d) imports any seditious publication, unless he has no reason to believe that it is seditious, is guilty of an offence and is liable to imprisonment for a term not exceeding three years; and any seditious publication shall be forfeited to the State.

(2) Any person who without lawful excuse **has in his possession any seditious publication** is guilty of an offence and is liable to imprisonment for a term not exceeding three years; and such publication shall be forfeited to the State.

[…]

(4) Any printing machine which has been, or is reasonably suspected of being, used for or in connection with the printing or reproduction of a seditious publication may be seized or otherwise secured by a police officer pending the trial and conviction or discharge or acquittal of any person accused of printing or reproducing any seditious publication; and, when any person is convicted of printing or reproducing a seditious publication, the court may, in addition to any other penalty which it may impose, order that the **printing machine on which the publication was printed or reproduced shall be either confiscated for a period not exceeding one year, or be forfeited to the State**, and may make such order whether or not the person convicted is, or was at the time when the publication was printed or reproduced, the owner of the printing machine. A printing machine forfeited under this subsection shall be sold, and the proceeds, less expenses, shall be paid into the general revenue.

[307] Id, section 51(5).
[308] "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 11.

(5) When a proprietor, publisher, printer or editor of a newspaper is convicted of printing or publishing a seditious publication in a newspaper, the court may, in addition to any other punishment it may impose, and whether or not it has made an order under subsection (4), make an **order prohibiting any further publication of the newspaper for a period not exceeding one year**.

50. Seditious intention

A seditious intention is an intention

(*a*) to bring into **hatred or contempt** or to **excite disaffection** against the person of
the
President or the **Government of Botswana** as established by law;
(*b*) **to excite the inhabitants of Botswana to attempt to procure the alteration, otherwise**
than by lawful means, of any other matter in Botswana as established by law;
(*c*) to bring into **hatred or contempt** or to **excite disaffection** against the **administration of justice** in Botswana;
(*d*) to raise discontent or disaffection amongst the inhabitants of Botswana; or
(*e*) to **promote feelings of ill-will and hostility between different classes of the population** of Botswana, but an act, speech or publication is ***not seditious*** by reason only that it intends –
(i) to show the **President has been misled or mistaken** in any of his measures;
(ii) to **point out errors or defects** in the Government or the Constitution of Botswana as established by law or in legislation or in the administration of justice **with a view to the remedying of such errors or defects**;
(iii) to **persuade the inhabitants of Botswana to attempt to procure by lawful means the alteration of any matter** in Botswana as established by law; or
(iv) **to point out, with a view to their removal, any matters which are producing or have a tendency to produce feelings of ill-will and enmity between different classes of the population** of Botswana.

(2) In determining whether the intention with which any act was done, any words were spoken, or any document was published, was not seditious, every person shall be deemed to intend the consequences which would naturally follow from his conduct at the time and under the circumstances which he so conducted himself.

Another broad and somewhat related provision in section 134 of the Penal Code criminalises "**undermining authority of public officers**" by acts or publications "calculated to bring into contempt, or to excite defiance of or disobedience to, the lawful authority of a public officer or any class of public officers" without "lawful excuse" – where the defence of "lawful excuse" must be proved by the accused. The penalty is imprisonment for up to three years.[309]

[309] Penal Code [Chapter 08:01], section 134.

Section 60, entitled "**defamation of foreign princes**", criminalises the publication of "anything intended to be read, or any sign or visible representation, tending to degrade, revile or expose to hatred or contempt any foreign prince, potentate, ambassador or other foreign dignitary" with the intent to disturb the peace and friendship between Botswana and the country in question. Such publications can be defended on the same basis as defamation of private persons.[310] However, we have found no evidence of this provision being used in practice against the media.

Section 93 makes it an offence **to use "abusive, obscene or insulting language"** in relation to the **President, any other member of the National Assembly or any public officer *in a public place or at a public gathering***.[311] While this appears to be an unfounded restriction on freedom of expression, it does not appear on its face to apply to publications of any kind.

Another aspect of the Penal Code that could be used to stifle freedom of expression concerns "**prohibited publications**". The President has complete discretion to declare any publication or series of publications to be a "prohibited publication" if it is, in his or her opinion, "contrary to the public interest" – defined as the "interests of defence, public safety, public order, public morality or public health". The prohibition can apply to any publication or class of publications, past or future, described in the President's order, including all subsequent issues of a periodical publication.[312] (The definition of publication seems sufficiently wide to capture online publications.[313]) Reproduction, sale, distribution or possession of a prohibited publication is a criminal offence that can attract a penalty of imprisonment for up to three years,[314] and police officers or administrative officials have a broad authority to confiscate prohibited publications.[315] (The key provisions relating to this offence are reproduced at the end of this subsection.) We have located no reports of this provision being applied in practice to media outlets, but its far-reaching nature could have a chilling effect on media content.

[310] Id, section 60.
[311] Id, section 93.
[312] Id, section 47. There is a separate provision of the Penal Code on "traffic in obscene publications" (section 178).
[313] Id, section 2: "'publication' includes all written and printed matter, and any gramophone or other record, perforated roll, recording tape or wire, cinematograph film or other contrivance by means of which any words or ideas may be mechanically produced, represented or conveyed, and everything, whether of a nature similar to the foregoing or not, containing any visible representation or by its form, shape or other characteristics, or in any manner capable of producing, representing or conveying words or ideas, and every copy or reproduction or any publication".
[314] Id, section 48.
[315] Id, section 49.

PENAL CODE

47. Prohibited publications

(1) If the President is of the opinion that there is in any publication or series of publications published within or without Botswana by any person or association of persons matter which is contrary to the public interest, he may, in his absolute discretion, by order published in the *Gazette* and in such local newspapers as he may consider necessary, declare that that particular publication or series of publications, or all publications of any class of publication specified in the order published by that person or association of persons, shall be a prohibited publication or prohibited publications, as the case may be.

(2) If an order made under the provisions of subsection (1) specifies by name a publication which is a periodical publication, such order shall, unless a contrary intention be expressed therein, have effect -

(a) with respect to all subsequent issues of such publication; and

(b) not only with respect to any publication under that name, but also with respect to any publication published under any other name if the publishing thereof is in any respect a continuation of, or in substitution for, the publishing of the publication named in the order.

(3) If an order made under the provisions of subsection (1) declares that all publications of any class of publication published by a specified person shall be prohibited publications, such order shall, unless a contrary intention be expressed therein, have effect not only with respect to all publications of that class published by that person or association of persons before the date of the order but also with respect to all publications of that class so published on or after such date.

[…]

(8) In this section, "public interest" means the interests of defence, public safety, public order, public morality or public health.

48. Penalty for prohibited publications

(1) Any person who, otherwise than in his capacity and in the course of his duties as a public officer, prints, makes, imports, publishes, sells, supplies, offers for sale or supply, distributes, reproduces or has in his possession or under his control any prohibited publication is guilty of an offence and is liable to imprisonment for a term not exceeding three years […]

49. Seizure and disposal of prohibited publications

(1) Any police officer or administrative officer may seize and detain any prohibited publication which he finds in circumstances which raise a reasonable presumption that an offence under this Code has been, is being or is intended to be committed in relation thereto, or which he finds abandoned or without an apparent owner or possessor or in the possession or custody of any unauthorized person.

(2) Any of the following officers, that is to say –

(*a*) any police officer not below the rank of Sub-Inspector;
(*b*) any other person employed in the public service authorized in that behalf by the Minister, may detain, open and examine any package or article which he suspects to contain any prohibited publication, and during such examination may detain any person importing, distributing or posting such package or article or in whose possession such package or article is found.

(3) If any prohibited publication is found in such package or article, the whole package or article may be impounded and retained by the officer, and the person importing, distributing or posting it, or in whose possession it is found may be arrested by the officer and delivered to police custody to be dealt with according to law.
(4) Any prohibited publication which is seized or detained as aforesaid, or which in any other manner comes into the possession or custody of any court or any public officer, shall be forfeited to the State and may be destroyed or otherwise disposed of, as may be directed by such court or by the Commissioner of Police, as the case may be.

Section 92 of the *Penal Code* criminalises **hate speech** based on race, tribe, place of origin, colour or creed, but this is limited to statements or publications "expressing or showing hatred, ridicule or contempt" and so is fairly narrowly-drawn. It also includes the extra safeguard of requiring that prosecutions for this offence may be instituted only with the written consent of the Director of Public Prosecutions.[316] This offence is also much more narrowly-drawn than the corresponding offence for "insults" in the *Cybercrime and Computer Related Crimes Act, 2018* (discussed above).

Publications with "**intent to wound religious feelings**" are criminally punishable by imprisonment for up to one year, under section 140. No further detail is provided about what such publications must entail.[317]

C) COMMUNICATIONS REGULATORY AUTHORITY ACT 19 OF 2012

As touched on above in section 4.1 of this chapter, the Communications Regulatory Authority Act, 2012 has some provisions of relevance related to **suppliers of goods and services in the "regulated sector",** which means any sphere of activity within the telecommunications, broadcasting and postal service sectors" – including the provision of internet services.[318]

In terms of this Act, the Botswana Communications Regulatory Authority (BOCRA) may require from any regulated supplier any information it deems necessary to enable it to carry out its functions under the Act. Failure to comply with such a request is an offence.[319] The Act also requires regulated suppliers to maintain a register of their

[316] Id, section 92.
[317] Id, section 140.
[318] Communications Regulatory Authority Act 19 of 2012, section 2.
[319] Id, section 8(1).

customers or subscribers "in such manner as the Minister may prescribe", and to provide information from this register to BOCRA or any other person designated by BOCRA. It is an offence for a subscriber or a customer to fail to provide any information that the minister requires, and a regulated supplier that fails to comply with the rules on registers can be fined up to 10% of the net turnover of the business in the previous financial year.[320]

The Act contains a general duty of confidentiality in respect of messages transmitted over telecommunications systems, but this duty does not apply to the **disclosure of information in connection with the investigation of any criminal offence or for criminal proceedings**.[321]

The Act authorises the **interception of messages transmitted via any service provider "during any emergency"**, with the meaning of "emergency" left undefined; failure to comply is a criminal offence on the part of the service provider.[322]

This law also contains a content-based offence for **improper use of a public telecommunications system.** This applies to any message or other matter which is "offensive" or of "an indecent, obscene or menacing character" as well as to messages sent via a public telecommunications system "for the purpose of causing annoyance, inconvenience or anxiety to another person" or a message which is known to be false. The penalty for this excessively broad offence is a minimum fine of P10 000 (but not more than P50 000) or imprisonment for a minimum of one year (but not more than four years), or both.[323] One analysis comments: "It is not clear how to determine what is 'false' and the potential scope of what is considered annoying, inconvenient or intended to cause anxiety is excessively broad. The threshold of committing this offence in terms of the harm caused is thus very low. Section 55(b) therefore does not provide sufficient guidance for individuals to conform their behaviour and gives an overly wide degree of discretion to those charged with the enforcement of this law."[324]

No information on the application of any of these provisions was located.

[320] Id, section 50(3)-(5).
[321] Id, section 54(2).
[322] Id, section 53.
[323] Id, section 55.
[324] "LEXOTA Country Analysis: Botswana", last updated July 2022.

D) STATE SURVEILLANCE: CRIMINAL PROCEDURE AND EVIDENCE (CONTROLLED INVESTIGATIONS) ACT 14 OF 2022

In January 2022 the Government proposed a Criminal Procedure and Evidence (Controlled Investigations) Bill that would have authorised law enforcement officials to access communications by "any means", without a warrant. This proposal drew opposition from media groups as well as others, leading to amendments that introduced warrant requirements for the interception of communications as well as enhanced supervisory mechanisms.[325]

According to Prof. Balule, the Botswana government could have avoided the public outcry and backlash "if the government had widely consulted the people before coming up with that bill". He noted that a particular issue in Botswana was "that there's very little public participation in the law-making process in Botswana", which has led to poorly conceived draft laws making it to parliament over the years only for there to be an outcry and an embarrassing withdrawal of such problematic proposed laws.

The term "controlled investigation" includes interception of communication amongst other "undercover" methods of crime investigation. The Act makes it a criminal offence for an investigating officer to intercept communications without "an interception warrant" issued under this law.

An investigating officer must apply to a court for "an **interception warrant**" with a detailed motivation. A court can grant an application for an interception warrant only where it is satisfied that the person being investigated is involved in "serious" crime-related activities and that "material information" relating to the commission of an offence or the whereabouts of a suspect is contained in the communication.[326] Furthermore, the court must be satisfied that the requested information-gathering is necessary to avert "an actual threat to national security or to compelling national economic interest", or "a potential threat to public safety or national security".[327] An interception warrant is valid for a maximum of three months, but can be renewed for three-month periods. The court has the power to amend or revoke the authorisation at any time.[328] Any evidence collected via an interception warrant that exceeds the authority of the warrant is admissible in criminal proceedings, only with the leave of the court.[329]
It is an offence for a service provider to refuse to give assistance with lawful interceptions.[330]

As an additional safeguard, the law establishes a Controlled Investigations Coordination Committee which has the duty to:

(a) assess the effectiveness of policies and measures of criminal investigations to combat serious crime related activities;

[325] Jonathan Rozen, "Botswana journalists remain 'vigilant' under new surveillance law", Committee to Protect Journalists, 4 May 2022.
[326] Id, section 23.
[327] Id, section 24(1).
[328] Id, section 24(2)-(3).
[329] Id, section 25.
[330] Id, section 28.

(b) make recommendations to the Minister for legislative, administrative and policy reforms in respect to criminal investigations; and
(c) promote coordination among the investigatory authorities, supervisory authorities and other institutions with a view to improving the effectiveness of existing policies and measures to combat financial offences through criminal investigations.[331]

More specifically, this Committee is also tasked to protect the interests of interception subjects and targets and to consider complaints in respect of the use of warrants issued under the Act. It has the power to impose administrative sanctions, award compensation, follow up on enforcement procedures to ensure compliance with conditions of warrants issued under the Act and to recommend Codes of Conduct in connection with the Act. The Committee must be chaired by a judge (or a legal practitioner who qualifies to be appointed as a judge) and it includes certain ex *officio* government personnel as well as persons appointed on the basis of their relevant expertise.[332]

The Act as passed is commendable for setting a high bar for interception of communications, and for providing safeguards for its use. One aspect missing from the law, however, is any requirement that persons whose communications were monitored must be informed of this fact after the conclusion of the investigation. Given that the law has been in force for only a relatively short time (since 25 February 2022), its application in practice should be monitored over time.
There are two other legal provisions in different statutes that permit specified judicial officers to grant communication interception orders for law enforcement purposes.

- Section 20 of the **Counter-Terrorism Act 24 of 2014** allows an investigating officer to apply to a magistrate or a High Court judge for an order to intercept communications for the purpose of obtaining evidence of the commission of an offence under that Act or the whereabouts of a person suspected to have committed an offence under that Act. This would relate only to offences associated with terrorism and its financing. An initial interception order under this law can cover a period of up to 90 days and can be extended for up to 180 days.[333]
- Section 22 of the **Intelligence and Security Services Act 16 of 2007** allows the Director of Intelligence and Security to apply to a senior magistrate or a High Court judge for a warrant in connection with investigation of "any threat to national security" or to the ability of the Directorate of Intelligence and Security to perform any of its functions under this Act. Such a warrant can authorise any action specified in the warrant that the court considers necessary to obtain information which is likely to be of substantial value to the Directorate in the discharge of its functions and cannot be reasonably obtained through other means. This can include a warrant for the

[331] Id, Schedule: paragraph 1.
[332] Id, section 14 and Schedule.
[333] Counter-Terrorism Act 24 of 2014, section 20. This link is to the original version of the Act, which has been amended several times. See Tachilisa Badala Balule, "Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework", Media Policy and Democracy Project, November 2021, pages 10, 14.

interception of post, electronic mail, computer or telephonic communications (amongst other things). This power is particularly wide since the functions of the Directorate can include any duties and functions that the President determines to be "in the national interest". The Act also contains an extensive list of the types of acts that can constitute threats to national security. There is no time limit on the interception of communications pursuant to a warrant under this Act, and the Act allows for orders for bulk interception. It has been questioned whether this broad scheme is consistent with the requirements of the Constitution.[334]

E) OTHER LAWS AND REGULATIONS

The **Broadcasting Regulations, 2004** state that radio and television licensees must not broadcast any matter which, "measured by contemporary community standards" –

(a) offends against good taste or decency;
(b) contains the frequent use of offensive language, including blasphemy;
(c) presents sexual matters in an explicit and offensive manner;
(d) glorifies violence or depicts violence in an offensive manner; or
(e) is likely to incite or perpetuate hatred or vilify any person or section of the community on account of the race, ethnicity, nationality, gender, sexual preference, age, disability, religion or culture of that person or section of the community [335]

The inclusion of sexual preference in the last point is unusual and commendable. However, some of these prohibitions – such as the directive not to offend against good taste or decency – are vague.

The **Broadcasters' Code of Practice (2018)** reiterates these points and adds a directive not to violate contemporary community standards by broadcasting matter that is likely "to incite crime or lead to disorder".[336]

F) SIM CARD REGISTRATION

The law in Botswana requires a register of subscribers described more broadly. As noted above, the Communications Regulatory Authority Act 19 of 2012 requires regulated suppliers (telecommunications, broadcasting, internet and postal services) to maintain a register of their customers or subscribers "in such manner as the Minister may prescribe", and to provide information from this register to BOCRA or any other person designated by BOCRA. Failure to comply is It is an offence for a subscriber or a customer to fail to provide any information that the minister requires, and a

[334] Intelligence and Security Services Act 16 of 2007, sections 22, 5(1)(h) and 2 (definition of "threats to natinal security"). See Tachilisa Badala Balule, "Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework", Media Policy and Democracy Project, November 2021, pages 11-15.
[335] Broadcasting Regulations, 2004, regulation 11.
[336] Broadcasters' Code of Practice, item 1

regulated supplier that fails to comply with the rules on registers can be fined up to 10% of the net turnover of the business in the previous financial year.[337]

G) TAKE-DOWN NOTIFICATIONS

The Electronic Communications and Transactions Act 14 of 2014 makes provision for take-down notifications. A person who believes that online material has infringed a right must file a take-down notification with both the Communications Regulatory Authority and the relevant service provider (or its designated agent). Expeditious removal of material by a service provider in response to a take-down notification protects the service provider from liability for hosting, caching or linking to the material in question. However, it is not clear from the text of the provisions how the decision on whether a right is actually being infringed is made; take-down notifications are "administered" by the Communications Regulatory Authority in terms of section 44, but other provisions (sections 41 and 42) talk about actions by the service provider upon receipt of a take-down notification from an aggrieved party" while section 43 refers to removing or disabling reference or links to the electronic communication or activity in question within a reasonable time "after being informed" that it infringes the rights of a person.

A service provider bears no liability for wrongful removal of material in response to a take-down notification that complies with the legal requirements for such notices.

A person who lodges a take-down notification knowing that it materially misrepresents material facts is liable for any damages resulting from a wrongful take-down.[338]

4.5 ELECTION LAW AND FREEDOM OF EXPRESSION

General elections are expected to take place in Botswana in October 2024. Candidates for the National Assembly must state on the ballot paper which candidate they support for President, and the President is subsequently elected by the newly elected members of the National Assembly following general elections.[339]

The Constitution provides for an **Independent Electoral Commission (IEC)** selected by the Judicial Service Commission and a **Secretary** to the IEC appointed by the President.[340]

[337] Id, section 50(3)-(5).
[338] Electronic Communications and Transactions Act 14 of 2014, section 44 read with sections 41-43.
[339] Botswana's 1966 Constitution with amendments through 2016, Article 32.
[340] Id, Articles 65A and 66.

BOTSWANA CONSTITUTION

65A. APPOINTMENT OF INDEPENDENT ELECTORAL COMMISSION

1. There shall be an Independent Electoral Commission which shall consist of –
a. a Chairman who shall be a judge of the High Court appointed by the Judicial Service Commission;
b. a legal practitioner appointed by the Judicial Service Commission; and
c. five other persons who are fit, proper and impartial, appointed by the Judicial Service Commission from a list of persons recommended by the All Party Conference.

2. Where the All Party Conference fail to agree on all or any number of persons referred to in subsection (1)(c) of this section up to dissolution of Parliament, the Judicial Service Commission shall appoint such person or persons as are necessary to fill any vacancy.

3. For the purposes of this section, "All Party Conference" means a meeting of all registered political parties convened from time to time by the Minister.

4. The first appointments of the Chairman and the Members of the Commission shall be made not later than 31st January, 1999, and thereafter subsequent appointments shall be made at the last dissolution of every two successive lives of Parliament.

5. The Chairman and the members of the Commission shall hold office for a period of two successive lives of Parliament.

6. A person shall not be qualified to be appointed as a member of the Independent Electoral Commission if –
a. he or she has been declared insolvent or adjudged or otherwise declared bankrupt under any law in force in any part of the Commonwealth and has not been discharged, or has made a composition with his or her creditors and has not paid his or her debts in full; or
b. he or she has been convicted of any offence involving dishonesty in any country.

7. A person appointed a member of the Commission shall not enter upon the duties of the office of Commissioner until he or she has taken and subscribed the oath of allegiance and such oath for the due execution of his or her office as may be prescribed by an Act of Parliament.

8. The Commission shall regulate its own procedure and proceedings.

9. The Chairman shall preside over all proceedings, and in his or her absence, the legal practitioner referred to in subsection (1)(b) shall preside over the proceedings.

10. The quorum shall be four members, one of whom shall be the Chairman or the said legal practitioner.

11. All issues shall be decided by the decision of the majority of the members present and voting.

12. The Commission shall be responsible for –
a. the conduct and supervision of elections of the Elected Members of the National Assembly and members of a local authority, and conduct of a referendum;
b. giving instructions and directions to the Secretary of the Commission appointed under section 66 in regard to the exercise of his or her functions under the electoral law prescribed by an Act of Parliament;
c. ensuring that elections are conducted efficiently, properly, freely and fairly; and d. performing such other functions as may be prescribed by an Act of Parliament.

13. The Commission shall on the completion of any election conducted by it, submit a report on the exercise of its functions under the preceding provisions of this section to the Minister for the time being responsible for matters relating to such elections, and that Minister shall, not later than seven days after the National Assembly first meets after he or she has received the report, lay it before the National Assembly.

66. Appointment of Secretary to Independent Electoral Commission

1. There shall be a Secretary to the Independent Electoral Commission referred to in section 65A (in this section referred to as "the Secretary").

2. The Secretary shall be appointed by the President.

3. The functions of the Secretary shall, subject to the directions and supervision of the Independent Electoral Commission, be to exercise general supervision over the registration of voters for elections of –
a. the Elected Members of the National Assembly; and
b. the members of any local authority, and over the conduct of such elections.

4. A person shall not be qualified to be appointed as Secretary to the Independent Electoral Commission if –
a. he or she is not a citizen of Botswana;
b. he or she has been declared insolvent or adjudged or otherwise declared bankrupt under any law in force in any part of the Commonwealth and has not been discharged, or has made a composition with his or her creditors and has not paid his or her debts in full; or
c. he or she has been convicted of any offence involving dishonesty in any country.

5. A person shall not enter upon the duties of the office of Secretary until he or she has taken and subscribed to the oath of allegiance and such oath for the

due execution of his or her office as may be prescribed by an Act of Parliament.

6. For the purposes of the exercise of his or her functions under subsection (3) of this section, the Secretary may give such directions as he or she considers necessary or expedient to any registering officer, presiding officer or returning officer relating to the exercise by that officer of his or her functions under any law regulating the registration of voters or the conduct of elections, and any officer to whom directions are given under this subsection shall comply with those directions.

7. Subject to the provisions of this section, a person holding office as Secretary shall vacate that office on attaining the age of 65 years or such other age as may be prescribed by an Act of Parliament.

8. A holder of the office of Secretary may be removed from office only for inability to perform the functions of his or her office (whether arising from infirmity of body or mind or from any other cause) or for misbehaviour, and shall not be so removed except in accordance with the provisions of this section.

9. If the President considers that the question of removing the Secretary ought to be investigated then –

a. he or she shall appoint a tribunal which shall consist of a Chairman and not less than two members who hold or have held high judicial office;

b. the tribunal shall enquire into and report on the facts thereof to the President and advise the President whether the Secretary ought to be removed from office under this section for inability to perform the functions of his or her office or for misbehaviour.

10. Where a tribunal appointed under subsection (9) advises the President that the Secretary ought to be removed for inability to perform the functions of his or her office or for misbehaviour, the President shall remove him or her from office.

11. If the question of removing the Secretary from office has been referred to a tribunal under subsection (9) of this section, the President may suspend him or her from performing the functions of his or her office, and any such suspension may at any time be revoked by the President and shall cease to have effect if the tribunal advises the President that the Secretary ought not to be removed from office.

Brief background information on previous elections can be found in the 2022 Bertelsmann Transformation Index:

> *Botswana held its 12th general elections in October 2019. To date, the Botswana Democratic Party (BDP) has won each of these 12 elections. In 2019, under the leadership of President Mokgweetsi Masisi, who succeeded Ian Khama in April 2018, the BDP slightly increased its vote share to 53% from 47% in the 2014 elections. Although international observers declared the elections free, although not entirely fair, the opposition claimed that the elections had been fraudulent and contested the results for several constituencies in court without success.*
>
> *Despite having maintained a level of political and economic transformation that has delivered palpable benefits to the majority of the population, challenges persist. Botswana's transformation toward a mature economy has been slow, in part because of sluggish economic diversification and declining revenue from minerals, particularly diamonds. Botswana's economic vulnerabilities were exposed during the 2008–2009 Great Recession and again following the emergence of the COVID-19 pandemic in 2020. The main effect of the COVID-19 crisis on Botswana has been a reduction in global demand for the primary commodities on which Botswana's economy depends.*
>
> *Several constraints on press freedoms and the occasional arbitrary executive action have continued. State media has remained tightly controlled by the Office of the President. However, in 2018, 2019 and 2020, state media covered the leader of the opposition's response to President Masisi's State of the Nation Address – a development that would not have been possible under former President Khama. When President Mokgweetsi Masisi succeeded Ian Khama on April 1, 2018, there was a sense of optimism that the fear that had gripped the country under Khama was waning, as Khama had been considered an intolerant president. However, Masisi has also proven to be intolerant of his opponents. Furthermore, matters of dubious legality have continued, leading some to doubt Masisi's commitment to combating corruption and protecting the rule of law. The land rights of and development challenges facing indigenous people in the Kalahari Desert, the San (also called "Basarwa" or "Bushmen"), remain unresolved. The challenges posed by social risks, particularly increasing youth unemployment, present a serious threat to Botswana's long-term economic, political and social stability.*
>
> *The BDP's political dominance has persisted, despite the 2010 and 2019 party splits that led to the formation of the Botswana Movement for Democracy (BMD) and Botswana Patriotic Front (BPF). Subsequent to Masisi becoming president, a dispute between Masisi and Ian Khama erupted. The dispute between the two leaders could destabilize the country and its institutions. This dispute eventually led Khama to quit the BDP and join the BPF as its figurehead, citing President Masisi's intolerance of opposition. Furthermore, Khama publicly campaigned for the opposition UDC, which led to his former party losing one of its major strongholds, Central District, where Khama had been a chief.*[341]

[341] "Botswana Country Report 2022", Bertelsmann Transformation Index (BTI), Bertelsmann Stiftung, "Executive Summary".

Elections in Botswana are governed by the **electoral law contained in Chapter 02:09 of the laws of Botswana**.[342] Neither the law in force nor press reports on amendments to the electoral law proposed in 2023 mention the media or freedom of expression during election campaigns.

The **Broadcasters' Code of Practice (2018)** contains some guidelines for broadcasting during an election period.[343]

BROADCASTERS' CODE OF PRACTICE (2018)

9. Prohibition on Party-Political Broadcasts

9.1 The Licensee shall not permit party-political broadcasts under any circumstances except during an election period.

9.2 The Licensee shall not permit party-political adverts under any circumstances.

10. Elections

10.1 Party-political broadcasts;

10.1.1 the Licensee shall be required to air contesting party-political broadcasts, affording all contesting political parties similar opportunities.

10.2 Equitable treatment of political parties by Licensees;

10.2.1 if, during an election period, the programming of any Licensee extends to the elections, political parties and issues relevant thereto, the Licensee shall provide reasonable opportunities for the discussion of conflicting views and shall treat all political parties equitably.

10.2.2 In the event of any criticism against a political party being levelled in a particular programme of any Licensee without such party having been afforded an opportunity to respond thereto in the same programme or without the view of such political party being reflected therein, the Licensee concerned shall afford such party a reasonable opportunity to reply to the criticism.

10.2.3 If, within 48 hours before the commencement of the polling period, a Licensee intends broadcasting a programme in which a particular political party is criticised, the Licensee shall afford the political party a reasonable opportunity to reply thereto in the same programme, or as soon as is reasonably practicable and before polling day.

10.2.4 The opportunity to reply referred to in paragraphs 10.2.2 and 10.2.3 (above) shall be broadcast with the same degree of prominence and, where applicable, in substantially the same timeslot as the initial criticism.

[342] A clear and searchable copy of this law can be found here, but it is amended only up to 2008. A less clear copy that is not searchable, but contains amendments up to 2012, can be found here on the website of Botswana's Independent Electoral Commission.

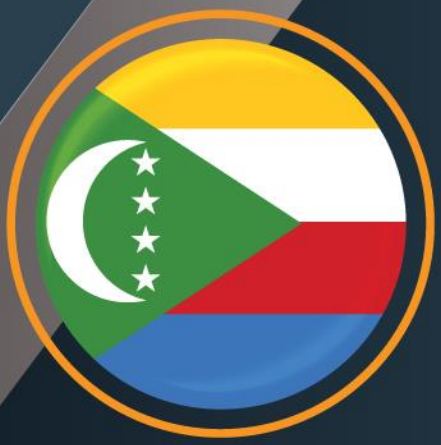
Press reports discuss an *Electoral (Amendment) Bill No. 6 of 2023*. A copy of the Bill appears to be available here, but only to subscribers. See "Morwaeng Tables Electoral Act Amendment Bill 2023", *Daily News*, 30 March 2023; "Electoral Act Amendment Imminent", *Africa Press*, 24 February 2023.

[343] Broadcasters' Code of Practice, item 1.

In accordance with the Authority's Complaints Handling Procedure, if the audience has been aggrieved by the broadcaster not adhering to this code while providing the broadcasting service, the audience is required to raise the complaint first with the Station Manager. In the event that the complaint is not resolved to the audience's satisfaction, then it should be escalated to BOCRA.

CHAPTER 5

COMOROS



CHAPTER 5: COMOROS

COMOROS KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **75th Globally; 16th out of 48 African Countries** "In this Indian Ocean archipelago with a population of less than 1 million, journalists are still often subjected to intimidation and arrest, especially during elections."
MALABO CONVENTION: Signatory but NOT party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Comoros' 2018 Constitution **ARTICLE 21** The right to liberty is inviolable. The freedom of thought and of expression, of association, of intellectual, artistic or cultural creation, of protest and the other freedoms consecrated by the Constitution, the laws and by the international law received within the juridical internal order, are guaranteed. **ARTICLE 28** Freedom of information, communication, and the press are guaranteed within the conditions established by law.
KEY LAWS: • Loi N°21-012/AU : Cyber Sécurité et à la Lutte contre la Cybercriminalité (Cybersecurity and the Fight against Cybercrime) • Loi N°20-038/AU: Code Pénal (Penal Code) (Chapter VI) • Loi n°21-011/AU: Code de l'Information et de la Communication en Union des Comores (Code on Information and Communication in the Union of Comoros; not available online as of mid-2023)
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: Comoros does not have a dedicated data protection law.[344]
ACCESS TO INFORMATION: Comoros does not have access to information law.

[344] A draft data protection law dated 2014 does not appear to have been enacted: Loi n°14-029/AU Portant protection des données à caractère personne, which can be downloaded here.

THIS CHAPTER WAS PREPARED WITH THE AID OF VARIOUS ONLINE TRANSLATION TOOLS.

5.1 CONTEXT

The following are some of the key laws and institutions relevant to the media and Information and Communications Technology in Comoros.[345]

The **National Press and Audiovisual Council (CNPA)** is the nation's independent public media regulatory authority. According to its website, in addition to its regulatory functions, it protects the rights of media professionals to carry out their work in freedom and security, helps to develop the country's media sector, and strives to improve working conditions in the media field. More specifically, it carries out these tasks:

- ensuring compliance with the law by press and audiovisual communication companies.
- deciding on requests by audiovisual communication companies for authorization.
- coordinating with ANRTIC with regard to the allocation of radio frequencies intended for audiovisual communication services, ensuring that priority is given to the satisfaction of public service missions.
- concluding agreements with audiovisual communication companies and monitoring compliance with them.
- ensuring amicable arbitration in the event of conflicts relating to freedom of expression and conscience between press companies or audiovisual communication companies and their journalists.
- ruling on disputes regarding the right of reply.
- taking care to guarantee freedom of expression and the pluralism of ideas and opinions, in particular with regard to programs relating to public affairs.
- ensuring pluralism of information during the electoral period.
- participating in the Inter-institutional Coordination Committee on issues related to the electoral cycle.
- where appropriate, penalizing offences committed by audiovisual communication companies.[346]

[345] A more detailed overview of the laws, policies and institutions relating to Information and Communications Technology in Comoros can be found here (last updated 23 May 2023).
[346] "Conseil National de la Presse et de l'Audiovisuel website", home page and "Nos Principes".

DECLARATION OF DUTIES AND RIGHTS OF JOURNALISTS

CNPA, 10 NOVEMBER 2014

The right to information, free expression and criticism is one of the fundamental freedoms of every human being.

This right of the public to know facts and opinions stems from all the duties and rights of journalists.

The responsibility of journalists vis-à-vis the public takes precedence over any other responsibility, in particular with regard to their employers and the public authorities. The mission of information necessarily includes limits that the journalists themselves impose spontaneously. Such is the object of the declaration of duties formulated here.

But these duties can only be effectively respected in the exercise of the profession of journalist if the conditions of independence and professional dignity are achieved. This is the object of the declaration of rights which follows.

The essential duties of the journalist, in researching, writing and commenting on events, are:

1. to respect the truth, whatever the consequences for himself, and this, because of the right that the public has to know;
2. to defend freedom of information, commentary and criticism;
3. publish only information whose origin is known or accompany it, if necessary, with the necessary reservations; not to delete essential information and not to alter texts and documents;
4. not to use unfair methods to obtain information, photographs and documents;
5. undertake to respect the privacy of individuals;
6. rectify any published information that proves to be inaccurate;
7. maintain professional secrecy and not disclose the source of information obtained confidentially;
8. refrain from plagiarism, slander, defamation, baseless accusations as well as from receiving any advantage due to the publication or deletion of information;
9. never confuse the job of journalist with that of advertiser or propagandist; not to accept any instructions, direct or indirect, from advertisers;
10. refuse any pressure and accept editorial instructions only from editors.

Any journalist worthy of the name makes a point of strictly observing the principles set out above; recognizing the law in force in each country, the journalist accepts, in matters of professional honour, only the jurisdiction of his peers, to the exclusion of any governmental or other interference.

1. Journalists claim free access to all sources of information and the right to investigate freely on all the facts that condition public life. The secrecy of

public or private affairs can in this case be opposed to the journalist only by exception based on clearly expressed reasons.

2. The journalist has the right to refuse any subordination that would be contrary to the general line of his business, as determined in writing in his contract of employment, as well as any subordination that would not be clearly implied by this general line.
3. The journalist cannot be forced to perform a professional act or to express an opinion that would be contrary to his conviction or his conscience.
4. The editorial team must be informed of any important decision likely to affect the life of the company. It must at least be consulted, before a final decision, on any measure affecting the composition of the editorial staff: hiring, dismissal, transfer, and promotion of journalists.
5. In consideration of his function and his responsibilities, the journalist is entitled not only to the benefit of collective agreements, but also to a personal contract ensuring his material and moral security as well as a remuneration corresponding to the social role which is his and sufficient to guarantee its economic independence.

The Declaration also includes aa additional section on the duties of journalists during election campaigns.

The **National Regulation Authority of Information and Communications Technology (ANRTIC)** regulates ICT in Comoros. It approves tariffs, enforces fair competition, promotes low prices, manages frequencies, approves equipment, ensures operators' compliance with legislation, and promotes the interests of consumers.[347] ANRTIC describes its mission as follows:

- Enforce and respect the ICT law.
- Guarantee healthy and fair competition between operators.
- Strengthen regulations in the sector.
- Regulate the ICT sector, promote cooperation between players and manage disputes.
- Defend consumers who use ICT services.
- Develop the sector to create wealth, employment and fight against poverty and inequality.
- Develop research, training and technological innovations.[348]

According to the Law on Electronic Communications, ANRTIC is "legally distinct and functionally independent from the Ministry in charge of electronic communications"[349]

[347] "Comoros: National Regulation Authority of Information and Communications Technology (ANRTIC)", Global Edge, undated. ANRTIC is established by "Le Décret N°09-065/PR du 20 mai 2009, portent creation, organisation et fonctionnement de l'Autorité Nationale de Régulation des Technologies de l'Information et de la Communication".
[348] ANRTIC website, "Missions". The key law enforced by ANRTIC is Le Décret n°14-197/PR portant promulgation de la loi n°14-031/AU du 17 mars 2014 relative aux communications électroniques (Decree No. 14-197/PR promulgating Law No. 14-031/AU of March 17, 2014 relating to electronic communications).
[349] Loi N°14-031, Article 6. The organization and functioning of ANRTIC are set by decree. Id, Article 7.

One of the key laws in the media sector is the **2021 Code of Information and Communication of the Union of Comoros**,[350] which was promulgated in January 2022. This law regulates journalists and sets out their qualifications, duties, and rights. It establishes a system of press cards for journalists, and reportedly strengthens journalists' right to protect confidential sources. It also provides a right for journalists to establish professional associations to assist them when they have been abused for exercising their profession.[351]

A journalist is defined in this Code as a natural person whose main occupation is regular and remunerated journalism in one or more press or audiovisual communication companies, where the person derives the main part of his or her income from this work.[352] Journalists who fall within this category can be issued with a professional press card by a national press card allocation commission which is to be set up by the minister in charge of information on the basis of a proposal by the CNPA. The professional cards will be issued only to journalists who have been practicing the profession for six months (for those who hold a diploma in journalism) and only after one year (for those who hold at least baccalaureate level qualification or equivalent diploma) I those with less experience can be issued with a "trainee journalist card". Other criteria and terms of allocation for the press cards are set by ministerial decree.[353]

The law strengthens journalists' right of access to sources of information,[354] as well as protecting legally recognized media personnel from pressure to disclose their sources.[355] On the flip side, it requires all journalists to respect and observe the professional ethics set out in the professional charters in force in the Comoros. Journalists must not publish information that is of a nature to undermine "human dignity, national security, unity and territorial integrity" (amongst other things). They also have a duty to publish information and comments "whose veracity and accuracy are established" and must refrain from publishing anything that incites hatred or discrimination, or advocates crime or separatism. Journalists must also respect and protect the rights of minor children, and refrain from revealing their identity and publishing their photos "in cases that undermine their dignity or are likely to harm their interests".[356]

The law also requires public authorities to guarantee to journalists their personal security and the security of their working material, as well as legal protection and respect for their dignity in the exercise of their profession. Journalists have the explicit the right to be assisted by professional organizations in the event that they is the victim of abuse in the exercise of their profession.[357]

---

[350] Le décret n°22-002/PR portant promulgation de la loi n°21-011/AU du 08 juin 2021 portant "Code de l'Information et de la Communication en Union des Comores".
[351] "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A. Because the text of the law could not be sourced online, the discussion here is based on the summary of the law in Chamsoudine Said Mhadji, "Code de l'information et de la communication I Les qualités, les devoirs et les droits d'un journaliste, selon la loi", *Al-watwan,* 21 January 2022.
[352] Loi n°21-011/AU du 08 juin 2021, Article 153
[353] Id, Articles 154-155.
[354] Id, Article 158: "in the exercise of his profession, the professional journalist has free access to sources of information".
[355] Id, Article 159: "the journalist is not required to disclose his sources and cannot, in this case, be troubled by the public authority".
[356] Id, Articles 161, 163.
[357] Id, Article 166.

5.2 CONSTITUTION

Although the Constitution protects freedom of expression as well as freedom of information, communication, and the press "within the conditions established by law", no illustrations of the application of these rights were located.[358] The Constitution does not enumerate the acceptable grounds for legal restrictions on these rights. Furthermore, since Comoros is one of the few countries in the world (and the only SADC country) that has *not* ratified the International Covenant on Civil and Political Rights (ICCPR),[359] the limits on the restriction of freedom of expression set out in Article 19 of that treaty would not necessarily be applicable.

Interestingly, the Constitution gives the State a duty to promote "the diffusion and the utilization of new technologies".[360] It also states that the law determines the fundamental principles "of information and of the New Technologies of Communication and Information".[361]

In general, it has been reported that Comoros has a weak rule of law.[362] According to Freedom House, the judicial system "is based on both Sharia (Islamic law) and the French legal code. Though the law establishes mechanisms for the selection of judges and attorneys, the executive often disregards these and simply appoints people to their positions. Court decisions are not always upheld."[363]

5.3 CASE STUDIES

Reporters Without Borders provides the following snapshot of the state of the media in Comoros:

> *La Gazette des Comores, a privately owned daily, and the state-owned Al Watwan newspaper are very popular. But a great deal of news and information circulates online, especially on social media, where people can be more outspoken although the reporting often falls far short of meeting journalistic standards. The Office de Radio et Télé des Comores (ORTC), the only public, free and national TV channel, is regarded as pro-government but has a large audience.*
>
> *Accustomed to controlling state media, succeeding governments have yet to come to terms with freedom of expression in the privately owned media, making censorship and arrests of journalists and bloggers still common. When the finance minister took office in 2021, he threatened to use "thugs" to "rip to pieces" any journalists who*

[358] The 2018 Constitution abolished the Constitutional Court, which was previously the country's highest judicial authority. Its duties have been transferred to a new Supreme Court chamber. "Comoros: Country Strategy Paper 2021-2025, Revised Version", African Development Bank Group, paragraph 2.1.1; "Freedom in the World 2022: Comoros", Freedom House, section A3.
[359] See the ICCPR status list maintained by the UN Treaty Body Database here.
[360] Comoros' 2018 Constitution, Article 8.
[361] Id, Article 91.
[362] See, for example, "Towards A More United & Prosperous Union of Comoros: Systematic Country Diagnostic", World Bank Group, [2019].
[363] "Freedom in the World 2022: Comoros", Freedom House, section F1.

criticised him. A few months before that, the president's communications coordinator, a renowned former journalist, recognised the existence of a "political culture that will have to change radically."

Although the 2001 Constitution, revised in 2018, guarantees press freedom, Comorian journalists routinely censor themselves because of the heavy penalties for defamation. A new information law was adopted in 2021 and a journalistic ethics commission was created. But, despite these provisions, journalists are still often pressured to reveal their sources while in police custody.

It is hard for media outlets to make a profit, and this undermines their independence. When state subsidies are issued, preference is given to state-owned media that support the government. It's often difficult for privately owned media to pay their journalists, which encourages recourse to advertorials and other forms of sponsored content presented as regular reporting.
As conservative religious influence is on the wane, the media increasingly cover subjects related to sex and prostitution, with the public's support.[364]

According to the US State Department's 2022 report on human rights practices in Comoros, the country is marked by "serious restrictions on free expression and media, including violence, threats of violence, and unjustified arrests or prosecutions against journalists".[365] This report goes on to say that individuals are not free to criticize the government or raise matters of public interest without constraint, given that authorities reportedly detain individuals for making public statements, including online statements, that are critical of the President. Some journalists were apparently subjected to harassment by government authorities due to their reporting, causing some to exercise self-censorship to avoid reprisals. [366] Self-censorship is also practised to avoid the heavy penalties that are imposed for defamation.[367]

In 2023, four journalists **were charged with "defamation and insult" by an executive of the Comoros Radio and Television Office (ORTC). The four are Andjouza Abouheir** of *La Gazette des Comores*, *RFI (Radio France Internationale),* correspondent **Abdallah Mzembaba** and **Oubeidillah Mchangama** of *Facebook FM Comores, and* **Toufé Maecha**, news director of the Comoros Radio and Television Office (ORTC) and president of the local section of the International Francophone Press Union. The origin of the case was a public allegation by Andjouza Abouheir that an ORTC executive had acts of "sexual violence" committed by against women journalists working at the national television station. Abdallah Mzembaba was accused of defamation for reporting on Abouheir's statements, without mentioning the name of the executive who was the alleged perpetrator. Toufé Maecha was suspected of being the instigator of the allegations. The legal proceeding against the journalists was not resolved as of mid-2023 but was deflecting attention from the alleged sexual violence.[368]

[364] "2023 World Press Freedom: Comoros", Reporters Without Borders.
[365] "2022 Country Reports on Human Rights Practices: Comoros", US State Department, Executive Summary.
[366] "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.
[367] "2023 World Press Freedom: Comoros", Reporters Without Borders, "Legal Framework".
[368] "Comoros: RSF denounces the abusive judicial proceedings against four journalists?", Reporters Without Borders, 21 June 2023; "2023 World Press Freedom: Comoros", Reporters Without Borders, "Safety".

In 2021, gendarmerie officers arrested **Oubeidillah** Mchangama, a reporter with the Facebook-based news outlet *FCBK FM*, after he reported on a protest in the capital city of Moroni. Another reporter and camera operator, Mkouboi, was also arrested. Both were released but had to appear in court on **charges of participating in protests against the government**. This move was understood to be a form of intimation to discourage reporting on protests and other issues of public interest.[369]

Oubeidillah Mchangama was also arrested in December 2020, in relation to FCBK FM post about a potential gas shortage, which authorities allege **disturbed "public order".** However, this arrest warrant was dropped by the court and his detention in custody was prolonged in relation to another post about alleged government mismanagement of public funds, which the court said constituted **spreading false news in violation of Article 254 of the Penal Code**,[370] according to the court. While this charge was under investigation, he was held under a judicial control order that included instructions forbidding him from making declarations to the media or publishing messages on social media.[371]

Earlier in 2020, two senior journalists - news director Binti Mhadjou and editor-in-chief Moinadjoumoi Papa Ali – were **suspended** from the Comoros public radio and television broadcasting station *ORTC*, for their allegedly biased coverage of a strike. According to Mhadjou, the government thought that the *ORTC* had given "too much time to the strikers", who were merchants protesting against hikes in customs duties and a lack of transparency in the way duties are charged. An official with Reporters Without Borders stated that the incident illustrates that the Comorian government still wants to exercise very close control over the public TV broadcaster, which had only just begun providing more independent coverage and a diversity of viewpoints.[372]

In the midst of the Covid pandemic, in 2020, journalist **Andjouza Abouheir wrote a report revealing that** samples taken from six persons suspected of being infected with Covid-19 were not sent for analysis – which could have explained why Comoros had no confirmed coronavirus cases. She was accused by government authorities of "**disinformation**", and a government spokesman threatened to bring legal proceedings against all journalists who published information about the pandemic without going through official channels". At the same time, the public health department contacted Abouheir to demand the identity of her source for the story.[373]

In 2019, Oubeidillah Mchangama was arrested along with another reporter for the Facebook news page FCBK FM, Abdallah Abdou Hassane, and held in pretrial detention on an array of charges for over a month. They were charged with **defamation**, **disturbing public order**, **incitement to violence**, **offense against the head of state**, **insulting the magistrate**, **forgery**, and **use of false materials**. The journalists had

[369] "Comorian journalists detained, accused of participating in protests", Committee to Protect Journalists, 21 January 2021. Two dates appear on this article: 21 January 2021 and 21 January 2020; it is not clear which date is correct.
[370] At that time, the relevant law was the Penal Code, "Loi N°- 082 P/A.F - Loi 95-012/AF portant Code pénal (Crimes et délits)" , Article 254. A new Penal Code is now in force.
[371] "Comoros journalist Oubeidillah Mchangama held for 3 days over Facebook posts", Committee to Protect Journalists, 22 December 2020; "Heavy penalty for Comorian journalist for Facebook post if convicted", Committee to Protect Journalists, 5 January 2021.
[372] "Two senior state broadcast journalists suspended in Comoros", Reporters Without Borders, 4 February 2020.
[373] "Comoros: Journalist threatened for exposing flaws in handling of coronavirus crisis", Reporters Without Borders, 7 April 2020.

frequently criticized the government in their posts and broadcasts, and on one occasion had called on President Azali Assoumani to resign. Some suspected that their detention was intended to silence them during the 2019 election period. Protests were held in Moroni calling for the release of the two journalists.[374]

Another journalist, editor-in-chief of the privately owned daily newspaper *Masiwa Komor*, Toufé Maecha, was detained in the aftermath of the disputed 2019 presidential election. He was threatened with **espionage** charges after going to the gendarmes' station to inquire about arrests made since the election. He was interrogated and forced to undress, then eventually released without charge but warned not to talk about his experience in custody.[375]

Three privately-owned newspapers (*La Gazette des Comores, Al-Fajr and Masiwa Komor)* had their print runs for specific days seized before they could reach newsstands in 2019 because they carried reports related to post-election disputes.[376]

Authorities reportedly monitored social media during the 2019 presidential campaign and shut down telecommunications services for one day in March 2019.[377]

5.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

Comoros has two recent laws on cybercrime that overlap to some extent: extensive provisions on cybercrime in Chapter VI of the 2021 **Penal Code** (Law 20-038, which was promulgated in 2021),[378] and the 2022 **Law on Cyber Security and the Fight against Cybercrime** (Law 21-012, which was promulgated in 2022)[379]

The Law on Cyber Security and the Fight against Cybercrime states that the provisions in the Penal Code and the Code of Criminal Procedure apply to offences in connection with that law, insofar as they are not contrary to its provisions.[380] This discussion will first summarise the cybercrime provisions in the Penal Code, since the Penal Code was enacted first and since it takes precedence in the absence of a direct conflict between the two laws. In fact, the Law on Cyber Security and the Fight against Cybercrime states that its cybercrime provisions are intended to strengthen and supplement the provisions of the Penal Code.[381]

[374] "Two journalists held in pretrial detention since February in Comoros", Committee to Protect Journalists, 26 March 2019.
[375] "Comoros authorities detain journalist, censor newspapers amid political crisis", Committee to Protect Journalists, 10 April 2019.
[376] Id.
[377] "Freedom in the World 2022: Comoros", Freedom House, section D4.
[378] Decret n° 21-018/PR portant promulgation de la loi n°20-038/AU du 29 décembre 2020, portant Code Pénal. The Penal Code contains Chapter IV (Articles 449-505) on cybercriminality ("*la cybercriminalité*").
[379] Decret n° 22-003/PR portant promulgation de la loi N°21-012/AU du 25 juin 2021 relative à la Cyber Sécurité et à la Lutte contre la Cybercriminalité en Union des Comores.
[380] Loi N°21-012/AU, Article 150.
[381] Id, Article 1.

The provisions in both the Penal Code and the Law on Cyber Security and the Fight against Cybercrime are untitled, but titles have been added to the tables below for ease of reference.

A) CYBERCRIMINALITY IN THE PENAL CODE

In terms of Article 449 of the Penal Code, "cybercrime" is defined to include a list of acts for the purposes of the law.[382] These are not definitions in the usual sense, as the items listed under the umbrella of "cybercrime" are not connected to specific terms used in the law. In general, cybercrime refers to "all criminal offences committed by means of or on a telecommunications network or an information system". Other manifestations of cybercrime set out in this list are referenced in the tables below where they seem most relevant.

CYBERCRIMINALITY IN THE PENAL CODE - TECHNICAL OFFENCES	
Article 450: Illegal dealings in cryptology	It is an offence to fail to declare to the ministry in charge of electronic communication the supply, transfer, import or export of a means of cryptology. The penalty is 5 years imprisonment and a fine. It is an offence to export a means of cryptology without previous authorization from the competent authority when such authorization is required. The penalty is 2 to 4 years imprisonment and a fine. It is an offence to sell or rent a means of cryptology that has been the subject of an administrative ban on circulation. The penalty is 2 to 4 years imprisonment and a fine. It is an offence to provide cryptology services aimed at ensuring confidentiality functions without authorization from the competent authorities. The penalty is 3 to 5 years imprisonment and a fine. o Article 449 indicates that cryptology refers to "any hardware or software designed or modified to transform data, whether information or signals, using secret keys or to perform an inverse operation with or without a secret key". It notes further: "These means of cryptology are mainly intended to guarantee the security of the storage or transmission of data, by making it possible to ensure their confidentiality, their authentication or the control of their integrity." o No specific defences are articulated. o Note that there are also rules about cryptology in Chapter IV of the Law on Cyber Security and the Fight against Cybercrime.
Article 451: Fraudulent access	It is an offence to fraudulently access or attempt to access all or part of an information system. The penalty is 1 to 2 years imprisonment and a fine. o Note that "mere access" is criminalised, without more – unless the requirement that this be done "fraudulently" ("*frauduleusement*") adds an additional element of wrongdoing.

[382] Penal Code, Article 449.

	○ No specific defences or justifications are articulated. ○ This offence overlaps with Article 373, which makes it an offence to fraudulently accessed or remains in all or part of *an automated data processing system*, punishable by imprisonment for 2 months to 1 year and a fine, or one of these penalties only. There are enhanced penalties where the access results in the deletion, modification or appropriation of data contained in the system, or an alteration of the operation of the system.
Article 452: Fraudulent remaining	It is an offence to remain or attempt to remain fraudulently in all or part of an information system. The penalty is 1 to 3 years imprisonment and a fine. ○ It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorized access.[383] ○ No specific defences or justifications are articulated. ○ This offence overlaps with Article 373, described in the row above.
Article 453: Unlawful interference with information system	It is an offence to obstruct, distort or attempt to obstruct or fraudulently distort the operation of an information system. The penalty is 3 to 5 years imprisonment and a fine. ○ No specific defences or justifications are articulated. ○ This offence overlaps with Article 374, which makes it an offence, intentionally and disregarding the rights of others, to obstruct or distort the operation of *an automated data processing system*. The penalty is 3 months to 3 years imprisonment and a fine, or only one of these two penalties.
Article 454: Fraudulent introduction of computer data	It is an offence to fraudulently introduce or attempt to introduce data into an information system. The penalty is 3 to 5 years imprisonment and a fine. ○ No specific defences or justifications are articulated. ○ A related provision is Article 376, which makes it an offence to falsify computerized documents, whatever their form, where this is likely to cause harm to others. The penalty is 1 to 5 years imprisonment and a fine. Under Article 377, knowingly making use of such falsified documents is also an offence punishable by 1 to 5 years imprisonment and a fine.
Article 455: Unlawful data interception	It is an offence to fraudulently intercept or attempt to intercept computer data by technical means during their non-public transmission to, from or within an information system. The penalty is 5 to 10 years imprisonment and a fine. ○ No specific defences or justifications are articulated.
Article 456: Unlawful data interference	It is an offence to fraudulently alter or attempt to alter, modify or attempt to modify, delete or attempt to delete computer data. The penalty is 5 to 10 years imprisonment and a fine. ○ No specific defences or justifications are articulated.

[383] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	○ This offence overlaps with Article 375, which makes it an offence, intentionally and disregarding the rights of others, directly or indirectly, to introduce data into *an automated processing system* or to delete or modify the data it contains or their processing or transmission methods. The penalty is imprisonment for 3 months to 3 years and a fine, or only one of these two penalties.
Article 457: Deception	It is an offence to produce or manufacture a set of data by the introduction, modification, alteration or deletion of computer data, resulting in counterfeit data, with the intention that they be taken into account or used for legal purposes as if they were original. The penalty is 5 to 10 years imprisonment and a fine.
Article 458: Use of fraudulently obtained computer data	It is an offence to knowingly use computer data that was fraudulently obtained. The penalty is 1 to 5 years imprisonment and a fine. ○ This offence could affect public access to information acquired by a whistleblower or placed in a cache such as Wikileaks. There is no exception for lawful excuse or acting in the public interest.
Article 459: Computer-related extortion	It is an offence to fraudulently obtain any advantage whatsoever, for oneself or others, by the introduction, use, modification, alteration or deletion of computer data or by any form of attack on an information system. The penalty is 1 to 5 years imprisonment and a fine.
Article 460: Fraudulent devices	It is an offence, with the intention of committing one of the offences provided for by this law, to knowingly produce, sell, import, hold, distribute, offer, transfer or make available - • equipment, a device or a computer program • a password, an access code or similar computer data. The penalty is 1 to 2 years imprisonment and a fine. ○ The required intention helps to narrow the offence appropriately.
Article 466: Identity-related offences	It is an offence. • to fraudulently use one or more identification elements of a natural or legal person through an information system. • to knowingly use, possess, offer, sell, make available or transmit false identification data. • to make or attempt to make false identification data. The penalty for any of these offences is 2 to 5 years imprisonment and a fine.
Article 467: Cryptology offences	It is an offence to fail to comply with the ban on exercising the profession of cryptology service provider or the obligation to withdraw the means of cryptology. The penalty is 1 to 5 years imprisonment and a fine. ○ This offence seems to be related to Article 450, which is discussed above.
Articles 468-470: Theft of information	It is an offence to - • fraudulently acquire knowledge of information within an electronic information system. • fraudulently copy information from such a system; or • fraudulently remove the physical medium on which information is located.

	• attempt to do any of these acts. The penalty is 5 to 10 years imprisonment and a fine. There is an enhanced penalty where the theft or attempted theft of information was accompanied by at least one of the following circumstances: • with violence resulting in injury; • with burglary, climbing or use of a false key; • in a meeting by at least two people; • with fraudulent use of a uniform or attire of a public, civil or military official, a title of an official, or a false order from a civil or military authority; • in a house that is inhabited or used as a dwelling or in professional premises: • with the use of a mask or other form of disguise that conceals the person's true face; • with the use of a vehicle to facilitate the offence or the escape; • where the acts took place at night. There is a higher enhanced penalty (a minimum of 20 years' imprisonment and a fine) where the theft or attempted theft of information was accompanied by either of the following circumstances: • if the perpetrator or an accomplice carried a visible or hidden weapon that injured the victim. • when the injuries have led to the death of the victim. Where death resulted, the culprit can be sentenced to death or life imprisonment. o There is no explicit protection for circumstances where theft of information might be justified in the public interest, such as where information is obtained by a whistleblower.
Article 471: Misuse of devices	It is an offence, intentionally and without right – • to produce, sell, obtain for use, import, distribute or otherwise make available a device, including a computer program, primarily designed, or adapted to allow the commission of information theft; or • to use a password, an access code or similar computer data allowing access to all or part of an information system, with the intention that these items be used to commit any of the offences provided for in the chapter of the Penal Code on cybercriminality. The penalty is the same as that provided for the offence itself or for the most severely punished offence amongst multiple offences involved. o It is good practice to provide that devices in such offences be designed or adapted *primarily* for illegal purposes, because of the existence of dual-use devices.
Article 473: Interference with or interception of electronic correspondence	It is an offence, in bad faith - • to open, delete, delay or divert electronic correspondence, whether or not it has arrived at its destination and addressed to a third party. • to fraudulently acquire knowledge of such correspondence. • to intercept, divert, use or disclose electronic correspondence sent, transmitted or received via electronic communications. • to install a device designed to carry out such interception.

	The penalty is 1 to 5 years imprisonment and a fine. o Article 134 of the Penal Code provides a similar offence in respect of items sent via the postal service.

The cybercriminality chapter of the Penal Code also contains a long list of content-based offences that involve information systems.

CYBERCRIMINALITY IN THE PENAL CODE – CONTENT-BASED OFFENCES	
Article 462: Pornography and violation of dignity.	It is an offence to produce, record, offer, make available, diffuse, or publish an image or a representation presenting an erotic pornographic character or contrary to good morals by means of an information system or a means of computer data storage. The penalty is 1 to 5 years imprisonment and a fine. o Article 449 indicates that pornography covers "any data, regardless of nature or form, visually representing persons engaging in an explicit sexual act or realistic images representing persons engaging in sexually explicit conduct". The concept of "good morals" is not defined - meaning that this offence is vague and susceptible to subjective enforcement. o There is no defense for materials with a genuine artistic, educational, legal, medical, scientific, or public benefit purpose. o It appears to be no defence where the image was created between consenting adults, or where it was produced only for private use. without being shared more widely. o This is one of the few cybercrime laws in the SADC region that widely captures pornography that does not involve children. (There is also a broad provision on pornography in Tanzania's Cybercrimes Act.) o This offence dovetails with Article 299, which addresses pornography in other forms. It is an offence to produce, record or counterfeit an image, or to make available, distribute or publish a counterfeit image, a video image or a representation presenting an erotic pornography character or contrary to good morals and which undermines the dignity of a person through a computer data storage system or means. The penalty is 2 to 7 years imprisonment and a fine. o The second part of this provision covers an entirely different matter; it appears to be aimed at protecting the dignity of the person depicted in a pornographic image or an image that is "contrary to good morals". Article 449 indicates that human dignity may be undermined by "any attack, excluding attacks on life, integrity or freedom, which has the essential effect of treating the person as a thing, as an animal or as a being to which any right would be denied". o There is no explicit requirement that the image in question be produced or shared without consent (where adults are involved), although that may be implied. There is also no explicit requirement that the person in question must be identifiable in the image, but this may also be implied in the concept of undermining the person's dignity.

	○ The definitional problems cited in respect of the first part of the provision apply here as well.
Article 463: Dealing in child pornography	It is an offence to obtain or procure from others, or to import or export, an image or representation having the character of erotic child pornography through an information system, or a computer data storage means. The penalty is 2 to 5 years imprisonment and a fine. ○ Article 449 indicates that child pornography applies "any data of whatever nature or form visually representing a child under the age of eighteen engaging in sexually explicit behaviour or images depicting a child under the age of fifteen engaging in sexually explicit behaviour". ○ There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose.
Article 464: Possession of child pornography	It is an offence to intentionally possess an image or representation having the character of erotic child pornography in an information system or a means of storing computer data. The penalty is 1 to 3 years imprisonment and a fine. ○ Article 449 indicates that child pornography applies "any data of whatever nature or form visually representing a child under the age of eighteen engaging in a sexually explicit act ("*un agissement sexuellement explicite*") or images depicting a child under the age of fifteen engaging in sexually explicit behaviour ("*un comportement sexuellement explicite*"). ○ There is no defence for materials with a genuine artistic, educational, legal, medical, scientific, or public benefit purpose.
Article 465: Facilitating minor's access to pornography	It is an offence to facilitate access by a minor to images, documents, sound or a representation having the character of erotic pornography. The penalty is 1 to 5 years imprisonment and a fine. ○ Article 449 indicates that pornography covers "any data, regardless of nature or form, visually representing persons engaging in an explicit sexual act or realistic images representing persons engaging in sexually explicit conduct".
Article 475: Infringement of intellectual property	There is a list of intellectual property infringements that constitute cybercrime offences if committed by means of an information system, all punishable by 1 to 10 years imprisonment and a fine. ○ This provision supplements Articles 421-425 of the Penal Code on intellectual property infringements in general.
Articles 476-478: Unauthorised online gambling	It is an offence without authorization to organise illicit online gambling characterized by the holding of games of chance, illicit lottery, prohibited lottery advertising, or illicit betting on electronic communication networks. The penalty is 1 to 5 years imprisonment and a fine. It is also prohibited for natural or legal persons to transfer money by payment card, bank transfer or any other means of payment in the context of illicit gambling on electronic communication networks. Banking or financial institutions operating on national territory must ensure compliance with this prohibition and notify the competent authorities of any observed violation or attempted violation of this prohibition. The penalty for violation of the money

	transfer ban by a natural person is 5 years imprisonment and a fine of 5 to 10 million Comorian francs. If the penalty is incurred by a legal person, the fine is twice the amount that applies to a natural person who committed the offence. If the prohibited money transfer is made to a foreign country, the offence committed also constitutes an offence against the regulations governing external financial relations and is punishable without prejudice to the provisions of the law relating to disputes relating to exchange control offences. o These offences dovetail with Chapter V of the Penal Code on games of chance, which prohibits lotteries or any other games of chance giving the hope of a significant gain for a relatively low wager.
Article 493: Racist or xenophobic ideas or theories	It is an offence to create, distribute or make available in any form - whether writings, messages, photos, sounds, videos, drawings or any other representation - of ideas or theories of a racist or xenophobic nature by means of an information system. The penalty is 10 to 20 years imprisonment and a fine. The penalty is 2 to 5 years imprisonment and a fine. o Article 449 indicates that this prohibition would apply to "any writing, image or other representation of ideas or theories which advocates or encourages hatred, discrimination or violence against a person on the basis of national origin or religion, to the extent that the latter serves as a pretext for any of these elements, or which incites to such acts".
Article 494: Threats of death or violence	It is an offence to threaten others with death or violence through an information system. If the threat has a racist, xenophobic, ethnic or religious character, or refers to a group characterized by race, color, descent or national or ethnic origin, the penalty is higher: 10 to 20 years imprisonment and a higher fine.
Article 495: Insult	It is an offence to utter or emit any offensive expression, any term of contempt or any invective that does not contain the imputation of any fact by means of an information system. The penalty is 1 to 5 years imprisonment and a fine. Est puni de un à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs comoriens d'amende, le fait pour toute personne de proférer ou d'émettre toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un système d'information. o This vague offence is a worrying limitation on freedom of expression. It appears to apply to private online communications as well as public ones, and the undefined concepts of "offensive expression", "term of contempt" and "invective" are very broad and subjective. This is particularly concerning given the mandatory sentence of at least one year in prison. o This offence overlaps with Articles 238-240 of the Penal Code, read with Article 234 (which defines "insult" as "offensive expressions, terms of contempt or invective which do not contain the imputation of any material fact".

Article 496: Genocide or crimes against humanity	It is an offence intentionally to deny, approve or justify acts constituting genocide or crimes against humanity by means of an information system. The penalty is 3 to 5 years imprisonment and a fine. o The terms "genocide" and "crimes against humanity" are not defined but would probably be understood to have the meaning given to them in the international context.
Article 497: Disturbing public order or undermining human dignity	It is an offence to produce, make available to others or disseminate data that is likely to disturb public order or undermine human dignity through an information system. The penalty is 1 month to 5 years imprisonment and a fine. Est puni d'un mois à cinq ans d' emprisonnement et de 1.000.000 à 20.000.000 de francs comoriens d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information. o This is another vague and worrying limitation on freedom of expression. It relies on the broad and undefined concepts of "disturbing public order" and "undermining human dignity", and it appears to apply to the production of such content using a computer even if that content is never shared. o The breadth of the offence appears to be contemplated in the fact that the minimum sentence is low compared to other cybercrime offences in the Penal Code, starting at 1 month in prison. o This offence is likely to lead to self-censorship.
Article 498: Information relating to destructive devices	It is an offence, through an information system, to disseminate or otherwise make available to others, with the exception of authorized persons, instructions on how to use or manufacture means of destruction likely to harm life, property or the environment. The penalty is 1 to 5 years imprisonment and a fine.
Article 499: Information inciting suicide	It is an offence, through an information system, to disseminate or otherwise make available to others, processes or information inciting suicide. The penalty is 1 to 5 years imprisonment and a fine.
Article 500: False information on harm, disaster or emergency	It is an offence to communicate or disclose through an information system, false information - • tending to make others believe that destruction, degradation or deterioration of property or harm to persons has been committed or is about to be committed. • giving the impression of a disaster or any other emergency situation. The penalty is 6 months to 2 years imprisonment and a fine. o The international experience with Covid-19 illustrates the difficulties that could be encountered in applying this offence in practice. Another newsworthy but contentious issue that might fall under this prohibition is climate change. o The breadth of the offence appears to be contemplated in the fact that the minimum sentence is low compared to other cybercrime offences in the Penal Code, starting at 6 months in prison. o This offence is likely to lead to self-censorship.

Article 501: Threats of harm to property or persons	It is an offence to threaten to commit, by means of an information system, the destruction, degradation or deterioration of property or harm to persons, by means of writing, image, sound, video or any other data. The penalty is 5 to 10 years imprisonment and a fine. o This offence appears to overlap with Article 494 in respect of threats of harm to persons. Other cybercrime laws typically add the requirement that some benefit is requested to avert the threatened harm, making this an offence of cyber extortion.
Article 502: Treason	It is an offence for *a Comorian* to use an information system to do any of the following acts in respect of information, a document, a process or computer data which must be kept secret in the interest of National Defence – • to deliver, or to possess with a view to delivering, such material to a foreign country or a foreign natural or legal person; • to destroy or allow the destruction of such material, with a view to favouring a foreign country or a foreign natural or legal person. These acts are forms of treason and are punishable by life imprisonment.
Article 503: Espionage	It is an offence for *any person* to use an information system to do any of the following acts in respect of information, a document, a process or computer data which must be kept secret in the interest of National Defence - • to deliver, or to possess with a view to delivering, such material to a foreign country or a foreign natural or legal person; • to destroy or allow the destruction of such material, with a view to favouring a foreign country or a foreign natural or legal person. These acts constitute espionage and are punishable by life imprisonment.

The **penalties** are stiff, with every offence being punishable by a **mandatory minimum sentence of imprisonment combined with a fine**; there is no possibility of paying a fine as an alternative to a sentence of imprisonment. These penalties seem particularly heavy in comparison with those in other SADC countries.

Whenever there is a conviction for any of these offences, the following **additional penalties** also apply:

- a 5-year prohibition on exercising a public function or exercising the professional or social activity that was being exercised at the time when the offence was committed;
- confiscation of the means used to commit the offence or intended for such use;
- confiscation of property which is the proceeds of the offence;
- a 5-year closure of the establishments of the company used to commit the offending acts;
- exclusion for 5 years from public contracts;
- a 5-year prohibition on issuing certain cheques;

- publication or broadcast of the court's decision at the perpetrator's expense.[384]

A judge may also impose additional confiscations, special confiscations, deprivation of other rights or a prohibition on the right to stay in Comoros, as provided for in the Penal Code.[385]

Participating in association or agreement with others to prepare for or commit any of the offences in the cybercriminality chapter of the Penal Code is also a crime, punishable by 10 to 20 years imprisonment and a fine of 7 to 15 million Comorian francs.[386]

When any of the offences relate to **an information system or a data processing program protected by a secret access code**, the penalty incurred must be a minimum of 10 years' imprisonment.[387]

A **legal entity**, other than the State, is criminally liable for any of the cybercrime offences committed on its behalf by its representatives, without excluding the liability of any natural persons who were involved in committing the offence. The penalty for legal persons is twice the fine provided for a natural person who committed the offence.[388]

The chapter on cybercrime in the Penal Code also sets out certain obligations of service providers, which are summarised below.

Cybercafés: Certain obligations relate specifically to **cybercafés**. Those who wish to access Internet service from a cybercafé must provide identification. The details of how the identification procedure must be carried out is to be prescribed in regulations. A minor (meaning a person under age 18) must be accompanied by an adult authorized by his parents or by the person responsible for his care in order to access the Internet in a cybercafé. Internet access for minors in a cybercafé must be limited access, filtered to exclude websites of a pornographic, violent, racist or degrading nature as well as all websites that violate human dignity or incite incivility. Violation of these rules by an internet access provider is punishable by 6 to 12 months of imprisonment.[389]

Filtering requirements: Service providers who provide access to online communication services must inform their subscribers of the existence of **technical filtering options** and offer them at least one of these means. Failure to follow this rule is punishable by a fine of 1 to 10 million Comorian francs.[390]

[384] Id, Article 474.
[385] Id, Article 505.
[386] Penal Code, Article 461.
[387] Id, Article 472.
[388] Id, Article 504.
[389] Id, Article 479-481.
[390] Id, Article 482.

Other obligations of service providers: Service providers (including all those who offer access to online communication services) do not have a general duty to monitor content or to search for illegal content – but a judicial authority may require them to carry out **targeted and temporary monitoring** of the activities carried out through their services.[391]

Service providers are required to **retain data that can be used to identify persons who have contributed to the creation of content on the service for three years**, in accordance with any legal or regulatory provisions relating to the protection of personal data. A judicial authority may require the service provider to provide this identification data.[392]
Commercial service providers must also publically identify themselves online; non-commercial service providers are allowed to preserve their anonymity but must still provide certain specified information.[393]

Failure to carry out these obligations is punishable by 1 to 5 years imprisonment and a fine; if the service provider is a legal person (such as a company), the penalty applies to its manager.[394]

Take-down notifications: The Penal Code makes provision for a person to notify an internet access provider of illegal content. This notification must include a description of the content and its precise location on the network; the reasons for requesting removal of the disputed content and a copy of the correspondence addressed to the author or publisher of the content in question, requesting the interruption, withdrawal or modification of the content, or reasons why the author or the publisher could not be contacted. Making a bad faith notification of this type with the aim of achieving the withdrawal of the content or stopping its dissemination is punishable with 1 to 5 years imprisonment and a fine of 1 to 5 million Comorian francs. Once an internet access provider receives such a notification, the service provider is deemed to have knowledge of the content in question and can be held criminally liable for it if they fail to act promptly to remove it or disable access to it.[395]

Internet access providers are required to set up an easily accessible and visible system on their websites inviting members of the public to bring illegal content to their attention, and they must publically disclose the means devoted to this initiative. They are also obligated to inform the appropriate public authorities of any illegal activities reported to them. Violation of these duties is an offence punishable by 1 to 5 years imprisonment and a fine.[396]

[391] Id, Article 486.
[392] Id, Article 488.
[393] Id, Article 489.
[394] Id, Article 490.
[395] Id, Articles 483-485.
[396] Id, Article 287.

B) LAW ON CYBER SECURITY AND THE FIGHT AGAINST CYBERCRIME

The Law on Cyber Security and the Fight against Cybercrime provides a security framework for electronic communications networks. To this end, it defines and punishes offences related to the use of information and communication technologies. Its aims are to –

- establish confidence in electronic communications networks and information systems;
- set out a legal regime for digital evidence, security, cryptography and electronic certification activities;
- protect the fundamental rights of natural persons, in particular the rights to human dignity, honour and respect for private life;
- protect the rights and interests of legal persons under the law.[397]

This law creates a public institution called the **National Agency for Digital Development (**L'Agence Nationale de Développement du Numérique **(ANADEN)**.) The details of its organization are to be set by decree. Its key function is to control and monitor activities related to the security of information systems and electronic communications networks.[398] Many of the law's provisions relate to "trust services", which concern services related to electronic transactions, certificates for website authentication and regulation of encryption services.[399] It also governs "vital and critical digital infrastructure", including criteria for their identification, security plans for protecting them and procedures for dealing with digital attacks, intrusions and incidents.[400]

Like the Penal Code, this law contains both technical and content-based offences. In many instances, the later law adds more detail – particularly in respect of the technical offence. Also, some of the offences in the later law were not covered at all in the Penal Code.

LAW ON CYBER SECURITY AND THE FIGHT AGAINST CYBERCRIME - TECHNICAL OFFENCES THE TITLES ADDED HERE ARE BASED ON THE OVERARCHING TERMS APPLIED TO THE ACTS COVERED BY THE OFFENCE IN THE TEXT OF THE LAW, WHERE SUCH TERMS ARE PROVIDED.	
Article 68: Attack on information systems	It is an offence to - • infect an information and communication system; • intrude into such a system by fraudulent or irregular access or remaining in all or part of an information system; • fraudulently introduce data into all or part of an information system/ It is an offence to produce or manufacture a set of data by the introduction or generation of counterfeit data, with the intention that such counterfeit data be taken into account or used for legal purposes as if they were original.

[397] Loi N°21-012/AU, Article 2.
[398] Id, Articles 6-7.
[399] Id, Article 18.
[400] Id, Articles 53-63.

	It is an offence to fraudulently acquire, for oneself or for others, any advantage whatsoever, by the introduction of computer data or by any form of attack on the information system. o These acts appear to overlap to some extent with the following provisions of the Penal Code: Articles 451 (Fraudulent access), 452 (Fraudulent remaining), 454 (Fraudulent introduction of computer data), 457 (Deception) and 459 (Computer-related extortion).
Article 69: Attack on the integrity of information systems	It is an offence to carry out any action, intentionally and without right, directly or indirectly by any technological means, which causes an interruption of the normal operation of a computer system. The penalties differ depending on whether the result was to - • affect the integrity of an information system; • damage data in the information system concerned or in any other information system • cause a serious disturbance or prevent, totally or partially, the normal functioning of the information system concerned or of any other information system; • affect one or more sensitive and critical infrastructures. It is irrelevant whether the effect was temporary or permanent. o This offence appears to overlap with Article 453 of the Penal Code (Unlawful interference with information system).
Article 70: Attack on the integrity of data	It is an offence to carry out any action, intentionally and without right, directly or indirectly, which alters or attempts to alter, modifies or attempts to modify, deletes or attempts to delete, damages or attempts to damage, erases or fraudulently attempts to erase computer data. The penalties differ depending on the intention or result: • if the acts were committed to fraudulently gain an advantage, for oneself or for others, through the use, modification, alteration or deletion of computer data or by any form of attack on the integrity of the data; • if the acts were likely to undermine the integrity of the data; • if the acts were carried out with fraudulent intent or with the aim of causing harm; It is irrelevant whether the effect was temporary or permanent. o This offence appears to overlap with Article 456 of the Penal Code (Unlawful data interference).
Article 71: Attack on computer data	It is an offence, intentionally and without right, by technical means, to intercept or attempt to intercept, disclose, use, alter or divert, computer data during their non-public transmission from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. The penalties differ depending on the circumstances of the offence: • if the acts damage computer data; • if the acts transfer data from an information system or a means of computer data storage without authorization; • if the acts were carried out with fraudulent intent;

	• if the acts were carried out in connection with an information system connected to another information system; • if the acts were carried out by circumventing protective measures put in place to prevent access to the content of the non-public transmission. The acts in question do not constitute an offence in these circumstances: • if the interception is carried out pursuant to a court order; • the communication is sent by or is intended for a person who has consented to the interception; • an authorized officer considers that an interception is necessary in an emergency, for the purpose of preventing death, injury or damage to the physical or mental health of a person, or of mitigating injury or damage to a person's physical or mental health; • a legal or natural person was legally authorized to do the acts in question for the purposes of public security or national defence, or under the provisions of the Code of Criminal Procedure. o This offence appears to overlap with the following provisions of the Penal Code: Articles 456 (Unlawful data interference) and 455 (Unlawful data interception).
Article 72: Computer sabotage	It is an offence – • to transmit or modify data without authorization; • to falsify or conceal data recorded on any information system; • to erase or destroy data and software; where this also hinders access to an information system. The penalties differ depending on the circumstances of the offence: • if the acts hinder or distort the operation of an information system (or attempt to do so); • if the acts alter, modify or delete computer data (or attempt to do so); • if the acts produce or manufacture a set of data by the modification, alteration or fraudulent deletion of computer data, generating counterfeit data, with the intention that it be taken into account or used for legal purposes as if it were original; • if the acts were committed to fraudulently gain an advantage, for oneself or for others, through modifying, altering or deleting computer data or by any form of computer sabotage.
Article 73: Computer hacking	It is an offence to manipulate or sabotage an information and communication system, by breaking the security system put in place by the owner, in order to access confidential information transferred into the system or to tamper with the system. There is an enhanced penalty when the offence relates to an information system or a data processing program protected by a secret access code.
Article 74: Identity theft	It is an offence to seize the identity of a third party or to make use of a third party's identification data (including his IP address or his pseudonym on a social network) to disturb his tranquillity or that of others, or to undermine his honour or his reputation. o This offence appears to overlap with Article 466 of the Penal Code (Identity-related offences).

Article 77: Violation of the secrecy of electronic correspondence	It is an offence to violate the secrecy of electronic correspondence by the opening, deletion, delay, listening, interception or storage of communications and related traffic data, or any other means of interception or surveillance, or by the diversion of electronic correspondence exclusively intended for a third party or for several natural or legal persons, whether or not it has arrived at its destination, without the users' consent. There is an enhanced penalty when this offence is committed by someone in public authority, acting in the course of their duties but without legal authority for the acts concerned. o This offence appears to overlap with Article 473 of the Penal Code (Interference with or interception of electronic correspondence).
Articles 78-79: Theft of information	o This provision is almost identical to Articles 468-470 of the Penal Code combined with Article 458. o There is no explicit protection for circumstances where theft of information might be justified in the public interest, such as where information is obtained by a whistleblower.
Article 81: Computer falsification	It is an offence to make a forgery, by introducing modified, altered or erased data into a computer system, intentionally and without right, so that they are deleted, absorbed or transmitted by an information system with the intention that they will be taken into account or used for legal purposes as if the falsified data were authentic. The penalties vary with the circumstances and intention.
Article 82: Deception	o This provision replicates Article 457 of the Penal Code, with a different range of fines.
Article 83: Fraud	It is an offence to fraudulently use one or more elements of the identification of a natural or legal person through an information system. There are different penalties for different manifestations of the offence. o This offence appears to overlap with Article 466 of the Penal Code (Identity-related offences).
Articles 84-85: Cryptology offences	It is an offence to violate the ban on exercising the profession of cryptology service provider, or the obligation to withdraw the means of cryptology in accordance with this law. It is an offence to fail to comply with the reporting obligations provided for in Article 63 of this law for supply, transfer, import or export of a means of cryptology, or the obligation to communicate such acts to the Minister in charge of electronic communications. It is an offence to export a means of cryptology or transfer this to another State without having the authorization required by Article 63 of this law or outside the conditions of any necessary authorization. It is an offence to sell or rent a banned means of cryptology. It is an offence to provide cryptology services aimed at ensuring confidentiality without having satisfied the requirements for declaration of this under Article 64 of this law.

	○ These offences appear to overlap with Article 450 (Illegal dealings in cryptology) and 467 (Cryptology offences) of the Penal Code. ○ The many rules on cryptology appear to be aimed at providing the State with the means to penetrate any anonymous communications.
Articles 86 and 88: Devices	It is an offence to knowingly, with the intention of committing one of the offences set out in this law, to produce, sell, import, hold, distribute, offer, transfer or make available - • equipment, a device or a computer program; • a password, access code or similar computer data It is an offence, when done intentionally and without right, to produce, sell, obtain for use, import, distribution or other forms of making available - • a device (including a computer program) that is primarily designed or adapted to allow the commission of information theft; • the use of a password, an access code or similar computer data allowing access to an information system, with the intention that they will be used to commit an offence under this law. It is also an offence to possess such a device or any other computer tool or program with the intention that it be used to commit an offence under this law. The penalties are the same as for the underlying offence. ○ These offences appear to overlap with Articles 460 and 471 of the Penal Code concerning devices.
Article 90: Sending an unsolicited message	It is an offence, punishable by a fine, to send an unsolicited electronic message on the basis of the collection of personal data, unless it contains a link that allows the recipient to unsubscribe.
Article 91: Misuse of data	It is an offence to use the identification elements of a natural or legal person to deceive the recipients of an electronic message or the users of a website for the purpose of getting them to communicate personal or confidential data. The penalty is 5 years imprisonment and a fine of 10 million Comorian francs. ○ The slang term for this act is "phishing".
Article 92: Embezzlement	It is an offence to communicate personal data or confidential information with the aim of embezzling public or private funds. The penalty is 10 years imprisonment and a fine of 20 million Comorian francs.
Article 93: Unauthorized data processing	It is an offence to process personal data either without having previously individually informed the persons concerned of - • their right of access, rectification or opposition • the nature of the data transmitted. • the recipients of such data. It is also an offence to process personal data despite the opposition of the person concerned. ○ This provision is more aligned to personal data protection than to cybercrime.

LAW ON CYBER SECURITY AND THE FIGHT AGAINST CYBERCRIME – CONTENT-BASED OFFENCES THE TITLES ADDED HERE ARE BASED ON THE OVERARCHING TERMS APPLIED TO THE ACTS COVERED BY THE OFFENCE IN THE TEXT OF THE LAW.	
Article 75: Cyber harassment	It is an offence to use an electronic communications network or service or another electronic method to initiate an electronic communication that coerces, intimidates, harasses or causes emotional distress in a person, with the aim of encouraging serious, repeated and hostile behaviour having as its object or effect a deterioration of that person's living conditions resulting in an alteration of his physical or mental health. The penalties differ depending on the intention or result: • if the culprit knew or should have known that the behaviour would seriously affect the tranquillity of the person concerned; • if the culprit initiates or relays false information about another person through social networks or any electronic medium; • if the victim was a person who was vulnerable due to age, pregnancy, illness, disability or physical or mental disability, and this was apparent or known to the perpetrator. The victim may request the withdrawal of the publications by their author or by the IT support manager. Article 5 defines cyber-harassment as "an aggressive, intentional act perpetrated by an individual or a group of individuals by means of electronic forms of communication, repeatedly against a victim who cannot defend himself." This description notes that cyber-harassment is practiced via mobile phones, instant messaging, forums, chats, online games, emails, social networks and photo sharing sites as well as other means. It also explains that cyber-harassment can take several forms such as online intimidation, insults, mockery or threats; spreading rumours; account hacking and digital identity theft; using social networks against a classmate; posting photos or videos showing the victim in a negative light; or producing images of young people that could be used in the context of child pornography. o The impact required as a result of cyber harassment narrows the offence, which should help to prevent abuse.
Article 76: Illegal dissemination of personal content	It is an offence to reveal, share with a third party or bring to the attention of the public, without the consent of the person concerned, one or more private images or audiovisual recordings of that person, where this seriously infringes the right to privacy of the person concerned. o "Revenge porn" would be one manifestation of this offence.
Article 80: Child pornography	This provision adds detail to the offences relating to child pornography in Articles 463-464 of the Penal Code, covering private possession as well as a wide range of acts including various aspects of production, trade and storage. Pornography is defined in Article 5 as any data, regardless of nature or form, visually depicting persons engaging in an explicit sexual act or realistic images depicting persons engaging in explicit sexual conduct. Child pornography is defined in Article 5 as-

	• any material visually depicting a child under the age of 18 engaging in sexually explicit conduct, real or simulated; • any representation of the sexual organs of a child under the age of 18 for primarily sexual purposes; • any material visually depicting a person who appears to be a child under the age of 18 engaging in explicit sexual behaviour, real or simulated; • any depiction of the sexual organs of a person who appears to be a child under the age of 18 • realistic images of a child under the age of 18 engaging in explicit sexual behaviour or realistic images of a child's sexual organs for a primarily sexual purpose. o Note that this provision, although it overlaps with Article 463-464 of the Penal Code, refers only to children under 18.
Article 94-98: Infringement of intellectual property	These provisions concern various forms of infringement of intellectual property by means of an information system. o These provisions overlap with Article 475 of the Penal Code.
Articles 99-104: Gambling	Gambling on electronic communication networks is permitted only under a regime of exclusive State rights granted to a limited number of operators. Any unauthorized online gambling is illegal, online gambling encompasses games of chance, illegal lotteries, prohibited lottery advertising and illegal betting. Transfers of money by payment card or bank transfer or any other means of payment in the context of illicit gambling on electronic communication networks are prohibited. Banking or financial institutions operating in Comoros must ensure compliance with this prohibition, and must notify the authorities of any violation of this prohibition. o These provisions overlap with Articles 476-478 of the Penal Code.
Article 121: Material of a racist, separatist or xenophobic nature	It is an offence to create, distribute or make available in any form writings, messages, photos, sounds, videos, drawings or any other representation of ideas or theories of a racist, separatist or xenophobic nature, through an information system. This is defined in Article 5 as any writing, image or other representation of ideas or theories that advocates, encourages or incites hatred, discrimination or violence against any person or group based on race, colour, descent, national origin or religion, insofar as the latter serves as a pretext for one or the other of these elements. o This provision overlaps to some extent with Article 493 of the Penal Code, but that law refers only to material of a racist or xenophobic nature (omitting separatist) and applies only to national origin and religion.
Article 122: Threats of death or violence	It is an offence to threaten others with death or violence through an information system. If the threat has a racist, xenophobic, ethnic, religious, separatist character or refers to a group characterized by race, colour, descent, insularity or

	national or ethnic origin, the penalty is higher: 10 to 20 years imprisonment and a higher fine. o This offence is virtually identical to Article 494 of the Penal Code, but with some added grounds for invoking the higher penalty.
Article 123: Images relating to the commission of offences	It is an offence to knowingly record, by any means whatsoever, on any medium whatsoever, images relating to the commission of offences, or to disseminate such images. This does not apply when the recording or dissemination results from the normal exercise of a profession whose purpose is to inform the public or is made in order to serve as evidence in court. o The exception would appear to cover journalists and the press.
Article 124: Insult	o This provision is identical to Article 495 of the Penal Code.
Article 125: Genocide or crimes against humanity	o This provision is identical to Article 495 of the Penal Code. o As in Article 495, the terms "genocide" and "crimes against humanity" are not defined but would probably be understood to have the meaning given to them in the international context.
Article 126: Disturbing public order or undermining human dignity	o This provision is identical to Article 497 of the Penal Code.
Article 127: Information relating to destructive devices	It is an offence to disseminate or make available to others, by means of or on an electronic communication network or an information system, instructions for use or processes allowing the manufacture of destructive devices likely to harm life, property or the environment, to be produced from powder or explosive substances, nuclear, biological or chemical materials, or from any other product intended for domestic, industrial or agricultural use. Professionals are exempted. There is an enhanced penalty where these processes have allowed the commission of murder or assassination. o This provision is similar to Article 498 of the Penal Code, with some added detail and an enhanced penalty when the offence results in death.
Article 128: Inciting suicide	o This provision is identical to Article 499 of the Penal Code.
Article 129: False information	o This provision is identical to Article 500 of the Penal Code.
Article 130: Threats of harm to property or persons	o This provision is identical to Article 501 of the Penal Code.

Article 131: Treason	○ This provision is identical to Article 502 of the Penal Code.
Article 132: Espionage	○ This provision is identical to Article 503 of the Penal Code.

As in the case of the Penal Code, the **penalties** are stiff, with most cybercrime offences being punishable by a **mandatory minimum sentence of imprisonment combined with a fine**; only a few of the listed offences allow for punishment by only one of these options.

The possible **additional penalties** that can be imposed on conviction are the same as those provided in the Penal Code.[401]

The rules on the liability of legal persons, and the consequences of participating in **association or agreement with others** to prepare or commit any of the offences in the law, are also the same as in the Penal Code.[402]

This law, like the Penal Code, imposes a range of obligations on service providers.

Cybercafés: There are a few changes of detail from the rule in the Penal Code on this topic. A child under age 10 (as opposed to age 18) must be accompanied to a cybercafé by an adult (as opposed to a parent or custodian). The other rules on cybercafés are the same as in the Penal Code.[403]

Filtering requirements: The rules on the provision of technical filtering means are the same as in the Penal Code.[404]

Subscriber data: Service providers must keep data identifying their subscribers for 10 years. They must pay a hefty fine if it is impossible to find the author of an electronic communication because of their failure to keep subscriber data.[405]

Preservation and production orders: A "competent authority" (which is not defined in the law) can issue a preservation order to a service provider, with no time limit, in respect of a specific criminal investigation. At the request of the public prosecutor or the order of the investigating judge, the competent authority can issue a production order in respect of deleted data in their possession or under their control, as well as traffic and subscriber data.[406]

Searches and seizures: The competent authority may conduct searches and seizures of computer equipment and computer storage media, according to the procedures

[401] Loi N°21-012/AU, Articles 133 and 89.
[402] Id, Articles 87 and 134.
[403] Id, Articles 105-106.
[404] Id, Articles 107-108.
[405] Id, Articles 116 and 136.
[406] Id, Articles 137-138.

in the Code of Criminal Procedure.[407] Data can be copied instead of seized if the examining magistrates finds this more appropriate.[408]

Content and traffic data: At the request of the public prosecutor or the order of the investigating judge, the competent authority can use technical means to collect or record traffic data or content associated with specific communications transmitted by means of an information system or require a service provider to allow the collection of real-time content and traffic data.[409]

Take-down notifications: The take-down notification procedure and related duties in this law[410] is essentially the same as in the Penal Code. However, this law adds a provision that authorises a judicial authority to protect the victim of the illegal content on an electronic communication service by prescribing any measures suitable for preventing future damage or putting an end to the damage already caused.[411]

C) ADDITIONAL SPEECH-RELATED OFFENCES IN THE PENAL CODE

There are some offences in other chapters of the Penal Code that overlap with the cybercrimes in Chapter IV of the Penal Code. These have been referenced above in the table on content-based offences.

Other offences elsewhere in the Code also explicitly involve means that include a wide variety of media, including online media. Several offences in other chapters refer to means of public dissemination set out in **Article 224 of the Penal Code**: "radio broadcasting, television, cinema, the press, display, exhibition, distribution of writings or images of all kinds, speeches, songs, cries or threats made in public places or meetings and generally all technical processes, including new information and communication technologies, intended to reach the public".

Defamation is covered generally in the Penal Code, in the chapter on offences against persons. Some of the features of relevance are as follows:

- Defamation is described as any allegation or imputation of a fact that undermines the honour or reputation of a person or body (Article 234).
- When defamation is committed by one of the means referred to in Article 224, it is punishable even if it targets a person or a body not expressly named, but whose identification is made possible by the materials that are disseminated (Article 234).
- Defamation committed against individuals by one of the means set out in Article 224 is punishable by imprisonment for one to six months plus a fine. If committed by the same means against a group of persons who belong, by their origin, to a specific race or religion, and the aim was to stir up hatred against members of that group, the penalty is imprisonment for two months to two years and a fine.

[407] Id, Articles 139-140 and 143.
[408] Id, Article 144.
[409] Id, Articles 141 and 145.
[410] Id, Articles 109-114.
[411] Id, Article 115.

- Defamation against public officials and institutions is somewhat more lightly punished. Defamation committed by one of the means set out in Article 224 against courts, tribunals, elected officials, the army and public administration, or against public officials, and certain other persons engaged in official duties, is punishable for imprisonment for two months to one year and a fine, or by only one of these two penalties.
- Any republication of defamatory matter will be deemed to be made in bad faith unless evidence to the contrary is provided by its author.
- Some additional penalties are also provided for specific instances of defamations or specific categories of culprits (Articles 243-247).

Article 57 of the Penal Code prohibits any statement or act–

- likely to establish or give rise to **discrimination** of any kind;
- aimed at provoking or maintaining **regionalist propagation**;
- which propagates news tending to **undermine the unity of the nation or the credit of the State**;
- **contrary to freedom of conscience and worship and likely to set citizens against each other**.

CODE PENAL

Article 57: Tout propos, tout acte de nature à établir ou à faire naître une discrimination de toute nature, tout propos, tout acte ayant pour but de provoquer ou d'entretenir une propagation régionaliste, toute propagation de nouvelles tendant à porter atteinte à l'unité de la nation ou au crédit de l'Etat, toute manifestation contraire à la liberté de conscience et au culte susceptible de dresser les citoyens les uns contre les autres, sera puni d'un emprisonnement de un à cinq ans.

The penalty is imprisonment for 1 to 5 years, which is a harsh penalty for a proscription that is so broad and general in its terms.

Article 127 makes it an offence to knowingly publish, by any means whatsoever, a **montage** made with the words or images of a person without that person's consent, if it does not appear obvious that it is a montage or if this is not expressly mentioned.

There are several offences that relate to **insults** in respect of **state authorities**:

- It is an offence to oppose by acts, words, gestures or other means the legitimate acts of a public authority or a person in charge of a ministry where this could undermine public order or hinder the smooth running of administrative or judicial services (Article 82).
- It is an offence to offend the President in speech or published words that are accessible to the public. The same applies to foreign Heads of State visiting the Comoros (Article 146).
- It is an offence to insult magistrates or assessors by word, writing or drawing, even if the insult is communicated only to the official and not made public (Article 146). The same applies to any ministerial officer or law enforcement official (Articles 147-148).

Article 299 is mainly concerned with pornography, but it also makes it an offence **to publicly incite others to practices contrary to morality** by word, writing or other means

of communication– which could be applied to communications about same-sex issues.[412] Article 312 makes it illegal to **habitually attack morals by inciting debauchery or promoting the corruption of minors**, which could be similarly applied.

False news is covered by two provisions in the Penal Code:

- Article 182 makes it an offence, punishable by imprisonment and a fine, to knowingly spread false news or false allegations to the public by any means where this is likely to directly or indirectly undermine their confidence in the credit of the State, local authorities, public establishments or other organizations in which public authorities and establishments have a stake.
- Article 231 makes it an offence, punishable by imprisonment and a fine, to publish, disseminate, disclose or republish by any means false news or information with fabricated facts or falsified attributions to third parties, where this results - or is *likely* to result - in disobedience to the country's laws, undermining of the morale of the population or discrediting public institutions. It is irrelevant whether or not the communication was made in bad faith.

It is unclear how one would determine whether news or allegations are "false" or "misleading", or what sorts of information would be likely to discredit the state or public institutions or undermine the morale of the population.[413] A provision in the previous version of the Penal Code which is analogous to Article 231 of the current Penal Code was applied against Comorian journalist Oubeidillah Mchangama, who runs a Facebook-based news outlet, in December 2020, following his publication about a potential gas shortage that allegedly disturbed "public order".[414]

CODE PENAL

Article 231: La publication, la diffusion, la divulgation ou la reproduction par quelques moyens que ce soit des nouvelles fausses, de pièces fabriquées, falsifies or mensongères attribuées ***à*** des tiers, sera punie d'un emprisonnement d'un an ***à*** trois ans et d'une amende de 75 000 à 750 000 francs comoriens, lorsque la publication, la diffusion, la divulgation, la reproduction faite ou non de mauvaise foi, aura entraîné la désobéissance aux lois du pays, ou porté atteinte au moral de la population ou jeté le discrédit sur les institutions publiques ou leur fonctionnement. Les mêmes peines seront également encourues lorsque cette publication, diffusion, divulgation ou reproduction auront été susceptibles d'entraîner les mêmes conséquences.

There are also several offences relating to **speech concerning religion**:

- It is an offence to propagate or teach any religion other than Islam to Muslims, or to offer to Muslims, any publications disclosing ("*divluguant*") a religion other than Islam (Article 175).
- It is an offence to "insult" a minister of a religion in the exercise of his functions (Article 176).

[412] Article 300 of the Penal Code prohibits any "act of a sexual nature contrary to mores or against nature".
[413] "LEXOTA Country Analysis: Comoros", last updated July 2022.
[414] Id.

One source reports that these prohibitions are not usually enforced.[415] However, another source reports that any "non-Sunni" religious expression (including on Facebook and in blog posts) is inhibited for fear that it will be considered proselytization.[416] It was also recently reported that, while there is no evidence of arrests based on religious practices, "members of non-Sunni groups reported broad self-censorship and stated they practised their beliefs only in private".[417]

A group of other provisions, considered together, could inhibit the reporting of information from whistleblowers or investigative journalism more broadly. It is generally illegal to listen to, record or transmit by means of any device the words spoken in a private place by a person without their consent (Article 124), or to take or transmit an image of a person in a private place without the latter's consent (Article 125). Article 126 makes it an offence under the law governing the press and press offences if such material is made public through the press. These prohibitions make sense to protect the privacy of individuals generally, but could be applied to matters of public interest, where information was gathered covertly by whistleblowers or journalists.

D) CRIMINAL INVESTIGATIVE POWERS AND STATE SURVEILLANCE

The **Law on Electronic Communications** makes it illegal to listen to, intercept or store communications and data without the consent of the persons in question, *unless this is authorized pursuant to regulations relating to national security*.[418] Electronic communications service providers are required to preserve traffic and location data for one year, in cases it is required for the investigation or prosecution of criminal offences. Police officials may demand this type of technical data in order to prevent acts of terrorism. Data about the content of electronic communications may not be stored and processed. More details are to be set out in regulations.[419]

In terms of the **Law on Cyber Security and the Fight against Cybercrime**, authorized agents may seize the means of cryptology with judicial authorization, based on a request containing the information to justify the seizure.[420]

According to the US State Department: "There were no credible reports the government monitored private online communications without appropriate legal authority, although it was widely suspected they did so." [421]

[415] "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.
[416] "Comoros: Full Country Dossier", Open Doors International/World Watch Research, January 2023, pages 20 and 23 (writing from a Christian perspective).
[417] "2022 Report on International Religious Freedom: Comoros", US State Department, Office of International Religious Freedom, "Executive Summary".
[418] Loi N°14-031, Article 69.
[419] Id, Article 70.
[420] Loi N°21-012/AU, Article 67.
[421] "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.

E) SIM CARD REGISTRATION

COMOROS DOES NOT HAVE A LAW ON MANDATORY SIM CARD REGISTRATION.[422]

F) TAKE-DOWN NOTIFICATIONS

Take-down procedures are contained in both the cybercrime chapter of the **Penal Code** and the **Law on Cyber Security and the Fight against Cybercrime** and have been discussed above.

[422] "Which governments impose SIM-card registration laws to collect data on their citizens?", *comparitech*, 20 March 2023.

CHAPTER 6

DEMOCRATIC REPUBLIC OF CONGO (DRC)

CHAPTER 6: DEMOCRATIC REPUBLIC OF CONGO (DRC)

DRC KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **124th globally; 37th out of 48 African countries** "Media pluralism is a reality in the DRC but, in the eastern province of Nord-Kivu, the media have been badly affected by fighting between the army and M23 rebels. Against this backdrop, the national assembly passed a new media law in April 2023, just months ahead of general elections."
MALABO CONVENTION: NOT signatory or party but the Council of Ministers approved a draft bill authorising ratification on 6 December 2022[423]
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Democratic Republic of the Congo 2005 Constitution The 2005 Constitution was amended in 2011, but the amendments did not affect these provisions.[424] **ARTICLE 23** All persons have the right to freedom of expression. This right implies the freedom to express their opinions and convictions, in particular by speech, in print and through pictures, subject to respect for the law, public order and morality. **ARTICLE 24** All persons have the right to information. The freedom of the press, the freedom of information and broadcasting by radio and television, written press or any other means of communication are guaranteed, subject to respect for the law, public order and the rights of others. The law determines the conditions for the exercise of these liberties. The audiovisual and written media of the State are public services to which all political and social movements are guaranteed access in an equitable manner. The status of the State media is established by law which guarantees objectivity, impartiality and plurality of views in the processing and distribution of information.
KEY LAWS: • Loi n° 20/17 du 25 novembre 20 relative aux telecommunications et aux technologies de l'information et de la communication

[423] "Democratic Republic of Congo: Council of Ministers authorises ratification of Malabo Convention", alt.advisory, 27 January 2023.
[424] Loi n° 11/002 of 20 janvier 2011, amending Articles 71, 110, 126, 149, 197, 198, 218 and 226.

• (Law no. 20/17 on telecommunications and information and communication technologies, which includes a cybercrime chapter) • **L'ordonnance-loi n°23/009 du 13 mars 2023**: Press Freedom Law • (this law could not be located online as of mid-2023, but a copy is on file with the authors) • L'ordonnance-loi n°23/010 du 13 mars 2023: Digital Code • Code Pénal Congolais (selected provisions)
CRIMINAL DEFAMATION: Yes[425]
DATA PROTECTION: DRC has provisions on personal data protection in a number of laws, including the recently-enacted Digital Code.[426]
ACCESS TO INFORMATION: DRC has a draft access to information law that has not yet been passed by both houses of Parliament.[427]

THIS CHAPTER WAS PREPARED WITH THE AID OF VARIOUS ONLINE TRANSLATION TOOLS.

6.1 CONTEXT

The key media regulatory body is the **High Council for Broadcasting and Communication** ("Conseil Supérieur de l'Audiovisuel et de la Communication"- **CSAC),** which is established by Article 212 of the Constitution and Organic Law no. 11/001.[428]

CSAC's main functions are:
- guaranteeing freedom of the press, information and mass communication
- overseeing adherence to a code of conduct in respect of information provision
- overseeing equitable access to state media by all political parties and associations
- developing a code of conduct
- mediating in media-related disputes

[425] Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, Article 74.
[426] Hogan Lovells, "DRC Overview: Guidance Note", Data Guidance, September 2022; "Recent developments in African data protection laws - Outlook for 2023", Lexology, [2022]; Jean-François Henrotte, "Protection des données en RDC", Lexing, [2023]. Other relevant laws on this topic are Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies") and L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Law no. 23/010 of 13 March 2023, the "Digital Code").
[427] Proposed Law on Access to Information (Proposition de Loi Relative a l'Access a l'Information). This law was passed by the Senate (the upper chamber of Parliament) in 2015, but not ratified by the National Assembly. See "Democratic Republic of Congo", PPLAAF, 2021; "Democratic Republic of Congo: High Commissioner update", UN High Commissioner for Human Rights, 30 March 2023.
[428] Loi organique n° 11/001 du 10 janvier 2011 portant composition, attribution et fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication ("Organic Law No. 11/001 of January 10, 2011 on the composition, attribution and functioning of the High Council for Broadcasting and Communication"). Note that Article 160 of the 2005 Constitution requires that all Organic Laws must be submitted to the Constitutional Court for a ruling on their conformity with the Constitution before they are promulgated. Internal regulations of the CSAC must also be submitted to the Court for a ruling on their constitutionality before they are applied.

- promoting excellence in media production
- promoting a culture of peace, democracy, human rights and fundamental freedoms
- promoting a national culture through the media
- protecting children
- filing reports to parliament
- providing advisory opinions on draft laws to Parliament or government.[429]

CSAC is governed by a Board of 15 members. They are all formally invested by the President, but the law requires that they represent a variety of stakeholders and the members appointed by government bodies are in the minority.[430]

DEMOCRATIC REPUBLIC OF THE CONGO 2005 CONSTITUTION

Article 212
A High Council for Broadcasting and Communication with legal personality is established.

It has the mission to guarantee and ensure the liberty and protection of the press as well as of all means of mass communication in respect of the laws.

It supervises the respect for good practice standards with regard to the information and the equitable access of political parties, associations and citizens to the official means of information and communication.

The composition, competences, organization and operation of the High Council for Broadcasting and Communication are determined by organic law.

CSAC has jurisdiction over "all means of mass communication", defined in the 2011 law as including "radio and/or television stations and/or television channels as well as print and electronic media outlets whose purpose is the collection, processing and dissemination of information or ideas".[431] It deals with media-related complaints from members of the public.[432] It is empowered to impose sanctions against journalists and media outlets for operating illegally, and it has unlimited discretionary powers to suspend a radio or television broadcasting service for up to three months, to suspend or cancel a specific programme, or to suspend or cancel a television channel or radio station or a section of a press organ. It can also seize media-related documents and materials.[433] CSAC can also approach the public prosecutor to institute criminal action.[434] Its powers to impose sanctions can respond to a complaint or be taken on its own initiative.[435]

The 2011 law prohibits the glorification of crime as well as incitement to violence, depravity of morals, xenophobia, tribal, ethnic, racial or religious hatred or any other form of discrimination;[436] there is no specific sanction for violating this stricture, but this could presumably support a finding of a violation of journalistic ethics or be used as a justification for imposing discretionary sanctions.

[429] Loi organique n° 11/001, Articles 8-10, as translated and summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 206 (hereinafter "Limpitlaw").
[430] Loi organique n° 11/001, Articles 24 and 26.
[431] Id, Article 4.
[432] Id, Article 57.
[433] Id, Articles 58-59; Limpitlaw, pages 206-207.
[434] Id, Articles 68 and 74.
[435] See id, Article 62.
[436] id, Article 6.

A recent case illustrates the powers that CSAC can wield. In May 2022, CSAC suspended journalist Louis-France Kuzikesa Ntotila of CML13 TV for 72 days for having "organized a media service whose content conveyed hate speech as well as remarks tending to incite violence against a tribe and to personal attacks". CSAC also cut off the CML13 television signal for 45 days and ordered that it could resume operations only on the presentation of all administrative documents, the program schedule and the specifications. Two elected officials who appeared as guests on the journalist's show "Free Debate" were also sanctioned by being deprived of access to media broadcasting in the DRC for 90 days.[437]

CSAC operates alongside the independent statutory **Regulatory Authority for Posts, Telecommunications and Information Technologies of Congo** (*"L'Autorité de Régulation de la Poste et des Télécommunications du Congo"*) (**ARPTIC**).[438] ARPTIC is responsible for processing licence applications and permits and overseeing adherence to the laws and regulations relating to telecommunications.[439] Licencing and other basic conditions for telecommunications service providers are set out in **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies**[440] - which also contains the provisions on cybercrime discussed below. It should be noted that this law gives the Minister power, acting on a proposal from ARPTIC, to suspend or withdraw licences issued under the law for failure to comply with legal obligations; one additional ground for withdrawal of a licence is "endangering state security".[441]

One analysis notes that, despite the existence of these two regulatory bodies (CSAC and ARPTIC), the real power over the media remains concentrated in the executive.[442]

The **Broadcast Press Freedom and Professional Practice Decree**[443] sets out a number of content requirements for broadcasters. For example, broadcasters will be held responsible for all content broadcasts. They must be impartial and objective when broadcasting political content, and it is forbidden to broadcast "political propaganda", which is not defined. Further broadcasting content restrictions are

[437] Oscar Bisimwa, "Urgent : le CSAC suspend le journaliste Louis-France Kuzikesa et sa chaîne CML13 TV", *Congo Reformes*, 22 mai 2023.
[438] This body was first created by Loi n°014/2002 du 16 octobre 2002, which was later replaced by Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies"). A table comparing the key points in these two laws can be found on the ARPTIC website here.
[439] Limpitlaw, page 209. Note that Limpitlaw's analysis does not cover the modifications made by the 2017 Telecommunications Law. Note also that the "Press Freedom Law" referred to in Limpitlaw is the 1996 version and not the one enacted in 2023.
[440] Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies").
[441] Id, Article 52.
[442] Limpitlaw, page 208: "The DRC has more than one regulatory authority for broadcasting and signal distribution. While regulators are established in terms of a number of different statutes, it is clear that real power in respect of broadcasting resides in the executive branch of government and, in particular, with the Ministry of Press and Information. Despite being a constitutionally mandated body, the [CSAC] operates alongside a Regulatory Authority [ARPTIC], which deals with technical matters, and is overshadowed by the very real powers exercised by the executive".
[443] Ministerial Decree 04/MIP/020/96, dated 26 November 1996.

contained in **The Broadcasting Press Freedom and Professional Practice Implementing Measures,**[444] which prohibits the broadcast of any content that contradicts Congolese laws, disturbs public order or infringes on good morals as well as any films, images or documentaries of a pornographic nature. There is also a **Radio and Television and Compliance Commission**,[445] that is charged with ensuring broadcasters' compliance with all applicable legal rules and making recommendations on sanctions in the case of breaches. [446]
Even the content of music and entertainment is regulated. The **National Song and Entertainment Censorship Commission**, which is a body appointed by the Minister of Justice, reviews content to ensure it does not disturb public order or good morals and does not contain racial or tribal slurs, insults, slanderous language, or pornographic content. These requirements have been applied at times as the basis for the arrest of artists whose work was critical of the government.[447]

In 2023, DRC enacted two new laws that are central to the topics under discussion: a Press Freedom Law[448] *and a Digital Code.*[449]

The new Press Freedom Law sets out procedures for the exercise of freedom of the press and freedom of information in respect of radio and television broadcasting, the written press and any other means of communication in the DRC, including the online press.[450] It applies to public and private, community and religious media.[451] It also governs professional journalists and media professionals.[452] This law repeals "all previous provisions" contrary to it.[453]

The previous 1996 Press Freedom Law was revised in 2023 "on the basis of the recommendations of a national media convention held in January 2022, which called for a more up-to-date and protective legal framework for journalism and the media".[454] According to a government spokesperson: "This law makes it possible to solve a large number of problems which disturb this sector on a daily basis, among others, the slippages and the non-compliance of certain media, especially the online news media which, with technological evolution, are advancing with remarkable

[444] Ministerial Decree 04/MCP/011/2002, dated 20 August 2002.
[445] Ministerial Decree 04/MIP/006/97 dated 28 February 1997.
[446] Limpitlaw, pages 226-229.
[447] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[448] **L'Ordonnance-Loi n°23/009 du 13 mars 2023** fixant les modalites d'exercice de la liberté de presse, la liberté d'information et d'emission par la radio et la télévision, la presse écrite ou tout autre moyen de communication en République Démocratique du Congo ("Ordinance-Law N°23/009 of March 13, 2023 fixing the procedures for the exercise of freedom of the press, freedom of information and emission by radio and television, the written press or any other means of communication in Democratic Republic of Congo") ("Press Freedom Law"). This law could not be located online as of mid-2023, but a copy is on file with the authors. It replaces Law no. 96/002 of 22 June 1996.
[449] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
[450] **L'Ordonnance-Loi n°23/009**, Articles 1 and 82.
[451] Id, Article 15.
[452] Id, Article 2.
[453] Id, Article 140.
[454] "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders, "Legal Framework".

speed." This spokesperson also expressed particular concern about community radio stations which were not previously governed by any law.[455]

The new law defines "**freedom of the press**" as the right to inform, to be informed, to have one's opinions and convictions and to communicate them without any hindrance, whatever the medium used, subject to compliance with the law, the public order, the rights of others and of good morals – thus generally following the constitutional articulations of this right.[456]

One positive element of the new law is that it gives journalists access to information of public interest that is not classified and does not involve state security or national defence. However, there are still weaknesses: the new press freedom law tightens the conditions for access to the profession of journalist and fails to explicitly abolish prison sentences for press offences – although it does at least add a "bad faith" element to the offences of publishing false information or allegations disturbing public order.[457] One online article describes it as "less repressive, but more restrictive" for journalists.[458]

The law defines a "**professional journalist**" as a person who graduated from a school of journalism recognized by the State and whose main, regular and remunerated activity consists in the collection, processing and dissemination of information, or a person holding a bachelor's degree or the equivalent who also has three years of professional practice in the collection, processing and dissemination of information within the editorial staff of a press company recognized by the State.[459] It also provides a broader definition of "**media professional**", which includes publishers, directors, editors, current affairs presenters, cartoonists, translator-editors, reporter-photographers, sound recording operators and others involved in media production.[460]

Media professionals must apply for a professional identity card and complete a probationary period of 12 to 24 months. At the end of the probationary period, the candidate must undertake to respect the code of ethics and professional conduct for journalists, by signing a written engagement with the body responsible for the self-regulation of the media profession. The training regime for media professionals and the other criteria for the granting, renewal and cancellation of the professional card, are set by the self-regulatory body of the profession.[461]

---

[455] Prince Mayiro, "RDC - Ass. Nat: Porté par Muyaya, le projet de loi de ratification de l'ordonnance-loi sur la liberté de la presse et la liberté d'information adopté",*7sur7.cd*, 5 avril 2023: "*Cette loi permet de résoudre un nombre important de problèmes qui dérangent ce secteur au quotidien, entre autres, les dérapages et la non-conformité de certains médias, surtout les médias d'informations en ligne qui, avec l'évolution technologique, avancent avec une rapidité remarquable.*" See also "Ordonnance loi fixant modalités de l'exercice de la liberté de la presse en RDC, Assemblée nationale : Patrick Muyaya explose et passe!", *Publié par La Prospérité*, 5 avril 2023.
[456] Compare Articles 23 and 24 of the Democratic Republic of the Congo 2005 Constitution quoted on the first page of this chapter.
[457] Id; "DRC enacts press law and digital code that criminalize journalism", Committee to Protect Journalists, 23 May 2023.
[458] "La RDC se dote d'une nouvelle Loi sur la Presse, moins répressive, mais plus contraignante, à quelques mois des élections à hauts risques", statement by Journaliste en Danger (JED), *deskeco.*, 7 avril 2023.
[459] Id, Article 3 (item 11).
[460] Id (item 20).
[461] Id, Articles 8-12, 93

Foreign media professionals must be accredited by the minister in charge of communication and media, who sets the requirements, procedures, costs and duration of such accreditations.[462]

Different categories of press, including written press, broadcast media, religious media and online media, must submit applications to CSAC to operate, with specific requirements for information that must be provided in respect of each category of press. They are free to operate only after they have received a receipt, not from CSAC, but from the minister responsible for media and communications. The duration of the authorizations issued by the minister for the operation of the various categories of press enterprises cannot exceed a maximum of ten years.[463] In the case of written publications or broadcast media, the receipt must be provided within 30 days of the application, unless the application is incomplete; otherwise, the right to publish or broadcast is automatically acquired.[464] A similar rule applies to online press, with the right to operate being automatically granted if there is no authority forthcoming after 90 days.[465]

Public radio and television stations are required to be "objective, impartial and pluralistic" and to broadcast programming based on the public's right to information, equal access, diversity of opinion and the values of democracy, tolerance, openness, dialogue and national cohesion.[466] **Community radio stations** must be administered and managed by bodies put in place by the local community or communities themselves, in compliance with the law on non-profit associations. They must be apolitical and they must promote peace, stability, cohesion, and the development of their respective communities but also of the whole nation.[467]

Any associative, community or religious media must have a Program Director who is a professional journalist.[468] (Associative media refers to a media outlet run by a non-profit association with a view to promoting its activities.[469]) The law also sets requirements for half of the content of such media, stipulating that they must fall within a range of categories devoted to the public good, such as the promotion of good governance or the promotion of traditional national cultural values.[470]

Online press organs must have a publication director and they must regularly employ at least two journalists. It must operate in a journalistic manner, by presenting regularly updated material and in respect of research, verification and formatting of its information. Its content must be of general public interest and must not be "likely to shock the Internet user by a representation of the human person undermining his dignity and decency or glorifying violence".[471] Online media must respect the law,

[462] Id, Article 94.
[463] Id, Article 59.
[464] Id, Article 6.
[465] Id, Article 84.
[466] Id, Articles 64-66.
[467] Id, Articles 67-70.
[468] Id, Article 77.
[469] Id, Article 3 (item 14).
[470] Id, Article 80.
[471] Id, Articles 87- 88.

public order, good morals and the rights of others.[472] This means that CSAC thus has the power to sanction online media for failing in these duties, either by withdrawing the notice of compliance or by temporarily banning their operation.[473]

Online press organs do not include personal websites and blogs published on a non-professional basis.[474]

On the **right of access to information**, media professionals have the right of access to all public and private sources of information "of public interest", and subject to the legal provisions in force, in particular on attacks on State security, national defence and professional secrecy, any holder of information has the obligation to provide media professionals with public interest information. Any unjustified retention of public interest information can be punished "in accordance with the law". **Media professionals are also explicitly protected against being required to divulge their sources of information**. Any person who delivers public information to a professional journalist is also protected against prosecution if the information delivered falls within the competencies that the person has assumed.[475]

The Press Freedom Law also includes a **right of reply and rectification.** Any natural or legal person cited or implicated in a written or online press article or in a radio or television broadcast, either by name or indirectly, but in such a way that they can be identified, has the right to have a response or correction inserted in the columns of said publication or to access said program for the same purpose, free of charge. However, when charges concern persons taken individually, these rights apply only to the extent that the person's interests are called into question.[476] There are specific directions on timing, length, placement and presentation of the reply or correction.[477] The law stipulates that the publication of the right of reply or rectification constitutes compensation for the injured party; in the event of a refusal to publish the reply or rectification, the injured party has the right to approach the courts for compensation.[478]

The law also created a number of new **crimes** that can be applied to journalists, which are discussed below in section 6.4 of this chapter.

The new Digital Code covers all digital activities and services, including electronic commerce, electronic signatures, digital government services, the regulation of digital platforms, the protection of personal data, cybersecurity and cybercrime.[479] It creates a **Digital Regulatory Authority ("***l'Autorité de Régulation du Numérique***"-ARN)** that regulates digital activities and services,[480] in addition to several other bodies

[472] Id, Article 92.
[473] "Les attributions du Conseil Supérieur de l'Audiovisuel et de la Communication, CSAC en sigle", Edmond Mbokolo Eilima, *LegaVox*, 11 mai 2023.
[474] **L'Ordonnance-Loi n°23/009**, Article 91.
[475] Id, Articles 95-97.
[476] Id, Article 104.
[477] Id, Articles 105-111.
[478] Id, Article 112.
[479] "The Democratic Republic of Congo takes a significant step in digital with the ratification of the Digital Code", *fatshimetrie*, 23 August 2023.
[480] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code"), Article 7

concerned with digital matters and cybersecurity. Its specifics on cybercrime are detailed in the cybercrime section of this chapter.

The state broadcast media, "**Radio Télévision Nationale Congolaise**" **(RTNC)**, is regulated by Ordinance 81/050 of 2 April 1981.[481] Its Board is appointed by the President, who also has the power to remove individual members during their terms of office.[482] The **Congolese Press Agency** ("Agence Ccongolaise Presse") **(ACP)**, which is the state newsgathering agency, is also regulated by law.[483]

Commenting for this study on the state's use of some of these laws for repressive purposes, Prof. Tresor Musole Maheshe, a law professor at the Catholic University of Bukavu, indicated that since its enactment, the **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** has been regularly deployed in a heavy-handed fashion to muzzle journalists and/or media organizations.[484] He also pointed to the new *Digital Code, despite it only being enacted in 2023, already having been used to censor some media outlets and journalists. Some of these examples are discussed in subsequent sections. He also expressed the opinion, based on anecdotal evidence, that the Digital Code has already created a "chilling effect" by contributing to journalists' self-censoring.*

6.2 CONSTITUTION

The DRC Constitution contains no general limitations clause. The rights to freedom of expression and freedom of information and the press are both made subject to respect for "the law, public order and morality".

In other words, these rights are subject to legislation. The Constitution articulates no limitations on the restrictions that can be imposed on these rights by legislation - such as requirements that such restrictions must be reasonable, proportional or necessary in an open and democratic society.

> The effect of this limitation formulation is the almost universal undermining of the very concept of constitutional supremacy. The protection given by a constitutional right is entirely subjugated to the content of legislation passed by parliament, and no special requirements in respect of such rights-limiting legislation are required.[485]

[481] L'Ordonnance n° 81/050 du 2 avril 1981 (not found online). See also Décret n°09/62 du 03 décembre 2009 fixant les statuts d'un établissement public dénommé Radio-Télévision Nationale Congolaise, en sigle « RTNC », which changed its name from "*L'Office Zaïrois de Radio diffusion et de television*" (OZRT) to "*Radio Télévision Nationale Congolaise*" (RTNC).
[482] Limpitlaw, page 216.
[483] It is currently regulated in terms of L'Ordonnance n° 81/052 du 2 avril 1981 (not found online).
[484] Tresor Musole Maheshe was interviewed via Zoom on 25 July 2023.
[485] Limpitlaw, page 187.

6.3 CASE STUDIES

This overview of the state of the media in DRC was published in 2021:

> *A number of laws limit the ability of the press to inform the public about matters of the day. All too often journalists are arrested and detained, and independent media houses are often raided and banned. In the case of broadcasters, many have had their broadcasting distribution signals suspended without notice. The DRC features regularly on international lists of poor media environments, and there is little doubt that the country is, sadly, not in line with international standards for democratic media regulation. Internet and social media shutdowns are frequent even though internet penetration is extremely low at approximately 6%.*[486]

Reporters Without Borders makes the following observations in its 2023 World Press Freedom Index:

> *The Congolese media landscape is marked by the presence of politicians who own or launch media outlets intended to promote their influence and rise to power. The national radio and TV broadcaster is a state media outlet that lacks independence. It is very common for local authorities, militiamen, religious groups, and politicians to exert pressure on the journalists and media outlets present in their province. […]*
>
> *Congolese journalists and media outlets lead a very precarious existence. Employment contracts are rare and the practice of "coupage" – whereby journalists receive a cash payment for covering an event or reporting some information – is widespread. The funding that the state has to legally provide to media outlets has never been distributed in a transparent manner. Very few media outlets are viable and independent, and most are influenced by those who back them.*
>
> *Journalists are sometimes targeted on the basis of their ethnic or community affiliation, and they are exposed to reprisals in connection with their work, particularly in the east of the country, where there are many armed groups. The conflict in Nord-Kivu is off-limits for the media, which are caught between rebel violence and the army's response. Some radio stations or radio broadcasts were suspended in 2021 for "incitement to tribalism and violence". Many journalists routinely censor themselves. Corruption and certain mining contracts are among the subjects that are most likely to prompt self-censorship.*
> *The dangers to which journalists and media are exposed include arrest, intimidation, physical violence, media closures, media outlets getting ransacked, and murder. In Nord-Kivu, they have been threatened by a wave of harassment and reprisals since the start of 2023 despite a ceasefire. M23 rebels ordered some media outlets to change their editorial policies. Discouraging the armed forces via the media in wartime is punishable by death. The security forces have been implicated in many abuses but enjoy complete impunity.*[487]

[486] Id, page 183 (footnotes omitted).
[487] "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders.

A media rights watchdog in the DRC, Journalistes en Danger, reported in November 2022 that there had been 124 cases of **attacks against journalists and media organizations** that year alone, including one instance of a journalist being killed while two journalists were abducted. Another 37 journalists were arrested, 18 were physically assaulted and 17 media organizations or programmes were shut down or suspended.[488]

It has been reported that journalists are frequently subjected to **violence, harassment, intimidation and even murder** by the government armed forces due to their reporting. For instance, Radio Okapi alleged in 2022 that a FARDC officer had shot and killed journalist Chadrack Senghi in retaliation for his reporting on army officials' harassment of civilians and their failures in the struggle against ISIS-DRC. The FARDC officer in question was reportedly arrested and charged with "flagrancy". [489]

The Committee to Protect Journalists reports numerous 2023 incidents that appear to be aimed at the **intimidation** of individual journalists:

- In June 2023, three journalists – Jeef Ngoyi, Marie-Louise Malou Mbela, and Jiresse Nkelani – were **arrested and assaulted** by at least 12 soldiers from the Armed Forces of the DRC (FARDC). They had been covering a land dispute in Kinshasa. They were all released by the next day, after interventions by the United Nations mission to the DRC. None of them were charged with any crime. The Committee to Protect Journalists notes that "repeated arrests and attacks on Congolese journalists by security forces that are supposed to be protecting the public make for an alarming pattern that must be reversed."[490]

- In April 2023, Gustave Bakuka, a reporter with the privately owned broadcaster Radio Mushauri, was **arrested** by three members of the Congolese National Intelligence Agency (ANR). He was accused of "**spreading false rumours**" in an article he wrote and shared through a WhatsApp group discussing security issues in Kindu, the capital of the Maniema province.[491]

- In a separate incident in April 2023, Diègo Kayiba, a reporter with the privately owned broadcaster Kin Actu TV and news website Reportage.cd, was **summoned and detained** by a prosecutor in Kinshasa in connection to two tweets which alleged that the head of the General Inspectorate of Finance had not been transparent about his personal spending and that he had betrayed the President through his own presidential ambitions.[492]

- In a third incident, an elected municipal representative in the city of Tshikapa, sent an audio message to journalist Sylvain Kabongo, a reporter with the privately owned Netic-news.net, **threatening him with arrest** for publishing a "baseless

[488] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
[489] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[490] "Congolese soldiers arrest, beat 3 journalists covering land dispute", Committee to Protect Journalists, 30 June 2023.
[491] "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
[492] Id

article" on his relationship with the minister of finance. The elected official claims that the article **damaged his reputation**, and he told the Committee to Protect Journalists that he intends to "punish" Kabongo and force him not to publish similar reports.[493]

- Also in April 2023, journalist Mills Tshibangu, director of the privately owned online broadcaster Chat Television, was arrested by a group of about 12 police officers in response to a **criminal defamation** complaint filed by the Minister of Mines in respect of reporting on alleged corruption involving a lithium mine. Tshibangu was held in custody overnight.

- In March 2023, journalist John Ngongo Lomango, director of the Radiotélévision Evangélique Phare (RTEP) broadcaster, was arrested by ANR agents in Kindu. He was accused of **distributing false information** in a news broadcast where he reported that Angolan soldiers had arrived in Kindu to assist the Congolese military in implementing a cease-fire with the M23 rebel group He was released two days later, but authorities confiscated his phone with the intention of searching it.[494]

- Also in March 2023, the Minister of Defense filed a criminal complaint against journalist Stanis Bujekera Tshamala, accusing him of **publishing false rumours that caused public alarm** in a tweet According to Bujekera, who is a correspondent for the France-based Jeune Afrique news website, the Reuters news agency, and the Congolese online new outlet Actualité.cd, the tweet had simply quoted from the official minutes of a Cabinet meeting in which the Minister of Defence had expressed surprise about the military advance by M23 rebels in the eastern part of the country. After intervention by the Minister of Communication, the Minister of Defence dropped the complaint.[495]

- In January 2023, the minister of communication and media for Lomami province ordered *Radio Tokomi Wapi* to suspend its operations and close its office in the provincial capital of Kabinda. Police were stationed at the broadcaster's offices to enforce the closure. Provincial officials alleged that the radio station had **incited the local population to tribalism, revolt, and disobedience of provincial authorities**, as well as failing to comply with journalistic ethics, after a guest on a call-in programme criticised the province's governor. The owner and the director of the radio station insisted that it had not broadcast anything that constituted incitement and considered the suspension to be politically motivated.[496]

- Also in January 2023, two journalists – Sylvain Kiomba, editor-in-chief of the privately owned radio station *Shilo FM*, and Joseph Ebondo, a reporter at the same station – were detained on suspicion of **criminal defamation** after they alleged that the

[493] Id.
[494] "Congolese journalist John Ngongo Lomango arrested over conflict reporting", Committee to Protect Journalists, 28 March 2023; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
[495] "DRC defence minister files, withdraws false news complaint against reporter Stanis Bujekera", Committee to Protect Journalists, 14 March 2023.
[496] "DRC broadcaster Radio Tokomi Wapi suspended, police shutter station", Committee to Protect Journalists, 18 January 2023.

ANR operated illegal secret holding cells in Lubao. They were questioned and then released without being charged two days later.[497]

The US State Department's 2022 Report on Human Rights Practices reports that there have been numerous cases where individuals have been charged with contempt, defamation, spreading false rumours, and public insult for criticizing the actions of government officials:

- In late July and early August 2022, several opposition party members and supporters were arrested in Kinshasa on separate charges of **defamation**, **public** insult, and **spreading false rumours**.

- In August 2022, the former head of the President's political party Union for Democracy and Social Progress, Jean-Marc Kabund, was arrested on the charges of **contempt of the head of state**, **defamation**, and **spreading false rumours.** The charges related to statements he made during a press conference, calling President Tshisekedi "irresponsible" and "a public danger" and accusing government officials of lying, manipulation, embezzlement of public funds, and corruption. Kabund remained in detention in November 2022, despite an August 2022 court order that he should be remanded to house arrest.

- At least five provincial and national politicians were **arrested** in North Kivu and Ituri for criticizing the state of siege in the two provinces.

- In November 2021, Luc Malembe, a spokesperson for the opposition party *Engagement for Citizenship and Development* (ECIDe), was arrested on charges of **spreading false rumours** after he criticized the state of siege in the eastern provinces in a social media post. He was acquitted after spending seven months in detention.[498]

In January 2022, freelance reporter Patrick Lola and Christian Bofaya, a reporter for the privately owned *E Radio*, were **arrested for allegedly disturbing public order** after they covered a public protest about a dispute concerning the election of three provincial deputies. They remained in detention until August 2022, when the Court of Cassation in Kinshasa granted bail. After the court decision, demonstrations broke out at Mbandaka Central Prison, where the journalists were held (along with the provincial deputies who had been arrested for organising the protests). Bofaya escaped from prison during the aftermath of this incident, but Lola remained in custody because he was unable to pay the 2 million Congolese francs set as bail. As of April 2023, Lola was still in custody.[499]

[497] "DRC authorities detain 2 journalists for 48 hours over reporting on alleged secret jails", Committee to Protect Journalists, 12 January 2023.
[498] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 1E. The report views these persons as political prisoners and detainees.
[499] "Patrick Lola Imprisoned", Committee to Protect Journalists, 10 January 2022; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.

In February 2022, National Deputy Josue Mufula was arrested at the airport in Goma, on charges of **contempt of the army**, **flagrancy**, and **provocation and incitement to breaches of public authority** because he passed out leaflets criticizing the state of siege.[500]

In June 2022, President Tshisekedi granted presidential amnesty to Jacky Ndala, a member of the opposition party *Ensemble pour la Republique*, who was sentenced to two years in prison on charges of **incitement to civil disobedience** for allegedly encouraging *Ensemble* party members to protest a draft law that would bar citizens with one non-Congolese parent from holding presidential office.[501]

In August 2022, officials arrested Marie Masemi, a social media star on charges of **defamation** and **public insult** after she posted a video on social media criticizing the First Lady and alleging that she was not Congolese. She was released Masemi after three days in custody, and the charges were dropped. Masemi posted a video to social media apologizing for her comments, but some wondered if the apology had been coerced as a condition of her release.[502]

In November 2022, Olivier Makambu of the community broadcaster Radio Communautaire pour le Renouveau du Kwango (RCRK) was detained after a Member of Parliament filed a **criminal defamation** complaint against him.[503]

In November 2021, the minister of communication and media in the Equateur province of DRC suspended *Radio Télévision Sarah (RTS)* for 60 days, accusing it of **insulting government authorities** and "**calling on the population to revolt,**" after it aired programmes critical of Equateur Governor Bobo Boloko Bolumbu. In January 2022, the Equateur government **extended the suspension indefinitely**. The media outlet filed a lawsuit against the Equateur government, and a local court of appeal in the provincial capital declared the closure to be illegal and ordered that the station must be permitted to reopen. The next day, when journalists arrived at the office, they found that all of the broadcasting equipment was missing. Armed police officers then arrived and blocked access to the broadcaster's office over the next several days. In 2022, a court in the provincial capital convicted *RTS* reporter Chilassy Bofumbo on charges of "**prejudicial accusations, contempt for authority, public insult, and inciting hatred and rebellion**" in connection with his coverage of a street protest against the governor. He was released after being held for seven months. In 2019, the director of RTS, Steve Mwanyo Iwewe, was sentenced to 12 months imprisonment on a charge of **insulting the governor**, tied to his coverage of a protest on the eve of elections. He was released after two months of incarceration.[504]

---

[500] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[501] Id, section 1E
[502] Id, section 2A.
[503] Joel Simon, Carlos Lauría and Ona Flores,"Weaponizing the Law: Attacks on Media Freedom", Thompson Reuters Foundation and Tow Centre for Digital Journalism, April 2023, page 18.
[504] "Governor of DRC's Equateur province defies court order allowing Radio Télévision Sarah to reopen", Committee to Protect Journalists, 13 June 2023; "In DRC, provincial governor blocks radio station's bid to resume broadcasting", Reporters Without Borders, 20 June 2023.

In March 2021, the Mayor of Kolwezi filed a complaint of **criminal defamation under Article 74 of the Penal Code** against Donat Kambola, the Coordinator of the *Initiative Bonne Gouvernance et Droits Humains* (IBGDH) ("Good Governance and Human Rights Initiative"). IBGDH is a member of the umbrella NGO body *La Synergie des Organizations de la Société Civile de Lualaba Œuvrant dans le secteur des Ressources Naturelles* (SOLORN) ("The Coalition of Civil Society Organizations in Lualaba working in the Natural Resources Sector"), and Kambola is the coordinator of that coalition. The charges appear to stem from a letter by SOLORN to the Provincial Government of Lualaba denouncing the poor state of the roads in some parts of Kolwezi and calling for an investigation into conflicts of interest and alleged irregularities in the sale of government land. SOLORN also filed a criminal complaint with the public prosecutor related to conflicts of interest in public office and embezzlement of public property.[505]

These are just a few of many more cases that could be cited. The US State Department reported in 2022 that provincial governments sometimes prevented journalists from filming or covering certain protests or pressured the media not to cover certain events – including those organized by opposition parties or local activists. [506]

Multiple sources indicated that many journalists exercise self-censorship due to concerns of harassment, intimidation, or arrest.
A 2021 report states that the government limits access to the Internet in several ways:

- Total shutdowns
- Targeted shutdowns, where only particular sites are blocked.
- Throttled internet, where the speed of the internet is deliberately slowed so as to render it effectively unusable.[507]

This is authorised by Article 125 of **Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies**.[508]

Loi n° 20/17 du 25 novembre 20 relative aux telecommunications et aux technologies de l'information et de la communication

ARTICLE 125:
Sans préjudice des droits et libertés fondamentaux individuels ou collectifs garantis par la Constitution et des procédures y attachées, l'Etat peut, durant le temps qu'il détermine, soit pour des raisons de sécurité intérieure et/ou extérieure, de défense nationale ou d'ordre public, soit dans l'intérêt du service public de télécommunications, soit pour tout autre motif jugé nécessaire, suspendre,

505 "DRC: Drop Defamation Charges Against Human Rights Defender", Amnesty International Public Statement, AFR 62/3924/2021, 30 March 2021.
506 "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
507 Limpitlaw, page 221.
508 Such moves could also have been implemented by ARPTIC under Article 3(i) of Loi n° 014-2002 du 16 octobre 2002 portant création de l'Autorité de régularisation de la poste et des télécommunications which empowers it to protect the public interest. Limpitlaw, page 221. (Limpitlaw also mentions the Telecommunications Act 13-2002 of 16 October 2002 as possible authority, but this law was repealed by Article 202 of Law 20/17.)

restreindre, filtrer, interdire ou fermer certains services et applications, en tout ou en partie, y compris l'usage des installations.

Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies

ARTICLE 125:
Without prejudice to the fundamental individual or collective rights and freedoms guaranteed by the Constitution and the procedures attached thereto, the State may, during the time it determines, either for reasons of internal and/or external security, national defence or public order, or in the interest of the public telecommunications service, or for any other reason deemed necessary, suspend, restrict, filter, prohibit or close certain services and applications, in whole or in part, including the use of installations.

This is an overview of internet shutdowns between 2015 and 2019:

> *The Democratic Republic of Congo has experienced many internet shutdowns over the past several years. These have ranged from complete country wide shutdowns to targeted regional shutdowns of social media platforms. […] The internet shutdowns are often accompanied by outages of SMS services, cuts to radio and television signals for independent broadcasters, and the implementation of roadblocks in population centres such as Kinshasa.*
>
> *The first reported internet shutdown occurred in January 2015. This followed an earlier 25 day cut to SMS services in December of 2011. Again, on 19 December 2016, the government ordered the internet to be shut down on the day Joseph Kabila was set to step down as head of State. On 30 December 2017, the Democratic Republic of Congo's Telecommunications Minister, Emery Okundji, ordered the country's telecommunications providers to shutdown internet and SMS services across the country. There was another three-day internet blockage beginning 21 January 2018. Then on 25 February 2018 there was a ten-hour blockage. From 31 December 2018 to 6 January 2019, during the election count, internet users in the Democratic Republic of Congo were again shut off from the internet.*[509]

[509] "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, page 9 (footnote omitted).

6.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

DRC does not have a single dedicated cybercrime law. Instead, **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** contains chapters on cybersecurity, cryptology and cybercrime.[510] In addition**, Ordinance-Law no, 23/010 of 13 March 2023**, the Digital Code, contains provisions on cybersecurity, cryptology and cybercrime.[511] The Digital Code states that it repeals all previous provisions contrary to it,[512] but it generally appears to supplement **Law no. 20/17** rather than to supersede it**.**

A) CYBERCRIME PROVISIONS IN LAW NO. 20/17 ON TELECOMMUNICATIONS AND INFORMATION AND COMMUNICATION TECHNOLOGIES

Article 153 of Law no. 20/17 provides an overview of the acts that constitute cybercrime:

1. child pornography;
2. racism;
3. xenophobia
4. infringements, in particular those involving:
    a. the activities of providers of electronic communication services for the public;
    b. electronic advertising,
    c. direct marketing;

5. damage to property related to information and communication technologies
6. attacks by any means of public dissemination;
7. attacks on national defence;
8. breaches of the confidentiality of computer systems;
9. breaches of the integrity of computer systems;
10. damage to the availability of computer systems;
11. computer data breaches in general;
12. specific breaches of the law relating to personal data.

Specific offences in these categories are set out in another part of the same law,[513] as summarised in the tables below. Titles have been added to the tables for ease of reference, but there are no titles in the law itself. The French text of some of the technical offences is provided in footnotes, where the translation may have misinterpreted what is prohibited.

[510] Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication (Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies). This law is administered by ARPTIC, under the supervision of the relevant minister. Id, Articles 12-13.
[511] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
[512] Id, Article 389.
[513] Loi n° 20/17, Article 154.

LAW NO. 20/17 - TECHNICAL OFFENCES	
Article 179: Violating secrecy of correspondence or manipulating personal data	Without prejudice to the payment of damages to the victim, it is an offence to violate the secrecy of correspondence or to manipulate personal data without prior authorization. The penalty is penal servitude for the individual who acted in this manner, and a fine for that individual's employer. o Note that Article 126 lifts the secrecy of correspondence – * At the request of the public prosecutor * With the authorization of the Courts and Tribunals within the framework of a judicial investigation of a crime; * By competent public authorities, for reasons of internal and/or external security of the State, national defence or public order.
Article 180: Intercepting private communications or correspondence	It is an offence to intercept, listen to, record or transcribe by means of any device a communication or private correspondence. The penalty is 1 to 3 years of primary penal servitude and/or a fine.[514]
Article 182: Disrupting the Hertzian emissions of an authorized service	It is an offence to disrupt the Hertzian emissions of an authorized service using, without right, a frequency or a radio installation. The punishment is primary penal servitude for one month to one year and/or a fine.[515]
Article 184: Interrupting electronic communications	It is an offence to intentionally interrupt electronic communications by any means. The penalty is penal servitude for 2 to 5 years and/or a fine.
Article 185: Unauthorized use of frequencies or numbers	It is an offence to use or transfer frequencies, numbers or blocks of numbers that have not been allocated. The penalty is a fine.
Article 186: Fraudulent access or remaining	It is an offence to fraudulently access, or remain in, all or part of an electronic communication system. The penalty is penal servitude of six months to three years and a fine, or one of these penalities only.[516] It is also an offence to obtain any advantage whatsoever, for oneself or others, by fraudulently accessing. or remaining in. all or part of an electronic communication system. The penalty is the same as above.[517]

[514] "Est punie de un à trois ans de servitude pénale principale et/ou d'une amende de 1.000.000 à 10.000.000 de francs congolais, toute interception, écoute, enregistrement, transcription au moyen d'un quelconque dispositif pour divulgation d'une communication ou correspondance privée."

[515] "Est puni d'une peine de servitude pénale principale d'un mois à un an et/ou d'une amende de 50.000.000 à 100.000.000 de Francs congolais, toute personne qui perturbe, en utilisant, sans titre, une fréquence ou une installation radioélectrique, les émissions hertziennes d'un service autorisé."

[516] "*Quiconque accède ou se maintient frauduleusement dans tout ou partie d'un système de communication électronique est puni d'une servitude pénale de six mois à trois ans et d'une amende 1.000.000 à 10.000.000 de francs congolais ou de l'une de ces peines seulement*".

[517] "*Est également puni des mêmes peines, celui qui se procure poir soi-même ou pour autrui, un avantage quelconque, en s'introduisant ou se maintenant frauduleusement dans tout ou partie d'un système de communication électronique.*"

	○ The offences of fraudulent access and remaining, which are separated in some SADC countries, are combined into one here. Some say that both are forms of unauthorized access.[518] ○ There appears to be no defense of justified access for a purpose that is in the public interest, such as security testing or gaining information for use in whistleblowing.
Article 187: Fraudulent data interference	It is an offence to fraudulently introduce data into an electronic communication system that obstructs or distorts its operation. The penalty is primary penal servitude of one to five years and/or a fine.
Article 188: Computer-related forgery by changing data	It is an offence to damage, erase, deteriorate, alter or fraudulently modify the data in an electronic communication system. The penalty is the same as provided in the Penal Code for forgery in writing.
Article 189: Computer-related forgery by producing or manufacturing data & using unlawful data	It is an offence to produce or manufacture a set of digitized data by fraudulently entering, erasing or deleting data from an electronic communication system. The penalty is the same as provided in the Penal Code for forgery in writing. The same penalties apply to knowingly making use of the data obtained under the conditions provided for in Articles 185 to 187 of this law. ○ The prohibition on the use of data that was obtained in violation of Article 186 (Fraudulent access or remaining) could affect the ability of journalists to use whistleblower data or data in a cache such as Wikileaks.
Article 190: Unauthorised processing of personal data	It is an offence to process personal data (or to cause it to be processed) without the prior authorization required by Article 126. The penalty is penal servitude for an unspecified time for the individual who committed the offence, and a fine for that individual's employer. ○ "Personal data" is defined in Article 4 (item 37) as "any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social or economic identity". ○ "Processing of personal data" is defined in Article 4 (item 95) as "any operation or set of operations carried out using automated or non-automated processes and applied to the data, such as the collection, processing, recording, organization, storage, adaptation, modification, extraction, saving, copying, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, as well as the blocking, encryption, erasure or destruction of personal data". ○ These definitions are based on the Malabo Convention. ○ The authorization referred to in Article 126 is authorization by Courts and Tribunals within the framework of a judicial investigation of a crime.

[518] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	○ It is unusual in the region for illegal personal data processing to be classified as a cybercrime.
Article 191: Devices for unlawful use	It is an offence to produce, sell, import, hold, distribute, offer, assign or make available equipment, a computer program, a device or data designed or specially adapted to commit one or more of the offences provided for in Articles 186 to 189 of this law. It is also an offence to do the same acts with a password, an access code or similar computerized data allowing access to all or part of the electronic communication system. The penalty in either case is the same as for the underlying offence, or the most severely sanctioned underlying offence. ○ Similar provisions in many other SADC countries refer to devices *primarily* designed or adapted for illegal purposes, because of the existence of dual-use devices.
Article 196: Theft of information	The fraudulent embezzlement of information to the detriment of others through a system of electronic communication is a form of theft. The penalty is the same as provided in the Penal Code for theft.

With respect to the **penalties** for technical offences, all are punishable by a term of imprisonment or a fine, or both.

LAW NO. 20/17 – CONTENT-BASED OFFENCES	
Article 181: Obscene, racist or xenophobic material or false distress calls	It is an offence to transmit or put into circulation – • obscene, racist or xenophobic signals, images and messages; or • false or misleading distress calls by means of telecommunications or ICT. The penalty is primary penal servitude for 6 months to a year and/or a fine. ○ There is no definition of the key terms "obscene", "racist" or "xenophobic", which opens the door to subjective enforcement and self-censorship.
Article 193: Child pornography	It is an offence to produce, record, offer, make available, distribute, transmit, import or export an image or representation containing child pornography through an electronic communication system. The penalty is primary penal servitude for five to ten years and/or a fine. ○ "Child pornography" is defined in Article 4 (item 76) as "any data of whatever nature or form visually depicting a minor engaging in sexually explicit conduct or realistic images depicting a minor engaging in sexually explicit conduct. ○ This offence overlaps with Article 174m of the Penal Code which contains a broader definition of "child pornography".[519]

[519] Code pénal congolais, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006. Article 174 applies to "any representation by any means whatsoever, of a child engaging in sexual activities explicit, real or simulated, or any representation of the sexual organs of a child, for primarily sexual purposes".

Article 194: Ideas or theories of a racist or xenophobic nature	It is an offence to create, download, distribute or make available in any form whatsoever writings, messages, photos, drawings or any other representation of ideas or theories of a racist or xenophobic nature through an electronic communication system. The penalty is a primary penal servitude of five to ten years and/or a fine. o There is no definition of the "ideas or theories of a racist or xenophobic nature", which opens the door to subjective enforcement and self-censorship. o Similar provisions in other SADC countries do not criminalize the mere *download* of such material where it is not further disseminated. This could, for instance, hinder a journalistic investigation into racist or xenophobic groups. It is also unusual to prohibit the creation of such material where it is not publicly shared.
Article 194: Discriminatory threats	Any threat, by means of an electronic communication system, to commit an offence against a person because of his membership of a group which is characterized by race, descent or national or ethnic origin, or religion where this serves as a pretext for one of the other elements. The penalty is penal servitude of 5 to 10 years and a fine. o This is one of the few offences that imposes a mandatory prison sentence, without the option of a fine instead of imprisonment.
Article 197: Treason	It is treason through an electronic communications system to – • deliver to a foreign power or its agents, in whatever form or by any means whatsoever, any information, object, document, procedure, digitized data or computerized file that must be kept secret in the interest of the national defence; • secure any of these items for the purpose of delivering them to a foreign power or its agents; • destroys such items, or allows them to be destroyed, in order to favour a foreign country. The penalty is the same as provided in the Penal Code for treason. o This offence overlaps with Articles 184-185 of the Penal Code.[520] The penalty is death.
Article 198: Failure to safeguard information related to national defence	It is an offence for any guardian or custodian of any information, object, document, process, digitized data or computerized file which must be kept secret in the interest of national defence – without any intention of treason or espionage – to, through an electronic communication system, destroy, remove, reproduce, withdraw, transfer or reproduce the item, or allow it to be brought to the attention of an unqualified person or the public. The penalty is penal servitude for 5 to 10 years.

With respect to the **penalties** for content-based offences, only the offence of discriminatory threats makes no provision for a fine to be imposed as an alternative to imprisonment (instead of imposing the two kinds of penalties in conjunction). The logic behind treating this offence differently from the others on the list is unclear.

[520] Code pénal congolais, Articles 184-185. The Penal Code provides separate offences for Congolese citizens (treason) and for foreigners (espionage). The cybercrime offence applies to "any person".

Across the board, it is an offence to **participate in an association or an agreement** established with a view to preparing for or committing a cybercrime. The penalty is the same as any other kind of criminal association.[521]

Law no. 20/17 imposes a range of duties on telecommunications and internet service providers.

SIM card registration: Telecommunications service providers are required by Article 92 to collect and store identifying information in respect of all their subscribers, and to keep "identification cards containing the minimum essential information". The specific conditions and procedures for identifying subscribers are set out in orders issued by the relevant minister.[522] The sale of SIM cards to unidentified users, the provision of access to unidentified users, or providing or allowing clandestine avenues for accessing telecommunications services are criminal offences.[523] According to Privacy International, the ministerial order on SIM card registration "requires telecom operators to respect the secrecy of information collected from their subscribers except for compelling reasons related to internal and external security or in the event of legal proceedings".[524]

Cybercafés: Article 58 requires that the intention to offer cybercafés or "hot spots" must be declared to ARPTIC, which will issue a certificate of approval and inform the relevant minister. The terms and conditions for granting approval are set by ministerial order.

Preservation of connection and traffic data: In terms of Article 143, network operators and service providers are required to retain connection and traffic data for 12 months and to install data traffic monitoring mechanisms on their networks. The stored data must be accessible during legal investigations, under the conditions set by laws and regulations relevant to such investigations.

Prohibition on undermining State security: A provision unusual in the region is Article 176, which makes it an offence for any network operator or service provider to undermine the security of the State, or to facilitate this.

Filters: Under Article 139, network content providers are required to set up filters to deal with harmful attacks on the personal data and privacy of users. Article 140 requires operators that provide access to information systems to inform users of the need to install parental control devices and the existence of filtering devices, as well as offering at least one filtering tool.

[521] Loi n° 20/17, Article 192.
[522] Id, Articles 92-95.
[523] Id, Articles 156-157 and 172-173.
[524] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 26. The ministerial order referenced in this source could not be located online.

Warnings about risks: Article 140 requires operators that provide access to information systems to warn users of the dangers of insecure information systems and the risks of security breaches and computer viruses. They must also provide information about tools to protect against viruses, spyware and misleading software, the activation of personal firewalls, intrusion detection systems and the activation of automatic updates. in terms of Article 141, they must also inform users that is it illegal to use the network to disseminate illegal content, and that it is illegal to design and distribute spyware or other tools that can be used for fraudulent behaviour.

Cryptology: Article 146 requires service providers to declare any intention to offer encryption services to ARPTIC, which will issue a certificate of approval and inform the relevant minister. The declaration by the service provider must include a description of the technical characteristics of the cryptology means, as well as the source code of the software used. Article 145 exempts consular or diplomatic missions and the use of encryption related to state security agencies from the declaration requirements.[525]

Enforcement: Under Article 168, government officials may carry out unannounced checks for telecommunications and ICT offences, and at the request of the public prosecutor – and in accordance with the provisions of the Code of Criminal Procedure - carry out searches and seizures for this purpose.

B) CYBERCRIME PROVISIONS IN LAW NO. 23/010, DIGITAL CODE

The Digital Code, like the law on telecommunications and information and communication technologies, contains both technical and content-based offences. It also establishes the principle that existing common law offences can be committed by means of an electronic communication network or a computer system.[526]

As in the case of the law on telecommunications and information and communication technologies, titles have been added to the tables for ease of reference, but are not provided in the law itself, except in some cases as paragraph headings for one or more articles. Also, here again, the French text of some of the technical offences is provided in footnotes for precision.

[525] See id, page 25 for more details.

[526] L'Ordonnance-Loi n°23/010, Article 331: "*Les infractions de droit commun commises au moyen d'un ou sur un reseau de communication electronlque ou un svsterne informatique sont reprirnees conforrnernent au Code penal congolais et aux dispositions penales particulleres en vigueur.*"

LAW NO. 23/010 (DIGITAL CODE) - TECHNICAL OFFENCES	
Article 332: Unlawful access or remaining	It is an offence, intentionally and without right, to access, or remain in, all or part of an electronic communication system with a fraudulent intention. The penalty is penal servitude of three to five years and a fine, or one of these penalties only.[527] It is also an offence to exceed one's power of legal access to a computer system with fraudulent intent or with intent to harm. The penalty is penal servitude for two to five years and a fine, or one of these penalties only.[528] o "Access" is defined in Article 2 (item 1) as direct or indirect connection to all or any part of a computer system or an electronic communication network. o The offences of fraudulent access and remaining, which are separated in some SADC countries, are combined into one here. Some say that both are forms of unauthorized access.[529] o These offences overlap with Article 186 of *Law no. 20/17* discussed above.
Article 333: Unlawful access or remaining that affects computer data or the operation of the computer system.	When the illegal access or remaining described in Article 332 results in deleting, obtaining or modifying data contained in the computer system, or an altering of the operation of the computer system, the penalties are increased. The penalties are increased still further if the acts referred to are committed in violation of security measures.
Article 334: Interception or other technical interference with non-public transmission of data	It is an offence, intentionally and without right, and by technical means, to intercept, disclose, use, alter or misappropriate data during non-public transmission to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such data. The penalty is penal servitude of five to ten years and a fine. o This offence overlaps with Articles 180 and 182 of *Law no. 20/17* discussed above.
Article 335: Unauthorised transfer of personal data	It is an offence to transfer, without the authorization of the person concerned, that person's personal data from one information system or means of data storage to another. The penalty is penal servitude for six months to three years and a fine.[530] There are enhanced penalties if this offence is committed with fraudulent intent, in connection with a computer system connected to another

[527] Id, Article 332: "*Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un svsteme informatique, avec une intention frauduleuse est puni dune peine de servitude penale de trois a cinq ans et d'une amende de clnquante millions a cent rnlllions de francs Congolais ou de l'une de ces peines seulement.*"

[528] Id: "*Quiconque, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'acces legal a un svsterne informatique, est puni d'une peine de servitude penale de deux a cinq ans et d'une amende de cinquante millions a cent millions de francs congolais ou de l'une de ces peines seulement.*"

[529] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

[530] L'Ordonnance-Loi n°23/010, Article 332: "*Est puni d'une servitude penale de six moi à trois ans et d'une amende de cinq millions a cent millions de francs conqolals, celui qui transfère, sans autorisation de la personne concernée, des données à caractère personnel de cette dernière d'un systerne informatlque ou d'un moyen de stockage de données vers un autre.*"

	computer system, or by means of bypassing protective measures put in place to prevent access to the content of a non-public transmission. This offence does not apply in the following cases: • an interception carried out in accordance with a judicial warrant; • communication sent by or intended for a person who has consented to the interception; • interception carried out by a legal person authorized to do this for the purposes of public safety or national defence; • interception carried out by a legal or natural person legally authorized to do this under the legal provisions and regulations in force in the DRC.
Article 336: Data breach	It is an offence, intentionally and without right, to directly or indirectly damage, erase, deteriorate, alter or delete data. The penalty is penal servitude for six months to five years and a fine, or one of these penalties only. There is an enhnaced penalty if the offence is committed with fraudulent intent or intent to harm.
Article 337: Interruption of normal operaton of computer system	It is an offence, intentionally and without right, to directly or indirectly cause by any technological means an interruption of the normal operation of a computer system. The penalty is penal servitude for one to ten years and a fine, or one of these penalties only. There is an enhanced penalty where the offence causes damage to data in the affected computer system or in any other computer system. There is also an enhanced penalty where the offence causes a serious disturbance or prevents, totally or partially, the normal functioning of the computer system concerned or any other computer system. There is an enhanced penalty where the offence affects one or more sensitive or critical infrastructures. It is irrelevant whether the impact of the offence is temporary or permanent. o There is no definition of sensitive or critical infrastructure ("*infrastructures sensibles ou critiques*"),. However, Article 2 (item 43) defines critical or essential infrastructure ("*infrastructure critique· ou essentielle*") as facilities, resources, equipment and/or services, non-interchangeable and with particular characteristics where it would be impossible for potential competitors to reproduce them by reasonable means because of the prohibitive cost of their reproduction.
Article 338: Devices for unlawful use	It is an offence, intentionally and without right, to produce, sell, import, export, distribute or make available in another form, any electronic device or equipment including data or computer programs, primarily designed or adapted for the commission of one or more offences provided for in the Digital Code. The penalty is penal servitude for two to five years and a fine, or one of these penalties only. It is an offence, intentionally and without right, to possess any device, including data, primarily designed or adapted to enable the commission

	of one or more offences provided for in the Digital Code. The penalty is penal servitude for six months to five years and a fine, or one of these penalties only. It is an offence for any officer, public official or law enforcement office, in the exercise of his duties - except in the cases provided for by law – to unduly possess, produce, sell, obtain with a view to its use, import, distribute or make available in other forms a device, including data, primarily designed or adapted to enable the commission of one or more offences referred to in the Digital Code. The penalty is penal servitude for two to five years and a fine, or one of these penalties only. o This provision overlaps with Article 191 of *Law no. 20/17* discussed above. This formulation is an improvement over Article 191 because it refers to devices *primarily* designed or adapted for illegal purposes, and thus avoids criminalization of dual-use devices.
Article 339: Falsification of data or forgery	It is an offence to commit forgery by introducing, intentionally and without right, modified, altered or erased data into a computer system, so that they are stored, processed or transmitted by a computer system or electronic communication network, or by modifying data by any other technological means, for possible use of such data or modification of their legal scope. The penalty is penal servitude for three to five years and a fine, or one of these penalties only.[531] Anyone who makes use of such data, while knowing that the data are false; is punished with penal servitude of five to ten years and a fine of twenty to fifty million Congolese francs, or one of these penalties only. o This provision overlaps with Articles 188 and 189 of *Law no. 20/17* discussed above.
Article 340: Computer fraud	It is an offence, intentionally and without right, to cause or seek to cause harm to another with intent to gain an illegal economic advantage for oneself or a third party, by - • introducing into a computer system, modified, altered or erased data that is stored, processed or transmitted by a computer system; • interfering with the normal operation of a computer system or data contained therein. The penalty is penal servitude for five to ten years and a fine.
Article 348: Sending unsolicited messages	It is an offence to send any unsolicited electronic message based on the collection of personal data without a link that allows recipients to unsubscribe. Failure to comply with this provision exposes the offender to a fine.
Article 349: Deception	It is an offence to use elements of identification of a natural or legal person with the aim of tricking the recipients of an electronic message or the users

[531] Id, Article 339: "*Quiconque commet un faux en introduisant, intentionnellement et sans droit, dans un système informatique ou un réseau de communication électronique, en modifiant, en altérant ou en effaçant des données qui sont stockées, traitées ou transmises par un système informatique ou un réseau de communication électronique ou en modifiant par tout autre moyen technologique, l'utilisation possible des données dans un système informatique ou un réseau de communication électronique, et par la modifie là portée juridique de telles données, est puni d'une servitude penale de trois a cinq ans et d'une amende de·vingt millions a cinquante millions de francs congolais, ou l;une de ces peines seulement.*"

	of a website into communicating personal data or confidential information. The penalty is penal servitude for six months to two years and a fine, or one of these penalties only.
Article 350: Unauthorised processing or personal data	It is an offence to process personal data without having previously informed the person concerned of their right of appeal, rectification or opposition, the nature of the data transmitted and the destination of the data, or despite the opposition of the person concerned. The penalty is penal servitude of six months to two years and a fine, or one of these penalties only.
Article 351: Identity theft	It is an offence, intentionally and without right, to usurp another's identity through a computer system, by phishing or any other means, by using one or more forms of data that make it possible to attribute oneself falsely and to assume the identity of others in order to disturb their peace or to attack their honour, their reputation or their interests. The penalty is penal servitude for one to five years and a fine. It is an offence to intentionally and wrongfully avail oneself of a reason or legitimate justification, using a computer system at any stage of the offence, to transfer, possess or use a means of identifying oneself as another person with the intention of committing, aiding or encouraging an illegal activity. The penalty is penal servitude for two to five years and a fine, or one of these penalties only. It is an offence to pretend through a computer system to be a third party (institutional, trust or otherwise) with the aim of inciting or compelling the victim to communicate personal data. The penalty is penal servitude for five to ten years and a fine, or one of these penalties only.
Article 352: Misuse of personal data or confidential information for misappropriatio n of funds	It is an offence to use personal data or confidential information for the purpose of misappropriating public or private funds. The penalty is penal servitude for one to ten years and a fine.
Article 353: Bank card fraud	It is an offence to - • counterfeit or tamper with a payment or withdrawal card by means of or on an electronic communication network or a computer system; • knowingly use a counterfeit or falslfied payment or withdrawal card by means of or on an electronic communication network or computer system; • knowingly accept or agree to receive payment by means of a counterfeit or falsified payment card by means of or on an electronic communication network or a computer system. The penalty is penal servitude for two to five years and a fine, or one of these penalties only.
Article 354: Facilitating bank card fraud	It is an offence to manufacture, acquire, hold, transfer, offer or provide equipment, instruments, computer programs or any data, designed or specially adapted, to carry out the offences provided for in Article 353. The penalty is penal servitude for five to ten years and a fine, or one of these penalties only.

	Counterfeit or falisified cards must be confiscated for the purpose of destruction, as well as any items intended or used for bank card offences except where they were used without the knowledge of the owner. In cases of recidivism, a judicial authority may interdict the perpetrator's civil rights and prohibit professional or social activity for one to two years.
Article 363: Junk mail and spam	It is an offence to do any of the following, intentionally and without legitimate cause or justification, or where the perpetrator has wrongly availed himself of a motive or a justification: • trigger the transmission of erroneous, unwanted or unlawful messages from multiple emails or by an intermediate computer system; • use a computer system or a protected electronic communications network for relaying or retransmitting messages from multiple emails for the purpose of spoofing or to mislead users or the electronic or internet service provider as to the origin of these messages; • severely falsify header information in messages from multiple emails and intentionally trigger the transmission of these messages.
Article 380: Damage to an effective technical measure	It is an offence to use or to provide various listed means to circumvent, neutralize, suppress or undermine a protection or control mechanism (otherwise than for the purposes of IT security).

There are additional offences relating to **cryptology** which are not listed in the table above. In brief, cryptology services or the supply, import or export of certain means of cryptology, must be declared to and approved by the National Agency of Cybersecurity. It is a criminal offence to violate these rules. It is also an offence to sell or rent to others a means of cryptology which has been the subject of an administrative ban on use and circulation or to obstruct a criminal investigation a means of cryptology or refuse to provide related information or documents. Furthermore, using cryptology to facilitate or commit a crime can result in a doubled penalty. It is an offence to refuse to provide a cryptology key where cryptology has been utilised in an offence – and the penally is enhanced if the refusal results in a failure to prevent the commission of an offence or to limit its effects. [532]

LAW NO. 23/010 (DIGITAL CODE) – CONTENT-BASED OFFENCES	
Article 355: Online gambling	Online gambling is prohibited, and it is an offence to advertise unauthorized gambling by means of or on an electronic communications network or a computer system. The penalty is a fine. The competent court may increase the amount of the fine to quadruple the amount of advertising expenditure devoted to the illegal operation.
Article 356: Dissemination of tribalist, racist and xenophobic material through	It is an offence to intentionally create, upload, distribute or make available to the public through a computer system, writings, content, messages, photos, sounds, videos, drawings or any other representation of ideas or theories of racist, tribalist or xenophobic nature or in any form whatsoever in the sense of the present ordinance-law and in accordance with the provisions of ordinance-law no. 66-342 of 07 June 1966 on the repression

[532] Id, Articles 341-347.

an electronic system	of racism and tribalism. The punishment is penal servitude for one month to two years and a fine, or one of these penalties only.[533] o The Digital Code does not define ideas or theories of racist, tribalist or xenophobic nature. It is broader than some offences of this nature in the SADC region since it does not require that the material in question incite hatred or discrimination. Also, it appears to outlaw the creation of material of this nature by means of a computer system even if the material is not shared.
Article 357: Child pornography	It is an offence to produce, distribute, broadcast, import, export, offer, make available, sell, procure for oneself or others or possess any pornographic material featuring a child through a computer system or an electronic communications network. The penalty is penal servitude for five to fifteen years and a fine. o The Digital Code contains no definition of "pornographic material".
Article 358: Harassment through electronic communication (with intent)	It is an offence to initiate electronic communication that coerces, intimidates, harasses or causes emotional distress in a person, using a computer system, for the purpose of encouraging hateful, tribal and hostile behaviour towards good morals and patriotic values. The penalty is penal servitude for one month to two years and a fine. "Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement haineux, tribal et hostile aux bonnes moeurs et aux valeurs patriotiques est puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais." o The Digital Code contains no definition of any of the key terms concerning content, making this provision very broad and vague - which opens the door to subjective application and abuse.
Article 359: Harassment through electronic communication (with knowledge)	It is an offence to harass a person through a computer system or electronic communication network, while the harasser knew or should have known that he would seriously affect the tranquillity of the person targeted by this behaviour. The penalty is penal servitude for one month to two years and a fine, or only one of these penalties. "Quiconque aura harcèle, par le biais d'un système informatique ou d'un réseau de communication électronique, une personne alors qu'il savait ou aurait du savoir qu'il affecterait gravement a ce comportement la tranquillité de la personne visée, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais ou de l'une de ces deux peines seulement." o The Digital Code contains no definition of harassment, making this provision very broad and vague.

[533] Id, Article 356: "*Quiconque aura, intentionnellement, créé, téléchargé, diffusé ou mis à la disposition du public par le biais d'un systems informatique des écrlts, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idees ou de théories, de idées raciste, tribaliste ou xénophobe ou sous quelque-forme que ce soit […]*":

	○ In contrast to the provision above, this crime does not require an intention to harm the targeted person, but only that the harasser knew (or should have known) the likely effect of the behaviour. ○ The offence above, where there is purpose, results in a prison sentence *and* a fine. The penalty for this offence includes the option of a prison sentence *and/or* a fine.
Article 360: False information	It is an offence to initiate or relay false information against a person through social networks, computer systems, electronic communication networks or any form of electronic medium. The penalty is penal servitude for one to six months and a fine, or one of these penalties only. "Quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sodaux, des systèmes informatiques, des réseaux de communication électronique de ou toute forme de support électronique, est puni d'une servitude pénale d'un à six mois et d'une amende de cinq cent mille à un million de Francs congolais ou de l'une de ces peines seulement." ○ This offence has the potential to chill free speech severely, since it would be difficult if not entirely impossible to know if each and every aspect of a communication was true. Note that there is no requirement that the "false information" initiated or relayed must have caused any actual harm. ○ This is one of the few offences that specifically mentions social networks
Article 361: Negation, gross minimization, approval or justification of international crimes or sexual violence	It is an offence to broadcast or make available through a computer system or an electronic communications network data which denies, minimises, endorses or justifies acts constituting the crime of genocide, war crimes, crimes against humanity, crimes of aggression and/or sexual violence as defined by international instruments and the Congolese Penal Code and recognized as such by a final decision by a national or international court. The penalty is penal servitude for 10 to 20 years and a fine of one to six Congolese francs. ○ This offence is broader than many similar offences in the SADC region and has the potential to undermine political debate on some issues – such as whether a particular prison sentence was justified in a case of sexual violence. The reference to "crimes of aggression" is also very wide. ○ Although the paragraph heading above this provision refers to "gross minimisation" ("*minimisation grossière*"), the text of the provision refers only to "minimising" ("*minimisent*"). ○ The *minimum* penalty for this offence is very high: imprisonment for 10 years and a fine of one million Congolese francs.
Article 362: Incitement or provocation to commission of terrorist acts and apology for terrorist acts	It is an offence, by means of a computer system or an electronic communications network to incite or directly provoke acts of terrorism. The punishment will be in conformity with Articles 157 to 160 of the Congolese Military Penal Code. ○ The paragraph heading above this provision refers to "apology for terrorist acts" ("*apologie des actes terroristes*"), but the text of the provision covers only incitement and provocation.

Article 371: Cyberespionage	It is an offence to do any of the following acts by or through a computer system, intending or knowing that the offence will benefit a foreign government, a foreign company, a foreign intermediary or a foreign agent qualified as a spy: • to steal or, without authorization, to appropriate, take, carry, hide or obtain fraudulently, artificially or by trickery, information likely to undermine the State security and safety or a commercial or industrial secret; • without permission, to copy, duplicate, illustrate, draw, photograph, download, modify, destroy, photocopy, reproduce, transmit, send, address by mail, communicate or cede a commercial secret; • to collect, purchase, or possess a trade secret, knowing that it was stolen or appropriated, obtained or transformed without authorization; • to attempt or conspire to commit any of these offences. The penalty for a natural person is penal servitude of five to fifteen years and a fine from five billion to ten billion Congolese Francs, or one of these penalties only. The penalty for an organization is a fine of fifteen to twenty billion Congolese Francs.
Article 372: Recording of images relating to the commission of offences	It is an act of complicity in willful attacks on the integrity of the person, to knowingly record by any means on any medium whatsoever, images relating to the commission of offences. It is an offence to knowingly distribute such images. The penalty for distribution is penal servitude for one to five years and a fine. However, this does not apply in the case of the normal exercise of a profession whose purpose is to inform the public, or when it is carried out in order to prove the offence in court.[534] o Although professional journalists appear to be excluded, this offence could inhibit the role of ordinary citizens in exposing crime, particularly crimes committed by law enforcement or government officials.
Article 373: Distribution of instructions for manufacturing destructive devices	It is an offence to broadcast, by means of an electronic communications network or a computer system, methods for the manufacture of destructive devices made from gunpowder or explosive substances, nuclear, biological or chemical materials, or from any other product intended for domestic, industrial or agricultural use. The penalty is penal servitude of five to ten years and a fine. There is an enhanced penalty where the offence has resulted in murder or assassination.
Articles 375, 377-378, 381-382: Infringement of copyright intellectual and industrial property rights or neighbouring rights	There are various offences relating to infringements of copyright and similar rights by means of a computer system or an electronic communications network, or technological applications or devices.

[534] Id, Article 372: "*Le présent article n'est pas applicable lorsque l'enregistrement soit la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public soit lorsqu'il est réalisé afin de servir de preuve en justice*."

Articles 375-376, 379: Copyright infringement, counterfeiting or piracy of computer programmes, software or hardware	There are several offences relating to infringement of the copyright of computer programmes and counterfeiting or piracy of computer software and hardware.

With respect to **penalties** for both technical and content-based offences, conviction for some of the offences results in a minimum term of imprisonment along with a fine – with no option for imposing only one of these penalties. Significantly, one such offence is the vaguely defined crime of online harassment, where this crime is committed with the intent to encourage hateful, tribal and hostile behaviour towards good morals and patriotic values.

Filters: The Digital Code requires internet service providers to inform subscribers of the existence of filtering mechanisms, with failure to do so being a criminal offence.[535]

Identity of subscribers and content creators: Online service providers are required to hold and maintain data likely to allow identification of anyone who controls the creation of any content of the services they provide. They must also obtain guarantees from the editors of online public communications services that the identity of the content creators can be provided. The Public Prosecutor or the Data Protection Authority may require online service providers to preserve or produce this information in accordance with applicable laws.[536]

Persons who edit online public communication services must make available to the subscribers of such services the names of the publication's director and editor, company name, address, email and telephone number.[537]

Take-down provisions: Online service providers are not responsible for the content of information they transmit and to which they give access, if they meet the following conditions:

1. they have not originated the transmission;
2. they have not selected the recipients of the transmission;
3. they have not modified the information in the transmission; and

[535] Id, Article 364.
[536] Id, Article 282: "*Le fournisseur des services en ligne est tenu détenir et de conserver les données de nature à permettre l'identification de quiconque aura contrlbué à la création du contenu ou de l'un des·contenus des services dont ils sont prestataires.*
Il est éqalement tenu de fournir aux personnes qui éditent un service de communication au public en ligne des garanties permettant à celles-ci de satisfaire aux conditions d'identification prévues à la présente ordonnance-loi.
L'Officier du Ministère Public ou l'Autorité protection des données peut requerir aupres des fournlsseurs de services en ligne, conformément à la loi en la rnatiere, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées à alinéa 1 du présent article."
[537] Id, Article 288..

4. they have informed their subscribers of the existence of technical means making it possible to restrict access to certain services, or selected and offered one such means. (art 283)

Internet access providers and online service providers do not incur civil or criminal liability for the activities or information stored at the request of a recipient of their services, if they were unaware of their illegal character, or if they acted promptly to remove the data or to make access to it impossible as soon as they became aware of its illegal nature (art 284).[538]

Internet access providers and online service providers must contribute to the fight against the offences provided for in this ordinance-law by putting in place an easily accessible and visible device allowing anyone to bring to their attention the facts of an infraction of the law.[539]

Knowledge of disputed facts is presumed to have been acquired by a supplier of online services when notified of the following:

1. the date of the notification;
2. if the notifier is a natural person: his name, occupation, residence, birth date, date and place of birth;
3. if the notifier is a legal person: its legal form, its company denomination and its seat of operation;
4. the addressee's name and address or, if it is a legal person, its corporate name and head office;
5. a description of the disputed facts and, if possible, their precise location;
6. the reasons why the content should be removed;
7. a copy of the correspondence addressed to the author or publisher of the contentious information or activities requesting their discontinuation. withdrawal or modification, or any explanation of why the justification author or publisher could not be contacted.[540]

The person who knowingly reports inaccurate information about illegal content or activities to an online service provider, with the aim of obtaining the withdrawal or stopping the dissemination of such content or activities, commits a criminal offence.[541]

Internet access providers and online service providers do not have a general duty to monitor the information they transmit or store, unless requested to do so temporarily by an officer of the Ministry of Public Affairs, the National Agency for Cybersecurity, or an agency responsible for security and maintenance of public order.[542]

[538] Id..Similar rules apply to caching and linking to illegal information. Id, Articles 290-291.
[539] Id, Article 287.
[540] Id, Article 285. The statute refers to notification of *one* of the listed elements ("*La connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il·lui est notifié l'un des elements suivants…*"), but it appears to be intended to refer to a notification containing the listed elements.
[541] Id, Article 365.
[542] Id, Article 286.

Internet access providers and online service providers are required to promptly inform competent authorities of all illegal activities reported to them.[543] They also have a duty to suspend any content likely to infringe morality *("tout contenu sussceptible de porter atteinte à la moralité")*.[544] This broad authority is particularly worrying, particularly in the absence of any further details or definitions as to what this might encompass.

A judicial authority may order any online service provider, and failing that, any internet access provider, to apply specific measures to prevent damage or stop damage caused by the content of an online service, in accordance with applicable laws.[545]

Criminal sanctions: It is a crime for internet service providers to fail to meet any of the obligations placed on them by the Digital Code– with this rule applying to a legal person, as well as to any natural person or any manager of a legal person, that is by law or *de facto* carrying out the activities of an online communication services provider.[546]

C) PENAL CODE OFFENCES RELATED TO FREEDOM OF EXPRESSION

The Penal Code contains a number of content-based offences which seem to be frequently applied in practice to limit freedom of speech. The key provisions of this nature are summarised here.[547]

Criminal defamation is covered by Article 74. It applies to anyone who maliciously and publicly imputes a specific fact to a person that is likely to undermine their honour or reputation, or to expose them to public contempt. The punishment is penal servitude of eight days to one year, and a fine of twenty-five to one thousand zaires, or one of these penalties only. The requirement of malicious intent narrows the offence, in theory, but note that there is no explicit mention of truth or fair comment as defences.

CODE PENAL CONGOLAIS

Article 74: Celui qui a méchamment et publiquement imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur ou à la considération de cette personne, ou à l'exposer au mépris public, sera puni d'une servitude pénale de huit jours à un an et d'une amende de vingt-cinq à mille zaïres ou d'une de ces peines seulement.

[543] Id, Article 287.
[544] Id, Article 287: *Ils sont également tenus, d;une part,d'informer et promptement les autorités compétentes de toutes activités illicites mentionnées qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part suspendre tout contenu sussceptible de porter atteinte à la moralité*".
[545] Id.
[546] Id, Articles 366-368.
[547] Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006 modifiant et complétant le Décret du 30 janvier 1940 portant Code pénal congolais.

Under Article 75, **public insult** can be punished with penal servitude from eight days to two months and a fine of up to five hundred zaires, or one of these penalties only. This is a shocking broad and vague offence that has been frequently applied in practice, as the case studies provided in this chapter illustrate.

CODE PENAL CONGOLAIS

Article 75: Quiconque aura publiquement injurié une personne sera puni d'une servitude pénale de huit jours à deux mois et d'une amende n'excédant pas cinq cents zaïres ou d'une de ces peines seulement.

Article 77 appears to criminalise **insults directed at a person** even if they are not made publically. The penalty is relatively minor, constituting penal servitude of eight days and a fine of a maximum of two hundred zaires, or one of these penalties only.

CODE PENAL CONGOLAIS

Article 77: Sera puni d'une servitude pénale de huit jours et d'une amende de deux cents zaïres au maximum ou d'une de ces peines seulement celui qui aura dirigé contre une personne des injures autres que celles prévues dans les dispositions précédentes de la présente section.

There are also a number of offences that on speech relating to **public authorities**:

- Article 76 punishes **slanderous denunciation** ("*une dénonciation calomnieuse*") **of a judicial authority, a public official or a subordinate**, made verbally or in writing.
- Article 135*bis* makes it an offence to directly **instigate disobedience to the laws**.
- Article 135*ter* makes it an offence **to provoke soldiers to turn away from their military duties and from the obedience they owe to their leaders**, in any way whatsoever.
- Article 136 makes it an offence to **insult**, through words, deeds, gestures or threats, certain **public functionaries in the exercise of their mandate or functions**. The steepest punishment is for insulting a member of the Political Bureau, the National Assembly, the Government, or the Constitutional Court. It is a somewhat lesser offence to insult a member of the courts and tribunals, an officer of a public ministry, a senior officer of the Armed Forces or the gendarmerie, or a governor in this manner. It is a still lesser offence to insult other agents of a public authority. **Insults against government bodies** is a similar crime, under Article 137. However, Article 138*ter* provides that prosecutions for these offences can be initiated only on a complaint from the injured person or the body to which the person belongs.

There are several offences that apply to the dissemination of **false information**:

- Article 199*bis* makes it an offence to knowingly spread false rumours that are likely to alarm the public, worry them, or incite them against "the established powers", where this is done with the intention of bringing trouble to the State. The penalty is imprisonment and a fine, or one of these penalties only.
- Article 199*ter* covers the same acts where they are knowingly committed without the intention of bringing trouble to the State. The penalty is imprisonment and a fine, or one of these penalties only – within a slightly lower range of time or money given the absence of the indicated intention.

- Article 211 makes it an offence to knowingly contribute to the publication, dissemination or reproduction, by any means whatsoever, of false news, fabricated or falsified material or material falsely attributed to third parties where this is done with the intention of disturbing the public peace. It is also an offence to exhibit in public any drawings, posters, engravings, paintings, photographs, objects or images that are likely to disturb the public peace, regardless of intention. The penalty is imprisonment or a fine, or both.

The law is not clear on how to determine what is considered a "false rumour" or "false news" or what the threshold is for deciding that information is likely to alarm or worry the public or incite them against "established powers". Thus, they provide an overly wide degree of discretion to those who enforce the law.[548]

CODE PENAL CONGOLAIS

Article 199*bis*: Quiconque, en répandant sciemment de faux bruits de nature à alarmer les populations, à les inquiéter ou les exciter contre les pouvoirs établis, aura porté ou aura cherché à porter le trouble dans l'Etat, sera puni d'une servitude pénale de deux mois à trois ans et d'une amende de cent à cinq cents zaïres, ou d'une de ces peines seulement.

Article 199*ter*:
Sera puni de un mois à un an de servitude pénale et d'une amende de vingt à cent zaïres ou de l'une de ces peines seulement, celui qui, sans intention de porter le trouble dans l'Etat, aura néanmoins sciemment répandu de faux bruits de nature à alarmer les populations, à les inquiéter ou à les exciter contre les pouvoirs établis.

Article 211: Sera puni d'une servitude pénale de deux mois à trois ans et d'une amende de mille à dix mille zaïres, ou d'une de ces peines seulement:
- celui qui, en vue de troubler la paix publique, aura sciemment contribué à la publication, à la diffusion ou à la reproduction, par quelque moyen que ce soit, de nouvelles fausses ou de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers;
- celui qui aura exposé ou fait exposer, dans les lieux publics ou ouverts au public, des dessins, affiches, gravures, peintures, photographies, tous objets ou images de nature à troubler la paix publique.

Anonymous publications are prohibited.[549]

D) PRESS FREEDOM LAW OFFENCES RELATED TO FREEDOM OF EXPRESSION

The Press Freedom Law enacted in 2023 states that it is considered an "**attack through the press**" ("*atteinte par voie de presse*") for a *media professional* to engage in any act or behaviour during the exercise of his profession that undermines public order, the rights of others or good morals and causes harm. It is also an "**attack**" ("*atteinte*") for a *media user* to violate and damage public order, the rights of others and good morals. Offences by the online press are punished in accordance with the legislation in force in criminal matters. [550] Sanctions for other types of media or for media users are not discussed in this provision, but presumably also fall under the criminal law.

[548] "LEXOTA Country Analysis: Democratic Republic of Congo", last updated July 2022.
[549] Code pénal congolais, Article 150h-150i.
[550] **L'ordonnance-loi n°23/009**, Article 113.

It is an offence for anyone **acting in bad faith** to publish, disseminate or transmit **false news or allegations, or inaccurate facts**, by way of written press, online press, broadcast media or any other medium, where this has disturbed public order, aroused fear among the population, or caused the destruction of public property.[551] This also applies to false information against magistrates, civil servants or agents invested with the public authority in respect of the exercise of their functions.[552] It is similarly an offence, acting in bad faith, to publish, distribute or reproduce false news, fabricated or falsified material or material falsely attributed to third parties where this has disturbed the public peace.[553] These acts will be "punished according to law" - – which seemingly refers to the Penal Code provisions on false information discussed above, with the addition of a bad faith requirement and a requirement that actual harm must result in respect of the press. The publication, distribution or reproduction of false information in bad faith will be punished in accordance with the code of military justice when it has shaken the discipline or morale of the armies or hindered a war effort of the nation.[554]

It is an offence to **falsely claim to be a media professional**, punishable under the relevant provisions of the Penal Code.[555]

There are several points on **legal proceedings** and **information about crimes committed**. It is also punishable under the Penal Code for the press to violate the secrecy of a criminal investigation, to undermine the presumption of innocence in respect of a criminal proceeding, It is also prohibited to publish by any means photographs or portraits of people with the aim of thus disclosing all or part of the circumstances of a murder, an assassination, a suicide, a poisoning, threats, blows and injuries, attacks on morality and public morals or kidnapping. A further offence is the publication of information about the trial of a minor child or any trial in which a minor child is involved.[556]

It is also forbidden to offer, give or sell to **minor children** publications of any kind inciting to debauchery, prostitution, crime or the consumption or trafficking of drugs, alcohol or tobacco.[557]

It will also be punished according to the Penal Code -

- to directly provoke attacks on persons, in particular murder, assassination, theft, rape, violence, destruction and terrorism
- to apologise for war crimes, crimes against humanity, crimes of genocide or crimes of terrorism;
- to directly incite hatred, in particular religious, ethnic, tribal, regional or racial hatred.[558]

[551] Id, Article 120
[552] Id, Article 124.
[553] Id, Article 123.
[554] Id.
[555] Id, Article 124.
[556] Id, Articles 125-126.
[557] Id, Article 126.
[558] Id, Article 136.

The Press Freedom Law also contains provisions concerning which specific media professionals have criminal, civil and professional liability for wrongs committed by the press.[559]

E) STATE SURVEILLANCE

The provisions of **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** that justify interference with information privacy, have been analysed as follows:

> *These exceptions include the lifting of the secrecy of correspondence at the request of the public prosecutor's office or with the authorisation of the courts and tribunals in the context of a judicial investigation, and derogation from this secrecy by the competent services – including the ANR – for reasons of internal and/or external state security, national defence or public order (Article 126). Next, Article 127 provides that "only the needs of information motivated by the requirements of the ultimate demonstration of the truth in a judicial case may authorise the Public Prosecutor's Office at the Court of Cassation to prescribe the interception, recording and transcription of correspondence emitted by means of telecommunications and information and communication technologies". Article 129 goes further by empowering the public prosecutor's office at the Court of Cassation to request any agent of a service or body to install a device necessary to carry out the operations indicated in the previous Article 127(1), while Article 128 provides that this decision may last for three months, renewable for the purposes of the investigation. The vagueness of these exceptions leads to disproportionate infringements of these rights in the Democratic Republic of Congo, which can be extended for as long as the person making the decision invokes the need for the investigation, as the number of renewals is not limited.*[560]

Decree-Law No. 003-2003 on the creation and organization of the National Intelligence Agency authorises state surveillance of any persons or groups suspected of carrying out an activity that could undermine state security, while **Decree-Law 1-61 of 25 February 1961 on State security measures** allows the Minister of the Interior to place persons who undermine state security under surveillance by a simple written decision. The broad justification of "state security" is reportedly abused as a means of stifling political opponents.[561]

In addition, **Ministerial Order No. CAB/MIN/PT&NTIC/AKIM/KL/Kbs/002 of 10 June 2020** has authorised the establishment of a Central Electric Identity Register (CEIR), as well as allowing the government to monitor mobile telephone subscribers. Through this registry, the government has access to information about millions of mobile phones that can facilitate State surveillance.[562]

---

[559] Id, Articles 127-128.
[560] Trésor Maheshe Musole and Jean-Paul Mushagalusa Rwabashi, "Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection", Media Policy and Democracy Project, December 2021, page 20.
[561] Id, page 21.
[562] Id, page 20.

In general, the legal criteria used to justify violations of privacy are based on national defence, national security, criminal investigations, the protection of public order and the prevention of crime, without much detail.[563] Yet, even though many of the laws relied upon to authorise state surveillance are broad and vague, there were reports that the government monitored private online communications without appropriate legal authority.[564]

At the same time, there are limits on citizen surveillance. Article 58 of **Law no. 20/17** requires that remote surveillance and video surveillance systems, in both closed private spaces and spaces open to the public, are permitted only after being declared to ARPTIC, which will provide a certificate and inform the Minister of the declaration. The terms and conditions for granting approval are set by ministerial order.

F) SIM CARD REGISTRATION

SIM card registration is mandatory and has been discussed above in the section on obligations of service provers in connection with cybercrime.

G) TAKE-DOWN NOTIFICATIONS

There are several provisions of the Digital Code which, taken together, constitute the equivalent of a take-down procedure. These have been discussed above.

6.5 ELECTION LAW AND FREEDOM OF EXPRESSION

DRC's next general election (which will include a presidential election) is scheduled for 20 December 2023.

Elections in DRC are regulated by the **Independent National Electoral Commission** ("*Commission Électorale Nationale Indépendante*") **(CENI),** which is established by the Constitution.[565] According to Freedom House, CENI is viewed by opposition parties and civil society as lacking independence and supporting the president. Freedom House also reports that President Tshisekedi reformed the CENI in July 2021, allocating seats for civil society groups, the ruling coalition, and the opposition. This move was

[563] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 24.
[564] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[565] Democratic Republic of the Congo 2005 Constitution, Article 211. CENI is governed by the Loi organique n° 10/013 du 28 juillet 2010 portant organisation et fonctionnement de la Commission Électorale Nationale Indépendante telle que modifiée et complétée par la Loi organique n° 13/012 du 19 avril 2013 et la Loi organique n° 21/012 du 03 juillet 2021 (Textes coordonnés et mis à jour) ("Organic Law No. 10/013 of 28 July 2010 on the organization and functioning of the Independent National Electoral Commission as amended and supplemented by Organic Law No. 13/012 of 19 April 2013 and Organic Law No. 21/012 of 03 July 2021 (Coordinated and updated texts)"). The CENI website can be found here.

criticised because the balance of the body tilts towards the government, which gives Tshisekedi control over future elections.[566]

DEMOCRATIC REPUBLIC OF THE CONGO 2005 CONSTITUTION

Article 211
An Independent National Electoral Commission with legal personality is established.
The Independent National Electoral Commission is charged with the organization of the electoral process, in particular the registration of voters, the maintenance of the electoral roll, voting operations, the counting of votes and any referendum.
It ensures the regularity of the electoral and referendum process.
An organic law establishes the organization and the operation of the Independent National Electoral Commission.

This brief overview of past election controversies provides context for the forthcoming elections:

The DRC gained independence from Belgium in 1960. Its post-independence history is bloody: the first post-independence leader, Patrice Lumumba, was assassinated in 1961. In 1965, military officer Mobutu Sese Seko assumed power after a period of civil war. Mobutu ruled his one-party state (which he renamed Zaire) until 1996, when he was ousted by an armed coalition led by Laurent Kabila. However, the country remained dangerously unstable and effectively in a state of civil war. In 2001, Laurent Kabila was assassinated by his bodyguard and was succeeded by his son, Joseph Kabila. Although Joseph Kabila is credited with introducing a number of important reforms, most notably a new constitution, his democratic credentials remained extremely poor. The last election which he won (in 2011) is disputed and lacked credibility due to widespread irregularities. President Kabila's second five-year term of office ended in December 2016, but the DRC failed to hold elections and he ruled without an electoral mandate, albeit with the backing of the Constitutional Court. In May 2016, the Constitutional Court, in a heavily criticised judgment, interpreted section 70 of the constitution, which provides that the president continues in office until the assumption of office of his successor, as entitling President Kabila to remain in office without an election having taken place. Critics argue that the Constitutional Court should have found section 75 of the constitution applicable — this provides for the Head of the Senate to assume office temporarily in the case of a presidential vacancy.

In August 2018, President Kabila announced he would not be running for a third term and the ruling party chose Emmanuel Shadari, seen as a Kabila loyalist, as its candidate for the presidential elections. The presidential elections were held on 30 December 2018. The outcome of the election was extremely controversial. The Electoral Commission and the Constitutional Court certified that Felix Tshisekedi, an opposition figure, won the election. However, powerful institutions, such as the Catholic

[566] "Freedom in the World 2022: Democratic Republic of the Congo", Freedom House, section A3; Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).

Church, disputed this, and it, and the international press, reported that another opposition leader, Martin Fayulu, had, in fact, won by a landslide as evidenced by leaked election data.

At the time, the African Union called for the DRC to delay announcing the election results due to serious discrepancies between the provisional results announced by the Electoral Commission and the actual ballots cast. This was ignored and, on 24 January 2019, Mr Tshisekedi (apparently with former-President Kabila's backing) was sworn in as the country's new president. Mr Tshisekedi's election has since been accepted by the European Union and the United States of America. The AU also backtracked on its objections to the election results as it elected Mr Tshisekedi the second vice-president of the AU on 16 February 2019.[567]

Looking at some of the freedom of expression issues in the last general election, CENI's decision to **refuse accreditation** to several international election observers and **media representatives** in the 2018 elections was internationally criticised. Another criticism of the 2018 election process was that Government authorities and the State Security Forces **prevented opposition parties from holding public meetings, assemblies, and peaceful protests**, or used force to prevent or disrupt their events. There were also reports that the government exercised **political influence in the distribution of media content during the election campaign**.[568]

RTNC, the **national broadcaster**, reportedly committed over 40% of its campaign airtime to the ruling party candidate and **failed to grant all candidates equal access**, while the CSAC did not enforce its decision to allocate equal airtime to all candidates, with no sanctions being imposed on RTNC or other media for their unequal coverage.[569]

During the 2018 campaign period, some candidates conducted digital campaigns on **social media platforms** even though internet reach in DRC is not widespread. It is reported that fake news and misinformation was rife on social media platforms at key stages of the process. [570]

Right after the general elections were held on 30 December 2018, the **government shut down all primary telecommunications**. A senior government official said that internet and SMS services were cut to preserve public order after "fictitious results" began circulating on social media, and that the communications services would be restored only after the publication of election results on 6 January. This step reportedly hindered the ability of electoral observers and witnesses to relay information from rural polling stations. The UN Special Rapporteur on freedom of expression at the time stated that this shutdown was in clear violation of international law and could not be

[567] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 182 (footnotes omitted).
[568] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 3.
[569] "Democratic Republic of the Congo 2018 Harmonized Presidential, Parliamentary and Provincial Elections: Expert Mission Report", The Carter Center, undated.
[570] Id.

justified by any means, urging government authorities to restore internet services as a matter of urgency.[571]

Despite the election controversies, the US State Department notes that "the 2019 inauguration of President Tshisekedi was the first peaceful transfer of power in the country's history".[572]

One recent analysis referred to the forthcoming 2023 elections as "the most unpredictable on the continent in 2023" and provides the following overview of the political environment:

> *The elections in the Democratic Republic of the Congo (DRC) mark another important inflection point in this country's long and elusive quest for democracy. To make progress, this country of more than 100 million people must overcome its deep-seated legacies of fraudulent, patronage-based, and opaque electoral practices institutionalized over the decades by the regimes of Mobutu Sese Seko and Laurent and Joseph Kabila.*
>
> *The incumbent, President Felix Tshisekedi, is seeking a second 5-year term. Son of the esteemed democracy champion, Etienne Tshisekedi, Felix Tshisekedi had an ignoble start to his presidency. In the view of many, he cut a power-sharing deal with the outgoing president, Joseph Kabila, to be declared the victor of the December 2018 elections. Independent analysts, including the respected election monitoring group, the National Episcopal Conference of Congo (CENCO), indicated that the genuine winner by a commanding margin was the leading opposition candidate, Martin Fayulu.*
>
> *Bowing to pressure from Kabila, the African Union and international democratic actors declined to demand a recount as called for by CENCO and many governments. A challenge of Tshisekedi's first term, thus, has been to overcome weak legitimacy in the eyes of his compatriots.*
>
> *Once in office, Tshisekedi has been able to claw away some influence from Kabila's entrenched grip on the institutions of power. This includes replacing the Kabila-backed speaker of the National Assembly as well as the influential prime minister. Tshisekedi has also made some progress on reforms. Perhaps most notable has been his reducing the repressiveness of the security services by replacing certain senior intelligence and internal security officials who had been sanctioned for human rights violations. Tshisekedi has also made headway in replacing some Kabila loyalists within senior ranks of the judiciary.*
>
> *This progress is noteworthy in that, upon stepping down, Kabila continued to exert great influence over the machinery of government in the DRC. Kabila's Common Front for Congo (FCC) alliance controlled 350 of the 500 seats in the National Assembly as well as a majority of ministries, judicial appointments, and senior officials throughout the security sector. Many observers expected Tshisekedi to be little more than a front man for Kabila's continued wielding of power behind the scenes.*

[571] "UN expert urges DRC to restore internet services", UN Office of the High Commissioner on Human Rights, 7 January 2019.
[572] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, "Executive Summary".

Tshisekedi was also a prominent defender of democratic norms on the continent during his 1-year tenure as African Union Chairman in 2021-2022.

Nonetheless, in the process of winning over Kabila allies in government, democracy activists worry that Tshisekedi has adopted some of [the] same tactics as his predecessor. This includes the reliance on patronage to direct the unwieldy bureaucracy of the Congolese state.

Finance Minister Nicolas Kazadi noted, for example, that the budget for exceptional security expenses had increased tenfold, though with little transparency over how these resources were improving security given the country's notoriously corrupt and abusive security sector.

Tshisekedi and his family have been linked to opaque deals with Chinese businesses for access to artisanal copper, cobalt, and diamonds. Tshisekedi has also been criticized for not doing enough to rein in the mechanisms of state capture employed by Kabila. This includes a $6-billion infrastructure-for-resources swap with Chinese state-owned firms dubbed the "deal of the century" and the embezzlement of $3.7 billion in state funds by internationally sanctioned mining magnate, Dan Gertler, through Kabila-endorsed contracts.

Tshisekedi controversially appointed close ally Denis Kadima as the new commissioner of the Independent National Election Commission (CENI) in 2021. Tshisekedi also modified the allocation of seats within CENI. While opposition parties and civil society are represented, critics feel the distribution still favours the ruling party.

Many democracy advocates, moreover, are critical that the Tshisekedi-led National Assembly failed to pass an amendment that would require CENI to adopt electoral best practices such as announcing electoral results at each polling center. Tallying and reporting of aggregate results from a central location is less transparent and more prone to rigging. In Kenya, for example, results announced at polling stations are final and cannot be altered. Additionally, the DRC relies on candidates gaining a plurality of votes rather than an absolute majority, making it easier for a candidate to win by solely appealing to their base rather than building a more inclusive coalition.

Tshisekedi faces credible opposition from numerous quarters. Most prominent among these is Martin Fayulu, the former ExxonMobil executive widely perceived to have won the 2018 election. Born in Kinshasa, Fayulu commands a broad following across the DRC's highly diverse constituencies. Moïse Katumbi, a former governor from the southeastern region of Katanga, is another popular rival. He was seen as such a threat by Kabila that the former leader launched several gratuitous court cases against him, forcing Katumbi into exile. Former Kabila Prime Minister Augustin Matata Ponyo Mapon is another prominent entrant to the presidential race. In 2018, there were nearly two dozen presidential contenders. The presence of so many candidates introduce considerable unpredictability given the DRC's single-round plurality system.

While the DRC's electoral institutions and oversight mechanisms may be weak, the country has a vibrant and organized civil society committed to a democratic system of government. These groups continue to demand transparency and popular participation in elections and holding leaders accountable to citizen interests. Among the most prominent, CENCO deployed over 40,000 election monitors in 2018. Through the experience gained from multiple cycles of parallel vote counting processes, it is

increasingly difficult for candidates to credibly claim outcomes that deviate significantly from independent tallies.

Another wild card in the 2023 election is the ongoing instability in the east of the country. This is a multilayered conflict involving rivalries between Rwanda and Uganda, access to and trafficking of the DRC's vast and unregulated mineral deposits, 140 local armed groups, ethnic rivalries, and legacies of previous conflicts in the Great Lakes region. Prospects of Chinese and Russian interests joining the competition for resources in the region adds another level of complexity. Perceptions that Tshisekedi may have made opaque deals for DRC's resources also sets off a strong nationalist resentment that may have political consequences.

The resurgence of the threat from the armed group M23 in late 2021 has heightened tensions among all parties and added to the displacement of more than 5.5 million people from Ituri, North and South Kivu, and Tanganyika Provinces. The deployment of the East African Standby Force at the end of 2022 has helped tamp down tensions, though this will need to be translated into longer-term mediated solutions.

Ongoing instability may affect the ability of these eastern provinces to vote—an issue also faced in 2018. A full-blown regional conflict would clearly scramble the entire electoral process. Tshisekedi advisors have suggested that the elections may need to be delayed due to the unrest. This is fueling concerns that the instability in the east may be used as a pretext for Tshisekedi to prolong his tenure—harkening back to Kabila's 2-year delay before holding elections after his second term had expired.

The 2023 elections will say much about the trajectory of the Tshisekedi presidency. Will it hold to his stated democratic and reformist aspirations? Or will it fall into the well-worn governance norms in DRC—building exclusive patronage networks at the expense of public goods and services?

With so many uncertainties, the DRC polls may be the most unpredictable on the continent in 2023. While the DRC does not have a strong track record of transparent and credible elections, this remains the aspiration of millions of Congolese citizens. Experience has also shown that civil society will not blithely accept a fabricated outcome. Much may once again come down to the courts—and how regional and international actors respond.[573]

The CSAC adopted a new **directive on media regulation during the electoral campaign** on 21 June 2023.[574] However, this directive could not be located online as of August 2023.[575]

[573] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
[574] Christel Insiwe "Élections: Le CSAC adopte la directive de réglementation de la campagne électorale dans les medias", *7sur7.cd*, 22 juin 2023; Emille Kayomba, "Processus électoral : le CSAC et la CENI en concertation pour des bonnes élections", *b-onetv*, 14 juillet 2023.
[575] As a point of comparison, the previous "Directive du Conseil Supérieur de l'Audiovisuel et de la Communication n°CSAC/AP/001/2015 du 05 mars 2015 relative à la campagne électorale à travers les medias" is available here.

CHAPTER 7

ESWATINI

CHAPTER 7: ESWATINI

ESWATINI KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **111th globally; 29th out of 48 African countries** "Renamed eSwatini by royal decree in 2018, the former Swaziland is an absolute monarchy that prevents journalists from working freely and independently."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: eSwatini's 2005 Constitution **24. PROTECTION OF FREEDOM OF EXPRESSION** 1. A person has a right of freedom of expression and opinion. 2. A person shall not except with the free consent of that person be hindered in the enjoyment of the freedom of expression, which includes the freedom of the press and other media, that is to say – a. freedom to hold opinions without interference; b. freedom to receive ideas and information without interference; c. freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons); and d. freedom from interference with the correspondence of that person. 3. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision – a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; b. that is reasonably required for the purpose of – i. protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings; ii. preventing the disclosure of information received in confidence; iii. maintaining the authority and independence of the courts; or iv. regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting or television or any other medium of communication; or c. that imposes reasonable restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under the authority of that law is shown not to be reasonably justifiable in a democratic society.
KEY LAWS: • Computer Crime & Cybercrime Act 6 of 2022 • **Sedition and Subversive Activities Act 46 of 1938** (certain provisions)

• Suppression of Terrorism Act 3 of 2008 (certain provisions)
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: eSwatini has a data protection law.[576]
ACCESS TO INFORMATION: eSwatini has no access to information law.

7.1 CONTEXT

The eSwatini media and civil society landscapes, as well as the general human rights climate, are characterised by continuous and ongoing repression.

The publication of newspapers requires registration under the **Books and Newspapers Act 20 of 1963.** Newspaper editors must be resident in eSwatini.[577]

The **Swaziland Communications Commission Act 10 of 2013** establishes a body that regulates all communications services in the country, including postal services, broadcast media and the internet. This body, now known as **eSwatini Communications Commission (the SCC)**, resorts under the Ministry of Information, Communication and Technology. The Board is appointed by the minister in consultation with the relevant Cabinet standing committee, and many of its functions require ministerial approval.[578] The SCC is thus not an independent authority. although it is charged with acting in "an objective, transparent, proportionate and non-discriminatory manner".[579] The creation of this Commission was reportedly the catalyst for the enactment of a trio of related laws in 2022: Computer Crime and Cyber Crime Act, 2022, the Data Protection Act, 2022, and the Electronic Communications and Transactions Act, 2022.[580]

The state broadcaster, the eSwatini Television Authority (STA), is established by **The Swaziland Television Authority Act, 1983.** It operates under the direction of a Board of Control, appointed by the minister, which monitors "the content of programmes and other transmissions to ensure that they conform with acceptable moral standards".[581]

Regulation of the broadcasting sector is in the process of being updated by the **eSwatini Broadcasting Bill 20 of 2019**, which has been repeatedly revised and delayed for years and is, as of mid-2023, awaiting Royal Assent.[582] According to press reports, this Bill will create a Broadcasting Corporation that merges the eSwatini Television

[576] Data Protection Act 5 of 2022.
[577] Books and Newspapers Act 20 of 1963, section 4. A "newspaper" is defined in section 2 to include "any printed matter containing news, or intelligence, or reports of occurrences of interest to the public or any section thereof, or any views, comments or observations thereon printed for sale or distribution and published periodically or in parts or numbers at intervals not exceeding one month but does not include a visiting or business card, billhead, letter-head, price list, annual report, trade circular, trade advertisement or other legal or trade or business document".
[578] The Swaziland Communications Commission Act 10 of 2013, read with section 6 of The Public Enterprises (Control And Monitoring) Act 8 of 1989.
[579] The Swaziland Communications Commission Act 10 of 2013, section 6.
[580] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
[581] The Swaziland Television Authority Act, 1983, sections 9-10 in particular.
[582] Personal communication with local expert, July 2023.

Authority and the eSwatini Broadcasting and Information Services (the State radio service). It would also create a three-tier broadcasting system for public, commercial and community broadcasting, transform state-owned media houses into independently controlled entities, and regulate the broadcasting sector in a way that will improve accountability and professionalism.[583]

The media has a self-regulating body in the form of the **Media Complaints Commission**, which was registered in 2011.[584] It has been reported that this body is underfunded, and its independence has been questioned.[585] The Commission's role is to ensure the implementation of the Swaziland Journalists Code of Ethics and to provide aggrieved persons with an opportunity for redress outside the courts in respect of the print media. However, as of 2018, it was reported that only two publications, the *Times* and the *Observer*, were participating in this body. The broadcasting sector is not engaged in the Commission and has no complaints body of its own.[586]

In general, according to one journalist, there is "not much freedom to report as most of the media houses are state owned and even the independent media outlets use self-censorship so that their licences wouldn't get revoked".[587]

7.2 CONSTITUTION

Section 24 of the Constitution is quoted in the table on the first page of this chapter. With regard to the grounds for justifiable limitation of the right which it enumerates, it has been observed that:

> *These limitations are generally not out of step with international norms for limitations on freedom of expression, except in one respect, namely, the restriction imposed on public officers. Obviously, many public officials do have secrecy obligations, particularly in defence, intelligence and police posts. Nevertheless, the general ability of whistleblowers in the public service to bring illegal conduct, including corruption, to the attention of the media in the public interest is a critical part of a functioning democracy. Consequently, such limitations provisions could have a chilling effect on public servants, unduly preventing the disclosure of official misconduct.*[588]

[583] Sifiso Nhlabatsi, "Parliament Passes Broadcasting Bill", *Eswatini Observer*, 16 October 2020; "Eswatini Broadcasting Bill heralds new hope", *Inhlase*, 31 October 2020; "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), section 3.
[584] "Eswatini: Misa Applauds Registration of Media Complaints Commission", Media Institute of Southern Africa (Windhoek) press release, 15 June 2011.
[585] "Freedom of the Press 2016 – Swaziland", Freedom House, "Legal Environment".
[586] "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 47.
[587] Journalist quoted anonymously in Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
[588] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 246.

In the 2014 *Swaziland Independent Publishers* case, the Supreme Court was asked to consider whether the conviction for contempt of court of editor and journalist Bheki Makhubu, along with the publisher of his articles, constituted an unjustifiable infringement of the right to freedom of expression. The case concerned two articles published in *The Nation* magazine. One article criticized the Swazi judiciary on the basis that they "could not be bothered to interpret the Constitution". Even though this article used words such as "criminal" and "treasonous" with reference to the judges, the Court found that this was merely the opinion of the author and overturned the conviction in respect of this article, saying that its criticisms of the judiciary were "bland and eminently permissible within the context of Swaziland's constitutional freedom of the press guarantees". The second article the second article compared the Chief Justice to Tarzan, a "high school punk" and a "street punk". The Court found that this article, in contrast to the other one, "mounted a scurrilous and unwarranted attack upon the judiciary as a whole, and upon the administration of justice in this Kingdom" and that the conviction of contempt of court for "scandalising the judiciary" was warranted in this instance but reduced the sentence imposed by the lower court.[589]

In 2015, the case of *Maseko v R* again considered convictions for contempt of court. Journalists Bheki Makhubu and Thulani Maseko wrote articles in *The Nation* magazine again criticizing the judiciary system for partiality and lack of independence. Both were arrested, charged, and convicted for two counts of contempt of court, and sentenced to two years in prison, with a fine being imposed on the publisher of the magazine. In the Supreme Court, the State Prosecutor conceded the appeal, The judge found that the case had constituted "a travesty of justice," noting that the High Court did not properly balance the right to freedom of expression with the authority of the courts. The Supreme Court judgment stated that the "importance of freedom of expression in promoting democracy and good governance cannot be over emphasized." The Supreme Court overturned the convictions and ordered the immediate release of the two journalists.[590]

In 2016, in the case of *Maseko v The Prime Minister of Swaziland*, the High Court struck down certain sections of the Sedition and Subversive Activities Act No. 46 of 1938 and the Suppression of Terrorism Act 3 of 2008 on the grounds that they infringed the fundamental rights to freedom of expression and association in a manner that was not reasonably required and proportionate. Thulani Maseko and Maxwell Dlamini were both charged with sedition, subversion, and contravention of the Terrorism Act on the basis of speeches at a May Day celebration in 2014. Dlamini along with two other political activists had been charged with seditious intention in 2013 for participating in a rally while carrying a banner calling for the boycott of the 2013 national elections. Maseko had previously been charged with "uttering words with a seditious intention" after speaking at a May Day Celebration in 2009. With respect to the Sedition and Subversive Activities Act, the High Court found that the challenged provisions of this law (sections 3(1), 4(a) and (e), and 5) were unconstitutional since it was unlawful to limit free speech for the sole purpose of shielding the government from criticism or discontent, which did not lie within the permissible constitutional

[589] *Swaziland Independent Publishers v The King* [2014] SZSC 25, 30 May 2014; see the case summary by Global Freedom of Expression here.
[590] *Maseko v R* [2015] SZSC 03, 29 July 2015; see the case summary by Global Freedom of Expression here.

grounds for limitation. Regarding the Suppression of Terrorism Act, the Court found that the State did not offer sufficient justification to save the impugned provisions (portions of section 2(1) and sections 11(1)(a) -(b), 11(2), 28 and 29(4)).[591] However, the State is now appalling this judgment. In 2022, the Supreme Court condoned the delays that should have caused the appeal to lapse, holding that the State's appeal can proceed, on the grounds that the constitutional issues at stake are too important to be decided by default.[592]

It should be noted that human rights lawyer Thulani Maseko, who was involved in two of the cases discussed here, was tragically shot dead by unknown assailants at his home in eSwatini on 21 January 2023 – the same day on which the King of eSwatini made a veiled threat against members of the country's pro-democracy movement.[593]

7.3 CASE STUDIES

Reporters without Borders observes that any criticism of the monarchy "is liable to lead to a trial and heavy penalties", noting further that "dozens of draconian laws muzzle freedom of expression and information, and the judicial system is often used to undermine journalism.[594] It also states that journalists are often arrested and subjected to violence.[595]

The US State Department's 2022 report on human rights practices in eSwatini contains the following overview:

> *Civil society tension remained high since 2021 unrest, resulting in reports of citizens, businesses, and even government officials and parliamentarians not exercising their right to free speech in fear of direct and indirect retaliation by the government, and fear of targeting by unidentified opposition elements that claimed responsibility for violent actions. [ ] Although journalists have spoken out against the government in recent years, criticism of the king was discouraged by government and traditional leaders. According to an October report by the Campaign for Free Expression and the Inhlase Center for Investigative Journalism, a widespread culture of self-censorship existed among journalists, especially regarding reporting related to the king and the royal family. Most journalists and broadcast media avoided criticizing the palace due to fear of reprisals such as being professionally ostracized or losing paid government advertising in their outlets. One independent monthly magazine that covered sociopolitical topics reportedly lost advertising revenue from a parastatal after it published criticism of the royal family. Self-*

[591] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016; see the case summary by Global Freedom of Expression here. See also Angelo Dube and Sibusiso Nhlabatsi, "The (Mis)application of the Limitation Analysis in *Maseko and others v Prime Minister of Swaziland and others*" [referring to the dissenting judgment], *Law, Democracy and Development*, Vol 22, 2018.
[592] Peter Fabricius, "Historic Swazi court judgment striking down parts of sedition and terrorism laws is under threat", *Daily Maverick*, 29 September 2022,
[593] "eSwatini: Experts condemn killing of human rights defender Thulani Maseko, demand accountability", UN Office of the High Commissioner on Human Rights, 26 January 2023; Pavan Kulkarni, "Assassination of Thulani Maseko has killed prospects of peaceful struggle in Swaziland", *People's Dispatch*, 27 January 2-23.
[594] "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Legal framework".
[595] Id, "Safety".

> *censorship only applied to matters regarding the palace and was virtually non-existent in relation to the government, which media frequently criticized. Daily independent newspapers routinely criticized government corruption and inefficiency but avoided criticizing the royal family. […]*[596]

A representative of the Media Institute of Southern Africa (MISA) stated: "The government is uneasy with the free flow of information. Every time a journalist reports something critical about the government, they and their families are hunted. The government and the King do not want press freedom in the country, because this would expose the underlying corruption and problems in the country".[597] In October 2022, the Inhlase Centre for Investigative Journalism described a "deeply concerning political and economic environment in Eswatini, where, following the June 2021 unrest, citizens are afraid to speak out to express their political views or to demand service delivery; journalists' work is being compromised by threats to their lives; and the right to protest is under attack." [598]

In 2022, a group of about 20 correctional officers reportedly **assaulted** Nomthandazo Maseko, a reporter for the news website *Swati Newsweek, after she* livestreamed a protest outside a prison where the local prison where two pro-democracy members of Parliament were detained. She stated that the correctional officers hauled her out of her care, slapped her, kicked her and beat her with sticks. She also stated that one officer pointed a gun at her and threatened to shoot her.[599]

In 2021, two South African reporters for the South African news website *New Frame,* Magnificent Mndebele and Cebelihle Mbuyisa, were **arrested** after attending the funeral of a police shooting victim. Soldiers reportedly threatened the journalists at gunpoint, seized their cameras, and forced them to delete footage of the funeral. They were then taken to a police station for interrogation, where they were tortured; amongst other assaults, police held plastic bags over their heads to suffocate them. They were released several hours later, and both received medical treatment at a local hospital. They both returned to South Africa the next day.[600]

In 2021, two Members of Parliament representing an opposition party, Mduduzi Bacede Mabuza and Mthandeni Dube, were charged under **section 5(1) of the Suppression of Terrorism Act, 2008** for "terrorist acts" in respect of three events: a gathering on 5 June 2021 where one of the MPs allegedly suggested that there be a democratically elected Prime Minister, rather than one appointed by the King; a meeting at a restaurant, where one of the MPs allegedly encouraged sending petitions to Tinkhundla centres (local government constituencies); and a speech in which one MP allegedly said "*Akuklalwa Namuhla*" (roughly translated to "not

596 "2022 Country Reports on Human Rights Practices: eSwatini", US State Department, section 2A.
597 Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021, quoting Nqaba Matshazi, MISA's fundraising and regional campaigns coordinator.
598 Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 3.
599 "eSwatini prison officers assault, threaten to shoot reporter covering pro-democracy protest", Committee to Protect Journalists, 16 February 2022.
600 "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.

sleeping today") – in other words, the "terrorist acts" constituted the voicing of political opinions that made no reference to violence.[601]

In 2020, Zweli Martin Dlamini, editor of the website *Swaziland News*, was arrested in connection with **sedition** after publishing two articles critical of the King. Police seized his laptops, cell phones, hard drives, and other electronic devices and took him into custody. There, police officers reportedly handcuffed him to a bench and tried to suffocate him by putting a plastic bag over his head. He was released without charge after some six hours, but police did not return the confiscated devices. Dlamini fled to South Africa the next day, where he received medical attention. His lawyers filed a complaint with eSwatini's Commission on Human Rights and Public Administration, accusing the police of "torture and humiliation" and violation of Dlamini's right of expression. The next day, *Swaziland News* published a report questioning the state of the King's health during the Covid pandemic. Police again raided Dlamini's home and confiscated some material, without producing a search warrant. They took Dlamini's wife into custody, leaving the couple's two young children alone in their home. She reported that she was questioned about Dlamini's whereabouts, slapped and verbally abused. She also alleged that police officers handcuffed her and covered her head with a plastic bag to suffocate her. She was released without charge after about three hours. The government denied that Dlamini's arrest related to his criticism of the King, stating that he had allegedly violated Covid regulations that criminalised the spreading of false news about the virus.[602]

In 2020, an assistant weekend editor of the privately owned newspaper *The Times of eSwatini*, Welcome Dlamini, received **threatening text messages** from a person who claimed to be a member of a banned opposition party after the newspaper published a column *supporting* eSwatini's system of government. He received another death threat via text after he opened a case with the police.[603]

In another 2020 incident, police officers reportedly raided the home of Eugene Dube, the editor and publisher of the privately owned news website *Swati Newsweek*, seizing three mobile phones, a laptop, and work documents. Dube was taken into custody and interrogated for about seven hours about two articles critical of the King. He was then brought before a magistrate to record a statement. before being released without charge. The police retained his devices and documents on the grounds that they were required for further investigation. According to Dube, police told him that the King was immune from criticism and warned him that he could face charges of **high treason**. Police then went to the home of journalist Mfomfo Nkhambule, who wrote one of the two articles published by Dube. Nkhambule was also taken to a police station and interrogated about the articles, where he was also threatened with charges of **treason**. Nkhambule said that he had also been interrogated by police in

[601] "More delays as Eswatini MPs languish in jail", Southern Africa Litigation Centre, 22 September 2021.
[602] "Swazi editor flees to South Africa, wanted in false news investigation", Committee to Protect Journalists, 15 May 2020. Dlamini had previously received death threats from a local businessman, in 2017, in connection with an article about the King's involvement in a corruption case. He fled to South Africa at that stage, and his newspaper, ,*Swaziland Shopping,* was shut down by the government. He returned to Swaziland in 2018 after the businessman who had threatened him passed away. "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Safety.
[603] "eSwatini editor receives death threats over pro-government article", Committee to Protect Journalists, 13 July 2020. The opposition party in question denied that the person who sent the threats was their member.

connection with articles about the King written the previous year for another online publication, *Swaziland News*. On that occasion, a police officer allegedly threatened to throw him out of a second floor window, explaining that they would cover it up by claiming that he had tried to escape.[604] A report in the weekly publication *Independent News quoted* police commissioner William Tsintsibala Dlamini as saying that authorities would come down hard on journalists who wrote negatively about King Mswati III and that the law would take its course. Government spokesperson Sabelo Dlamini said that Dube was under investigation for operating an unregistered media outlet, not for criticizing the King.[605]

In addition to government arrests and intimidation, it was reported in 2020 that there is an increasing trend of **civil defamation cases against the media** particularly by rich and powerful individuals, couples with concerns that courts do not always apply the principle of "fair comment" about matters of public interest as a defence against defamation claims. Bheki Makhubu, editor of *The Nation* magazine, was quoted as saying that the judiciary and prominent figures are turning the media into an "industry of compensation", as huge awards encourage people to become litigious. He worries that the judiciary "has moved beyond being an arbiter of justice and taken on a seeming censor's role. Fearful journalists then self-censor, shying away from reporting any story that might get them into trouble with the law. The media is now expected to do the bidding of the powerful people and government." [606] Some civil society groups have maintained that the hefty awards in defamation actions mean that "the justice delivery system is being used to create a climate of fear in the media that undermines reportage of issues of public interest and national development".[607] The managing editor of *Times of eSwatini,* Martin Dlamini, was quoted as stating said that hefty damages in civil defamation claims are sending a strong message to the media that they should not write stories critical of powerful people, noting that there are other avenues that aggrieved people can use to get redress from media houses, such as the Media Complaints Commission with an Ombud as well as some in-house ombuds at individual media outlets, but the courts do not encourage complainants to use them." [608]

The eSwatini Communications Commission **shut down Internet access** throughout the country on 29 June 2021 as protests against King Mswati III spread nationwide. This shutdown also prevented two print newspapers, the state-owned *eSwatini Observer* and the privately owned *Times of eSwatini*, from being able to publish on two consecutive days. General website traffic resumed on July 4, but social media platforms remained blocked until 8 July.[609] A MISA representative stated: "Without the access to internet the Eswatini government is able to control the narrative. Lack of

[604] "Swaziland journalists harassed, threatened with treason charges over reporting on king", Committee to Protect Journalists, 30 April 2020. Police apparently searched for Mthobisi Ntjangase, the reporter who wrote the other article, but could not find him.
[605] "Id. The *Independent News report referred to appears to be no longer available online.*
[606] Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020.
[607] Joint submission by the Women and Law in Southern Africa Research and Educational Trust Eswatini (WLSA) and the Advancing Rights in Southern Africa (ARISA) Program on Eswatini to the 39th Session of the Working Group on the Universal Periodic Review (undated), page 10.
[608] Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020,
[609] "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.

internet access is making it difficult for the journalists to report about the crackdown to the international audience and put pressure on the government. Eswatini media and citizens are now isolated and left on their own without access to information. As long as the internet is shut down, Eswatini is a dark spot, and nobody knows exactly what's going on there and what the real scale of the violence towards citizens and journalists is." [610] A second internet blackout was imposed for a brief period in October 2021.[611]

7.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) THE COMPUTER CRIME AND CYBER CRIME ACT, 2022

The Computer Crime and Cyber Crime Act, 2022 came into force on 4 March 2022.[612] The Association for Progressive Communications provides this overview:

> *The Computer Crime and Cyber Crime Act, 2022 criminalises offences committed against and through the use of computer systems and electronic communications networks. Whilst mechanisms to protect citizens against criminal and terrorist elements that emanate from the use of the internet are necessary, there is a danger and risk that this can be misused by governments to curtail freedom of expression on the internet, which has implications such as the shrinking of online civil society spaces. Among the concerns expressed is that the law has the potential to be interpreted in a way that targets vocal human rights defenders, media practitioners and activists. The regulations of the law are yet to be developed.*[613]

In early discussions around the Bill, the government proposed to include heavy fines and jail sentences for "Facebook abusers" and persons who posted "fake news" on the Internet.[614] This inspired a flurry of criticism.[615] No such provisions were included in the final law.

The Act is administered by the **Eswatini Communications Commission** established under the Eswatini Communications Commission Act, 2013, which has the power "to regulate and coordinate matters of cybersecurity and enforce standards applicable to the security of the critical information infrastructures".[616] The Act also authorizes the

[610] Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
[611] "Freedom in the World 2022: Eswatini", Freedom House, section D1.
[612] Computer Crime & Cybercrime Act 6 of 2022, section 1.
[613] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
[614] The Bill originally included a prohibition on the publication of "any statement or fake news through any medium, including social media with the intention to deceive any other person or group of persons" (section 19). "LEXOTA Country Analysis: Eswatini", last updated July 2022.
[615] Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022; "Fears that cybercrime bill will hit eSwatini's media freedom", The Economist Intelligence Unit, 14 September 2020.
[616] Computer Crime & Cybercrime Act 6 of 2022, section 2 (definition of "Commission") and section 52.

Prime Minister to establish a **National Cybersecurity Advisory Council** with a maximum of 15 members from a cross section of stakeholders, including the ICT, legal, finance, education, business, civil society, defence, police, international cooperation and national security sectors.[617]

The Act creates the technical offences listed in the table below. Most of these offences are actionable only if committed "intentionally, without lawful excuse or justification", which helps to narrow them and avoid capturing good faith conduct in the public interest – such as testing a computer system's vulnerabilities.

THE COMPUTER CRIME AND CYBER CRIME ACT - TECHNICAL OFFENCES	
Section 3: Illegal access	It is an offence to intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, access the whole or any part of a computer system. There is an enhanced penalty where such access infringes security measures with the intention of obtaining computer data. o "Access" for purposes of this section means "logging into a computer system" (section 2). o It has been asserted that this crime carries an excessive maximum penalty – a E500 000 fine or imprisonment for five years (as the enhanced penalty) – which is out of line with that imposed for similar offences in other SADC countries. [618]
Section 4: Illegally remaining logged onto a computer	It is an offence to intentionally, without lawful excuse or justification, infringe security measures or with the intention of obtaining computer data or with other dishonest intent, remain logged in a computer system or part of a computer system or continues to use a computer system. o The requirement of having "the intention of obtaining computer data" or "other dishonest intent" helps to prevent this offence from being overbroad. o It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorized access.[619]
Section 5: Illegal interception	It is an offence "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification", to intercept, by electronic means any non-public transmission to, from or within a computer system or any electromagnetic emissions from a computer system.
Section 6: Illegal data interference	All of the actions described in this section are offences only if done "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification". It is an offence to do any of the following:

[617] Id, section 53.
[618] "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022. This article cites the Botswana Cybercrime and Computer Related Crimes Act 18 of 2018 as a point of comparison, where a similar offence attracts a maximum fine of P20 000 (equivalent to E27 200) or imprisonment for a maximum of one year, or both. In Botswana, the related offence of unauthorised access to a computer service *with the intent to intercept data* attracts a doubled maximum penalty – which is still significantly less than the eSwatini penalty.
[619] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	• damage or deteriorate computer data; • delete computer data; • alter computer data; • render computer data meaningless, useless or ineffective; • obstruct, interrupt or interfere with the lawful use of computer data; • obstruct, interrupt or interfere with any person in the lawful use of computer data; or • deny access to computer data to any person authorized to access it. It is also an offence to commit any of the acts described in this section in order to deny access, including a partial denial of service, to any person authorized to such access or service. It is an offence - • to communicate, disclose or transmit any computer data, program, access code or command to any person not authorized to access it; • to access or destroy any computer data for purposes of concealing information necessary for an investigation into an offence; or • to receive computer data that the person in question is not authorized to receive. It is an offence to destroy or alter computer data that is required by law to be kept or maintained, or data that is evidence in relation to any proceeding under the Act by – • creating, destroying, mutilating, removing or modifying data or a program or any other form of information within or outside a computer or computer network; • activating, installing or downloading a program that is designed to create, destroy, mutilate, remove or modify data, a program or any other form of information within or outside a computer or computer network; or • creating, altering, or destroying a password, personal identification number, code or method used to access a computer or computer network, There is an enhanced penalty for data in "a critical database", and data concerned with "national security" or "the provision of an essential service". For purposes of these offences, it is immaterial whether an illegal interference or its intended effect is permanent or temporary. o The most concerning part of the list of offence is to receive computer data without authorization (subsection (3)(c)), which could affect data acquired by a whistleblower or placed in a cache such as Wikileaks. It is not clear if the exception of "justification" would apply to exposing such information in the public interest – and doubts about the application of this exception could result in self-censorship. o Regarding the enhanced penalties, "critical database" is not defined, but "critical infrastructure" is broadly defined in section 2 as "computer systems, devices, networks, computer programs, computer data, vital to the country [such] that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on, national or economic security, national public health and safety, national

	elections or any combination of those matters; or physical infrastructure, assets or systems declared as such by Government". There is no definition of "national security or "essential service". o Best practice avoids potential risks arising from an overly broad definition of "critical infrastructure".[620] o The Southern Africa Litigation Centre has asserted that subsection (6) (enhanced penalties in respect of data in a critical database, or data concerned with national security or the provision of an essential service, and subsection (7) (making it immaterial whether the interference or its effect is temporary or permanent) are "so overly broad that they cannot possibly pass constitutional muster".[621]
Section 7: Data espionage	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to obtain for oneself or another person computer data which is not meant for that person and which is "specially protected against unauthorized access". o Without knowing that would be covered by "justification", it is possible that this offence could inhibit some instances of investigative journalism. o This formulation of the offence raises the question of how a person would know if data is "specially protected", as opposed to merely "protected". o Without more specificity, "unauthorized access" could be interpreted broadly to include data which is not legally protected, but has only been arbitrarily declared to be prohibited from access by a government official. [622] o It has been asserted that "data espionage" offences are unnecessary because they are covered by the general offence of unauthorized access.[623]
Section 8: Illegal system interference	All of the actions described in this section are offences only if done "intentionally without lawful excuse or justification, or in excess of a lawful excuse or justification". It is an offence to hinder or interfere with the functioning of a computer system or with a person who is lawfully using or operating a computer system. It is an offence to seize or destroy any computer storage medium. It is an offence to hinder or interfere with a computer system that is exclusively for the use of critical infrastructure operations, or one that is used in critical infrastructure operations, where that conduct affects that use or impacts the operations of the critical infrastructure. This offence attracts a harsher penalty than the other offences in the section: a fine of up to one million Emalangeni or imprisonment for up to ten years, or both. o "Critical infrastructure" is broadly defined in section 2 as "computer systems, devices, networks, computer programs, computer data, vital to the country [such] that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on, national or economic security, national public health and safety, national

620 *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 15.
621 "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
622 Id.
623 *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	elections or any combination of those matters; or physical infrastructure, assets or systems declared as such by Government". o "Hinder" in relation to a computer system includes but is not limited to – o cutting the electricity supply to a computer system; o causing electromagnetic interference to a computer system; o corrupting a computer system by any means; and o inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (section 2). o The offence of seizing or destroying any computer storage medium is " overly broad and can easily lead to abuse".[624] Note that this offence is punishable by a maximum penalty of E500 000 or 4 years' imprisonment.
Section 9: Illegal devices	It is an offence "intentionally without lawful excuse or justification or in excess of a lawful excuse or justification" to produce, sell, introduce, spread, procure for use, use, import, export, distribute or otherwise make available any of the following: • a device, including a computer program, that is designed or adapted for the purpose of committing an offence under Part II of the Act • a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed • a software code that damages a computer or computer system. It is an offence even to possess any of the described items, with the exception of the software code. However, this offence requires the intent that the item in question is to be used by any person for committing an offence described in Part II of the Act. o Section 2 includes a wide and yet non-exhaustive definition of "device". o The aspect of this section on *using* an illegal device essentially makes the means of committing the underlying offence into an additional offence – thus imposing double criminalization on a single act.[625]
Section 10: Computer related forgery and uttering	It is an offence "intentionally without lawful excuse or justification or in excess of a lawful excuse or justification" to input, alter, delete, or suppress computer data, resulting in inauthentic data, with the intention that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. There is an enhanced penalty if this offence is committed by sending out multiple electronic mail messages from or through a computer system. o Section 2 defines "multiple electronic mail messages" as a mail message including e-mail and instant messaging sent to more than one recipient. The Southern Africa Litigation Centre suggested that this definition should require a message sent to more than 1000 recipients, to avoid overbreadth.[626]

[624] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[625] Id. SALC believes that this offence was incorrectly transcribed from the SADC Model Law.
[626] Id.

Section 11: Computer related fraud	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to cause loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system, with a fraudulent or dishonest intention of procuring, without permission, an economic benefit for oneself or someone else. o The required intent helps to ensure that this offence is properly targeted.
Section 12: Phishing	It is an offence "without a lawful excuse or justification" to use email, spoofed email, a website, social media or a text message to lure, deceive or threaten another person to give money or other value, or to reveal sensitive information, account login details, bank account or credit card information "or the like". o With regard to a "spoofed email", "spoofing" means "hiding the actual source address or identity behind another identity to appear as if the email or information is from the legitimate address (section 2). o The catch-all phrase "or the like" is arguably insufficiently clear to define a criminal offence.
Section 13: Cyber terrorism	It is an offence "intentionally without legal justification or legal excuse" to use a computer system - • to launch an attack on telecommunications or computer networks "through conventional methods"; • to launch attacks using physical devices, computer programs or other electronic means to - o render the financial or banking system of the country or city unusable; o compromise the defence system of the country; o seriously disrupt or interfere with the operations of the electricity grid, aviation control system, tax management systems, population register, government payroll and cabinet system; • to fund or raise funds with the purpose of financing or carrying out the listed acts. This offence carries a maximum penalty of a five hundred thousand Emalangeni fine or ten years' imprisonment or both. o The phrase used in other sections is "without lawful excuse or justification"; here it is "without legal justification or legal excuse". It is unknown if a different meaning was intended here. o Earlier versions of the bill had a much broader definition of this crime, but were evidently revised.[627] o It seems odd that a fine is a potential penalty for such a serious offence. o The Southern Africa Litigation Centre submits that cyberterrorism is already sufficiently covered by eSwatini's Suppression of Terrorism Act, as amended in 2017 and interpreted by the High Court. [628]
Section 16: Identity	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to make use of a computer system to utilize someone else's identity for any unlawful activity.

[627] Id.
[628] Id.

related crimes	
Section 18: Extortion	This offence extends the crime of extortion to situations where the act of extortion takes place through the internet, email or any computer system platform – on other words, to situations where a computer is the tool. o Section 2 defines "extortion" as "an act of demanding favour or benefit from a person through coercion, or arising from an advantage one holds over the victim, by threatening to inflict harm to his person, family members, reputation or property by unleashing the advantage he holds over the victim".
Section 19: Website defacement	It is an offence "intentionally or without lawful excuse" to commit or participate in the website defacement of another entity's website. o "Website defacement" is defined in section 2 "as the act of attacking a website by changing the visual appearance, adding, changing, deleting or replacing content by a party or parties not authorized by the website owner". o This offence uses the phrase "intentionally *or* without lawful excuse" as opposed to the phrase "intentionally *and* without lawful excuse or justification: that appears in most of the other provisions in the Act. It is unclear what distinction was intended.
Section 24: Spam or Spamming	It is an offence "intentionally and without lawful excuse or justification" - • to initiate the transmission of spam messages from or through a computer system; • to use a hidden or disguised computer system to relay or retransmit multiple electronic mail messages, with the intention to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or • to materially falsify header information in multiple electronic mail messages and intentionally initiate the transmission of such messages. There are exceptions for transmission of multiple electronic mail messages within a customer or business relationship, where the recipient has not opted out of the relationship. o Section 2 defines "spamming" or "spam" as "the use of messaging systems to send unsolicited mail messages, text messages or adverts, usually for marketing or promotional purposes to customers, former or potential customers or other recipients". o Section 2 defines "multiple electronic mail messages" as messages including e-mail and instant messaging sent to more than one recipient.
Section 25: Denial of service and botnets	It is an offence to take "illegal control" of a computer system in a network, or an entire network of computer systems or network components, partially or fully and "remotely or otherwise". It is an offence "intentionally, without justification" to cause or launch an attack with data traffic on a computer system or network so as to overwhelm the network resources, resulting in slowed or denied service.
Section 49: General	Any offence under any Act which is committed in whole or in part through the use of a computer, electronic device or in electronic form is deemed to

provision on cybercrimes	have been committed under that Act and the provisions of that Act shall apply with the necessary modification. o This provision appears to be aimed at ensuring that any crime committed with computer tools can be prosecuted under the relevant law for that crime.

The Act creates ten content-related offences, covering a broad array of topics.

THE COMPUTER CRIME AND CYBER CRIME ACT – CONTENT-BASED OFFENCES	
Section 14: Child pornography	There is an extensive set of offences relating to "child pornography". The production of child pornography is an offence regardless of the medium used, but the other acts relating to children pornography are offences only if they involve a computer system or information and communication technologies. It is a defence in most cases if the conduct in question was for "a genuine artistic, educational, legal, medical, scientific or public benefit purpose, including Eswatini cultural events". It is also an offence to expose children to pornography, to engage in cybersex with a child or someone who lacks capacity to give legal consent to sex, or to subject such a person to sexual grooming. o "Child pornography" is defined in section 2 to mean "any material that depicts, presents or represents a child engaged in sexual conduct, or in the nude without a justifiable cause, or images representing a child engaged in sexual conduct", It includes, but is not limited to, audio, visual or textual material. o "Cybersex" means "sexual activity or fantasy which may lead to sexual arousal or pleasure gained through communication, for that purpose, by computer system with another person" (section 2). This definition seems somewhat unclear. o "Sexual grooming" means intentionally befriending or establishing an emotional connection with a child or an adult who is legally not able to consent to sex, to train them to agree to participate in acts of sexual abuse or exploitation or to , or lower their inhibitions in respect of such acts (section 2). The Southern Africa Litigation Centre finds this definition problematically cursory.[629] o It has been noted that the cybercrime version of this offence does not align well with the overlapping provision on pornography in eSwatini's Sexual Offences and Domestic Violence Act, 2018., which could lead to difficulties in implementation.[630]
Section 15: Prohibition of distribution or publication of pornography	It is an offence - • to distribute, publish, advertise or expose material, which is pornographic *to a child, or to non-consenting adults*; • to publish or exhibit any pornographic material without printing in such his or her name and the prescribed particulars of his or her address or without indicating the age restriction or consumer advice; or

[629] Id.
[630] "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022.

	• to broadcast a pornographic film whether publicly or privately *to children or non-consenting adults.* There is a separate reference to commission of this offence by someone with parental power or control over the child in question, but the penalty prescribed is the same in this instance as in any other. o Note this offence is actually much narrower than its title suggests. o The definition of pornography is reasonably specific. "Pornography" means a visual, text or audio presentation, simulated or real of – o a person who is, or is depicted as, participating in or assisting another person to engage in a sexual act or sexual violations, or a lewd display of nudity which is intended for sexual gratification; o explicit sexual conduct which degrades a person, or which constitutes incitement to cause harm; or o a sexual act between a person and an animal (section 2). o This offence replicates a provision of the Sexual Offences and Domestic Violence Act, with the exception of the penalties imposed, which is likely to lead to confusion.[631]
Section 17: Cyberbullying and cyberstalking	It is an offence to engage in cyberbullying or cyberstalking, or to aid or abet another person in these acts. o "Cyberbullying" is defined in section 2 as "the use of electronic communication to bully a person typically by sending messages of an intimidating or threatening nature". This definition is unclear, particularly with regard to what might be considered "intimidating". o "Cyberstalking" is defined in section 2 as "the use of the Internet or other electronic means to inflict repeated unwarranted actions on a natural or juristic person(s). Such actions may include false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass; which may result in mental or corporate abuse." o The cybercrime law does not provide for restraining orders in cases where the cyberbullying or cyberstalking do not warrant imprisonment. The offence of cyberstalking is already provided for under the Sexual Offences and Domestic Violence Act, which defines unlawful stalking to include stalking by electronic means and is not limited to acts of a sexual nature; the Sexual Offences and Domestic Violence Act provides a remedy of a restraining order.[632]
Section 20: Racist, hate speech or xenophobic material	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" - • to produce racist, hate speech or xenophobic material with the intention of distributing it through a computer system; • to offer or make available racist, hate speech or xenophobic material through a computer system; or • to distribute or transmit racist, hate speech or xenophobic material through a computer system.

631 "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
632 Id.

	○ Section 2 defines "racist, xenophobic and hate speech [material]" as "any material, including but not limited to any image, video, audio recording or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals; which may be based on race, colour, descent, national or ethnic origin, religion, creed or social or economic standing, political opinion or disability". ○ This definition goes beyond the Malabo Convention requirements by including "creed or social or economic standing, political opinion or disability". The Southern Africa Litigation Centre suggested that it could also have included sex, gender, sexual orientation, and gender identity.[633]
Section 21: Racist, hate speech and xenophobic motivated insult	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification", through a computer system to "publicly" use language that "harms the reputation or feelings" of a person or a group of persons on the basis of race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors. ○ Although this is based on the Malabo Convention, criminalising "insult" - described here more widely than in the Convention as being harm to a person's reputation or feelings – seems extremely overbroad, even if based on one of the prohibited grounds. ○ The Southern Africa Litigation Centre suggested that this provision could also have included sex, gender, sexual orientation, and gender identity.[634] ○ One local journalism lecturer worries that this provision could result in "political opinion being classified as hate speech if one makes comments against certain political elements".[635]
Section 22: Genocide and crimes against humanity	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to distribute or otherwise make available through a computer system to the public or to another person "material that - • denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity. • aids, induces or incites others to commit such acts, or • incites, instigates, commands, or procures any other person to commit such acts. ○ There is no definition of "genocide" or "crimes against humanity". ○ The Malabo Convention makes it an offence only to deny, approve or justify acts constituting genocide or crimes against humanity. This offence, in contrast, criminalises these acts as well as the encouragement of others to commit future genocide or crimes against humanity. ○ Note that this offence would capture even a private message from one individual to another denying or minimising genocide or crimes against humanity if sent through a computer system. Communication with even

[633] Id.
[634] Id.
[635] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.

	a single individual *inciting* genocide or crimes against humanity is clearly justifiable, but merely expressing an opinion about historical events in a private communication raises harder questions about privacy and freedom of expression. The Malabo Convention does not specify whether or not the communication must be public; it merely calls on States to make it a criminal offence to "deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system".
Section 23: Trafficking in humans, endangered species or illegal merchandise	It is an offence "without justification or lawful excuse" to use electronic or online methods to participate in the trafficking of humans, endangered animals, protected plants or any goods that he is not authorized to traffic in. o "Trafficking" is defined in section 2 as "initiating, carrying out, or being party to, actively or passively, an act of moving or facilitating the illegal movement or illegal transportation of people, animals, plants, money or goods within a country or across international borders for trade purposes to fulfil personal goals through the use of a computer system". o This offence uses the phrase "intentionally *or* without lawful excuse" as opposed to the phrase "intentionally *and* without lawful excuse or justification" that appears in most of the other provisions in the Act. It is unclear what distinction was intended.
Section 28: Harassment utilising means of electronic communication	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to "initiate any electronic communication, with the intention to coerce, intimidate, insult, harass, or cause emotional distress to a person, using a computer system, to support hostile behaviour". o The drafting of this offence is somewhat confusing as it is not clear how the reference to supporting hostile behaviour fits in, even though this wording is similar to that used in the SADC Model Law on harassment.[636] o The Southern Africa Litigation Centre notes: "The offence of harassment is much broader than what is proposed in the SADC Model law. The Model law does not include "insult" under this offence and limits the offence to instances which are "severe, repeated *and* hostile", not simply "hostile". We submit that the approach of the SADC Model law is much clearer and preferred. We are concerned that the offence could be used to persecute human rights defenders."[637] o Insulting, harassing and causing emotional distress are all vague and subjective behaviours. None of these terms are defined, or applied with reference to an objective reasonable person. "Hostile behaviour" is similarly undefined. For example, legitimate criticism of improper behaviour by a government official might be seen as "hostile" and being insulting or causing emotional distress. This offence seems too broad and vague to constitute a justifiable restriction on freedom of

[636] *SADC Model Law on Computer Crime and Cyber Crime, 2012*, section 22: "A person, who initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, *using a computer system to support severe, repeated, and hostile behaviour*, commits an offence…".
[637] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.

	expression.
Section 29: Violation of intellectual property rights.	It is an offence to use any computer or electronic device to violate any intellectual property rights protected under any law or treaty applicable to intellectual property rights in the Kingdom of Eswatini.

In general, **attempting, abetting or conspiring to commit any offence under the Act** – whether technical or content based – is also an offence.[638] This general prohibition overlaps with the references to aiding and abetting in some of the individual provisions.

Some assert that the **fines and prison sentences** imposed by the law are excessive, and higher than those in similar legislation in other SADC countries.[639] The Southern Africa Litigation Centre also finds the penalties "incredibly high" and worries that they might result in arbitrary and disproportionate sentences in specific cases. It also submits that the reasons for the differences in penalties for different offences are often unclear.[640]
Commenting on the issue of excessive fines and prison sentences, Ndimphiwe Shabangu, advocacy and communications officer at the Coordinating Assembly of NGOs (CANGO) in eSwatini, indicated that these penalties were even higher in initial drafts of the law, but through intervention from civil society and other stakeholders these fines and sentences were reduced, even though they were still considered excessive as contained in the law.[641]

The Act has also been criticised for **failing to cover the non-consensual sharing of intimate images**.[642]

Turning to procedural aspects of the law, **searches and seizures** require a warrant from a magistrate's court or the High Court based on an affidavit from a law enforcement agent that there are reasonable grounds to suspect that there may be a thing or computer data in a certain place that is either material evidence in proving an offence, or that has been acquired by a person as a result of an offence.[643] A "law enforcement agent" includes personnel from Royal Eswatini Police, the Anti-Corruption Commission, the Eswatini Revenue Authority and the Eswatini Communications Commission. [644] Where a Court has issued a warrant, a person who is not a suspect, but who has knowledge about the functioning of the computer

[638] Computer Crime & Cybercrime Act 6 of 2022, section 30. Section 2 defines "abetting" as "to encourage or assist someone to commit a crime or other offence".
[639] "Computer, Cybercrime Act: a necessary evil", *Times of Eswatini*, 31 October 2022.
[640] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020. It cites these examples: "Using an illegal device to commit an offence can lead to a fine of E100m or 25 years' imprisonment or both (section 9), even though the offence being committed might be quite benign. In contrast, committing computer related forgery or computer related fraud can result in a lesser sentence of E10m or 10 years' imprisonment or both (section 10 and 11 respectively), but using a botnet to disrupt a service can attach E100m or 20 years' imprisonment." The SALC also noted that there is a lack of congruence between the fine and the number of years in imprisonment in respect of the various offences in the bill, but the examples it cites do not match the final law indicating that this issue was addressed.
[641] Ndimphiwe Shabangu was interviewed via Zoom on 19 July 2023.
[642] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[643] Computer Crime & Cybercrime Act 6 of 2022, section 33. There is a wide and non-exhaustive definition of "thing" in section 2.
[644] Id, section 2 (definition of "law enforcement agent").

system or measures applied to protect the computer data in the computer system, has a duty to assist law enforcement agents.[645]

A Court can also authorise the **general collection of traffic data by law enforcement agents** for the purposes of a specific criminal investigation; this must apply to a specified communication during a specified period, but the length of the period that can be covered by the authority is not specified .[646] It can also authorise the **interception of content data**, again only in respect of specified communications for a specific criminal investigation. There is no time limit on such an authorisation. [647]

Furthermore, a Court may issue authority for the **use of a remote forensic tool for monitoring purposes**, including the installation of a forensic tool on the suspect's computer system. However, this power is limited to criminal investigations relating to a list of serious offences. Such an authority is limited to 3 months, but can be renewed.[648]

A Court also has the power to issue **production orders** to service providers or other persons in control of computer systems.[649]

However, **expedited preservation notices** in respect of traffic data and notices directing the **partial disclosure of traffic data**, to identify the service provider or the path through which a communication was transmitted, can be issued by a law enforcement agent, without court involvement.[650] A preservation notice issued in this way can require that the data specified in the notice be preserved for a period of up to 28 days – which far exceeds the SADC Model Law's recommendation that data can be preserved for 7 days subject to such a notice, and on court order for a further 7 days at a maximum.[651]

Given the complexity of the procedural matters, the Southern Africa Litigation Centre recommended that they should be handled only by the High Court,[652] but this recommendation was not taken up. They also expressed concern about the avenues for evidence collection issued by law enforcement agents without court involvement, on the basis that this departs from acceptable criminal procedure.[653]

The Act contains a provision allowing a court to order **forfeiture of assets** for persons convicted of any offence under the Act. This can apply to any asset, money or property constituting or traceable to the proceeds of the offence, as well as any

[645] Id, section 34.
[646] Id section 38. Section 2 defines "traffic data" as "computer data that relates to a communication by means of a computer system and generated by a computer system that is part of the chain of electronic communication; and may show one or more of the following, the communication's origin, destination, route, time, date, size, duration or the type of underlying services".
[647] Id, section 39.
[648] Id, section 40. Section 2 defines a "remote forensic tool" as "an investigative tool including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address".
[649] Id, section 35.
[650] Id, sections 36-37.
[651] *SADC Computer Crime and Cybercrime Model Law, 2012*, section 28; "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[652] "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
[653] Id.

computer, equipment, software or other technology used or intended to be used to commit or facilitate the offence. The Act also requires in every case that persons convicted of an offence under the Act must forfeit their passport or international travelling document to the State until they have paid any fines or served any sentence imposed. A court may release a person's travel document upon application if travel is required for medical treatment or in the interest of the public.[654]

B) OTHER LAWS THAT MAY INHIBIT FREEDOM OF EXPRESSION

Concerns about legislation that restricts freedom of expression was a strong theme in eSwatini's most recent Universal Period Review, with the following laws in particular being cited: the **Suppression of Sedition and Subversive Activities Act, 1938**; the **Suppression of Terrorism Act, 2008 as amended in 2017**; and the **Public Order Act, 2017**.[655] For example, the US Government recommended that the government should repeal the Sedition and Subversive Activities Act, 1938 "which has been used to silence journalists, human rights defenders, and political activists".[656] According to the Southern Africa Litigation Centre, the Suppression of Terrorism Act, 2008 and the Sedition and Subversive Activities Act, 1938 "have frequently been used to suppress any speech that is critical of the Government and the Monarch".[657]

The **Sedition and Subversive Activities Act 46 of 1938** contains several provisions affecting freedom of expression. As discussed above, some of these have been struck down on constitutional grounds (sections 3(1), 4(a) and (e), and 5), but the State is making a belated appeal of this holding. The full text of this Act could not be located online, but the key provisions of concern are reproduced in the box below, as quoted in the court judgment.[658] Note the breadth of "seditious intentions", and the narrow margin between what is seditions and what falls into the exceptions in the quoted provisions – which is bound to lead to self-censorship. Note also the deeming provision in section 3(3) which (in the words of the High Court) is "plainly contrary to the constitutionally entrenched right of being presumed innocent until proven otherwise".[659]

SEDITION AND SUBVERSIVE ACTIVITIES ACT 46 OF 1938

KEY PROVISIONS ON EXPRESSION

The provisions indicated in boldface type have been struck down on constitutional grounds, with this decision currently on appeal by the State.

[654] Computer Crime & Cybercrime Act 6 of 2022, section 48.
[655] "Report of the Working Group on the Universal Periodic Review: Eswatini", A/HRC/49/14, 7 January 2022.
[656] "U.S. Statement at the Universal Periodic Review of eSwatini", U.S. Mission Geneva, 8 November 2021.
[657] "Statement: Concern as states continue to use terrorism laws to inhibit freedom of expression and access to information", Southern Africa Litigation Centre, 27 September 2021.
[658] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 18.
[659] Id, paragraph 21.

3.

(1) A "seditious intention" is an intention to -

(a) bring into hatred or contempt or to excite disaffection against the person of His Majesty the King, His Heirs or successors, or the Government of Swaziland as by law established; or

(b) excite His Majesty's subjects or inhabitants of Swaziland to attempt to procure the alteration, otherwise than by lawful means, of any matter in Swaziland as by law established; or

(c) bring into hatred or contempt or to excite disaffection against the administration of justice in Swaziland; or

(d) raise discontent or disaffection amongst His Majesty's subjects or the inhabitants of Swaziland; or

(e) promote feelings or ill-will and hostility between classes of the population of Swaziland.

(2) Notwithstanding subsection (1), an act, speech or publication shall not be seditious by reason only that it intends to -

(a) show that His Majesty has been misled or mistaken in any of His measures; or

(b) point out errors or defects in the government or constitution of Swaziland as by law established or in legislation or in the administration of justice with a view to the remedying of such errors or defects; or

(c) persuade His Majesty's subjects or the inhabitants of Swaziland to attempt to procure by lawful means the alteration of any matter in Swaziland as by law established; or

(d) point out, with a view to their removal, any matters which are producing or have a tendency to produce feelings of ill-will and enmity between different classes of the population of Swaziland.

(3) In determining whether the intention with which any act was done, any words were spoken, or any document was published, was or was not seditious, every person shall be deemed to intend the consequences which would naturally follow from his conduct at the time and under the circumstances in which he so conducted himself.

4. Any person who -

(a) does or attempts to do, or makes any preparation to do, or conspires with any person to do, any act with a seditious intention;

(b) utters any seditious words;

(c) prints, publishes, sells, offers for sale, distributes or reproduces any seditious publication; or,

(d) imports any seditious publication, unless he has no reason to believe that it is seditious;

(e) without lawful excuse has in his possession any seditious publication;

shall be guilty of an offence and liable on conviction to imprisonment not exceeding 15 years or a fine not exceeding E20, 000 and any seditious publication relating to an offence under this section shall be forfeited to the Government.

5.

(1) A person who does or attempts to do or makes any preparation to do an act with a subversive intention or who utters any words with a subversive intention shall be guilty of an offence and liable, on conviction, to imprisonment for a term not exceeding twenty years without the option of a fine.

(2) For the purposes of this section, "subversive" means -

(a) supporting, propagating or advocating any act or thing prejudicial to -

(i) public order;

(ii) the security of Swaziland; or

(iii) the administration of justice:

Provided that this paragraph shall not extend to any act or thing done in good faith with intent only to point out errors or defects in the government or constitution of Swaziland as by law established or in legislation or in the administration of justice with a view to remedying such errors or defects;

(b) inciting to violence or other disorder or crime, or counselling defiance of or disobedience to any law or lawful authority;

(c) intended or likely to support or assist or benefit, in or in relation to such act or intended acts as are hereinafter describe, persons who act, intend or act or have acted in a manner prejudicial to public order, the security of Swaziland or the administration of justice, or who incite, intend to incite, or have invited to violence or other disorder or crime, or who counsel, intend to counsel or have counselled defiance of or disobedience to any law or lawful authority;

(d) indicating, expressly or by implication, any connection, associated or affiliation with or support for an unlawful society;

(e) intended or likely to promote feelings or hatred or enmity between different races or communities in Swaziland: Provided that this paragraph shall not extend to comments or criticisms made In good faith and with a view to the removal of any causes of hatred or enmity between races or communities;

(f) intended or likely to bring into hatred or contempt or to excite disaffection against any public officer or any class of public officers in the execution of his or their duties, or any of His Majesty's armed forces, or any officer or other member of such a force in the execution of his duties: Provided that this paragraph shall not extend to comments or criticisms made in good faith and with a view to remedying or correcting errors, defects or misconduct on the part of such public officer, force or office or other member thereof and without attempting to bring into hatred or contempt or to excite disaffection against such a person or force;

(g) intended or likely to seduce from his allegiance or duty any public officer or any officer or other member of any of His Majesty's armed forces.

The **Suppression of Terrorism Act 3 of 2008, as amended in 2017,** has several problematic provisions, including these:

- Section 5(3)(e) makes it an offence to intentionally publish or communicate in any manner false information about the existence of any danger, dangerous thing, explosive or harmful or hazardous substance when that person does not believe in the existence of that thing or the truthfulness of that publication or communication.[660] This could, for instance, inhibit reports of threats that are doubtful but nonetheless newsworthy.

- Section 11(1)(a)-(b) makes it an offence to knowingly, and in any manner solicit support for, or give support to, any terrorist group or the commission of a terrorist act.[661] This provision was used to charge members of the Peoples United Democratic Movement (PUDEMO) because they were found wearing T-shirts and berets identifying this organization and chanting its slogans and demands.[662]

As discussed above, these provisions along with some other related ones have been struck down on constitutional grounds, but the State is making a belated appeal of this holding. Amnesty International and the Human Rights Institute of the International Bar Association called for the repeal of this law shortly after its enactment, on the grounds that it was inherently repressive, violated human rights standards, and was leading to violations of the rights of freedom of expression, association and assembly.[663]

Section 3 of the **Official Secrets Act 30 of 1968**, which could not be located online, makes it an offence, amongst other things, to publish any information that is likely to be even indirectly useful to an enemy. Section 4(2) makes it an offence to publish or communicate any information that relates to munitions of war or any other military or police matter in any manner or for a purpose prejudicial to the safety or interests of eSwatini. Section 9(b) essentially creates a presumption of guilt, by providing where a person is charged with publishing or communicating information for a purpose prejudicial to the safety or interests of eSwatini, without lawful authority, it is presumed that the purpose was prejudicial to the safety or interests of eSwatini.[664] This law has been cited as an impediment to whistleblowers and investigative journalists.[665]

---

[660] Suppression of Terrorism Act 3 of 2008, as amended by the Suppression of Terrorism (Amendment) Act 11 of 2017, section 5(3)(e).
[661] Id, section 11(1)(a)-(b).
[662] *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 28.
[663] "Suppression of Terrorism Act undermines Human Rights in Swaziland", Amnesty International and International Bar Association, 2009. Amnesty International made the following comments after the 2017 amendment:

> Although Eswatini amended the 2008 Suppression of Terrorism Act in 2017, the Act continues to be used to silence and punish dissent. The Act's amendments limit the definitions of what constitutes a terrorist act although the wording is overly broad and vague in relation to terrorism related acts. The law also contained provisions that undermined the rights to freedom of expression, association and peaceful assembly. The STA (Amendment) Act 2017 remains inconsistent with Eswatini's obligations under international and regional human rights law as well as Eswatini's Constitution.

"Eswatini: Broken Promises" Amnesty International Submission for the UN Universal Periodic Review, 39th Session of the UPR Working Group, 1 – 12 November 2021, "Restrictions to Fundamental Freedoms".
[664] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 270.
[665] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.

Public gatherings are regulated by the **Public Order Act 12 of 2017**, which requires a minimum of 48 hours advance notice to the relevant local authority of any gathering of more than 50 people. A local authority may prohibit an intended gathering if it believes that the gathering will "endanger the maintenance of public order and public safety".[666] As one positive point, the law explicitly requires police and local authorities to respect the rights of media and independent monitors to observe public gatherings and report on them., including the right to make video or audio recordings of public gatherings. It also states that a police officer "may not prevent or obstruct the lawful activities of journalists or independent monitors during gatherings".[667] Whether or not these safeguards are always observed in practice is a different issue.) Amongst the offences that apply to public gatherings is a prohibition on the use of "threatening, abusive or insulting words" or any act or display which is likely to result in "a breach of public order",[668] or doing anything "to incite hatred or contempt against the cultural and traditional heritage of the Swazi Nation".[669] The Act also contains a broadly-formulated offence of "intimidation or harassment" which includes the use of threats to reputation to influence persons to assume or abandon a particular standpoint.[670]

The **Obscene Publications Act 20 of 1927**, which could not be located online, makes it an offence to import, produce, sell or distribute any indecent or obscene publication, which is defined to include a newspaper or a magazine. Since the key terms "indecent" or" obscene" are not defined, this offence could be arbitrarily applied.[671]

Section 3 of the **Proscribed Publications Act 17 of 1968** empowers the Minister for Public Service and Information to declare any publication or series of publications to be a proscribed publication if it is prejudicial or potentially prejudicial to the interests of defence, public safety, public order, public morality or public health. This is done by notice in the *Government Gazette*, with no judicial involvement. It is an offence for any person, amongst other things, to distribute, print, publish or even possess a proscribed publication without the authority of the minister.[672] A 2001 notice which declared the *Guardian* newspaper and *The Nation* magazine to be proscribed publications was set aside by the High Court, on the grounds that the minister did not give any reasons for declaring the publications to be proscribed in the notice or in the papers filed with the court in response to the challenge to the notice. The Court accordingly declared the notice invalid.[673]

---

[666] Public Order Act 12 of 2017, sections 6 9 and 15(1), read with definition of "gathering" in section 2. See also section 16 on police power to prohibit any public event where "public disorder" is likely to arise.
[667] Id, section 14.
[668] Id, section 15(3)(b).
[669] Id, section 15(3)(h).
[670] Id, section 19.
[671] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 272.
[672] Proscribed Publications Act 17 of 1968, sections 3-4.
[673] *Swaziland Independent Publishers (Pty) Ltd T/A The Nation Magazine v the Minister of Public Service and Information* (Case 1155/01), as summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 282.

The **Cinematograph Act 31 of 1920** gives the minister discretion to require that any film intended for public showing must first be inspected by a state official.[674] No one may make a film (or take photographs for a film) that portrays gatherings of Africans or scenes of African life without the prior written consent of the Minister for Public Service and Information.[675] State authority is also required to make a film, or to take a photograph, of specified events that are observed in certain specified locations: Incwala Day (a cultural event), the King's Birthday, the Reed Dance (a cultural tradition that celebrates women's chastity and virginity) and Independence Day.[676] Violation of these requirement is a criminal offence.[677]

This Act also makes it an offence to exhibit an "objectionable picture", which includes films. A picture is objectionable if it represents any of the following in an offensive manner:

- impersonation of the king;
- scenes holding any member of the naval, military or air forces up to ridicule and contempt;
- scenes tending to "disparage public characters";
- scenes calculated to affect the religious convictions of any section of the public;
- scenes suggestive of immorality or indecency;
- executions, murders or other "revolting scenes";
- scenes of debauchery, drunkenness, brawling or any other habit of life not in accordance with good morals or decency;
- successful crime or violence;
- scenes that are in any way "prejudicial to the peace, order or good government" of the country.

The Minister also has complete discretion to declare any other picture to be objectionable. Notice of the declaration that a picture is objectionable must be given to the proprietor of any theatre which exhibits cinematograph films, and the exhibition of any prohibited picture is an offence punishable by a fine or imprisonment. [678] According to one local journalism lecturer: "The law is problematic because one cannot show an objectionable picture without getting permission from the Minister. The Minister's powers are not restricted, and he can determine what is objectionable. This impacts how the story of Eswatini is told."[679]

[674] Cinematograph Act 31 of 1920, sections 4-5.
[675] Id. section 3(1).
[676] Id, section 3(1bis).
[677] Id, section 3(4).
[678] Id, section 6.
[679] Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.

C) SIM CARD REGISTRATION (REGISTRATION OF ELECTRONIC COMMUNICATIONS AND MOBILE CUSTOMERS)

The **Swaziland Communications Commission (Subscriber Registration) Regulations, 2016** require service providers of electronic communications and mobile services to collect the full names, surnames and identity numbers of all their customers. Customers without identification documents must verify their identity with tax documents from Swaziland Revenue Authority, a bank statement, a municipal rates and taxes invoice, a recent telephone or cell phone account, a utility bill, a recent account from a retailer, a lease, a rental or credit sale agreement, an insurance policy, a television licence or a motor vehicle licence document. This requirement applies to both residents and foreign visitors. The identification information must be stored for five years after the end of the contract or service.[680] This removes the possibility of anonymous electronic communications.

D) TAKE-DOWN NOTIFICATIONS

A provision on take-down notifications is contained in the **Electronic Communications and Transactions Act, 2022**. Anyone can lodge a notification in electronic form with a service provider (a person or party that makes information services available) identifying material that is claimed to be unlawful and stating the remedial action required by the service provider. The service provider is not liable for taking down material in a *bona fide* response to a take-down notification but avoids civil liability for caching or hosting or linking to the material in question if it is removed, or if access to it is disabled, in response to a take-down notification. There is no involvement of a judicial authority, and no requirement that the person who posted the material be notified.[681] This scheme obviously militates in the direction of erring on the side of removing material on the basis of a mere allegation that it is infringing the rights of any person. A person who lodges a take-down notification knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.[682]

[680] Swaziland Communications Commission (Subscriber Registration) Regulations, 2016. Legal Notice No. 126 of 2016, issued in terms of section 54 of The Swaziland Communications Commission Act 10 of 2013 (which merely provides for regulations for the better carrying out of the Act).
[681] Electronic Communications and Transactions Act 3 of 2022, section 40 read with the definition of "service provider" in section 2 and with sections 37-39.
[682] Id, section 40(3).

7.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Eswatini will hold parliamentary elections in September 2023. By way of background, one article provides this very brief overview:

> *Eswatini - the last absolute monarchy in Africa where political parties are banned and lawmakers are sidelined by the king -- will hold parliamentary elections on September 29 […] The vote is unlikely to change the political scenery in the southern African nation of 1.2 million people that has been ruled by King Mswati III since 1986. The king wields absolute power. […] Elections in the country take place in a convoluted system that ensures Mswati faces no meaningful dissent. The vote comes two years after dozens of people were killed as police violently quashed demonstrations calling for democratic reforms. Winners in the 59 constituency ballots will take seats in parliament's lower house, along with 10 lawmakers that the king appoints directly. Mswati can veto any legislation, appoints the prime minister and cabinet, and is constitutionally above the law. He also selects 20 of the 30 senators in the upper house. The rest are elected by the lower house. Candidates cannot be affiliated to any political group under the constitution which emphasises "individual merit" as the basis for selecting members of parliament and public officials. […]*[683]

Another recent article gives a bit more detail about the election process:

> Eswatini is an absolute monarchy, but does have a unique electoral system, known as the *Tinkhundla* system, to conduct elections. The House of Assembly is made up of 66 seats, where 55 are elected via elections, 10 are appointed by the King and the remaining seat is given to the speaker of parliament who is chosen from outside of Parliament.
>
> The Senate on the other hand is made up of 31 members, 10 of whom are selected by the House of Assembly and 20 of whom are selected by the King. Under the *Tinkhundla* system, Eswatini is divided up into constituencies known as *inkhudla (Tinkhundla* in plural). The *Tinkhundla* are then divided up into smaller chiefdoms, where the first phase of elections takes place. Nominations for candidates to the legislature is done at the community level and in the open, where a person's name is called out and by a show of hands the community indicates if they nominate that person or not. The nominee then either accepts or rejects the nomination. A chiefdom must have at least three nominees, but no more than 20.
>
> Following the nomination process, primary elections take place in the chiefdom via secret ballot. The primary elections must produce one candidate to contest the secondary elections. Between the primary and secondary elections, the candidates have an opportunity to campaign for votes. However, since political parties are banned in Eswatini, candidates must campaign on a non-partisan basis. The secondary elections take place at the *Inkhudla* level to decide on the candidates who will represent the *Inkundla* at the national level.
>
> These scheduled elections are a key event in Eswatini. Elections have the potential in any country to heighten tensions and Eswatini may prove to be no different, especially

[683] "Eswatini to hold parliamentary elections in September", *Agence France-Presse*, 6 May 2023.

as tensions are already raised. Elections are also proving to be a point of contention amongst pro-democracy parties, as opinions are divided on whether or not to compete in the elections. Elections do provide an opportunity to get pro-democracy candidates into the national legislature, but an argument against competing in elections is that participation may be interpreted as condoning the current system of elections.[684]

Elections are supervised by the **Elections and Boundaries Commission (EBC)**, which is established by the Constitution. Article 90(9) of the Constitution requires that the Commission must act independently. However, in practice, the EBC is not considered impartial. "It is financially and administratively dependent on the executive, and its members are appointed by the king on the advice of the Judicial Service Commission, whose members are also royal appointees."[685]

ESWATINI CONSTITUTION

90. Elections and Boundaries Commission

i. There shall be an independent authority styled the Elections and Boundaries Commission ("the Commission") for Swaziland consisting of a chairperson, deputy chairperson and three other members.

i. The members of the Commission shall be appointed by the King on the advice of the Judicial Service Commission.
A person shall not be appointed member of the Commission where that person –

a. is a member of Parliament;
b. is or has been in the last five years actively engaged in politics;
c. is a public officer other than judge of a superior court or magistrate;
d. is an unrehabilitated insolvent;
e. has been convicted of an offence involving dishonesty in any country during the last ten years.

4. A person shall be deemed to be "actively engaged in politics" or to have been so engaged during the relevant period or any part of that period where that person –

a. is or was at any time during that period a member of the House or a Senator;
b. is or was at any time during that period, nominated as a candidate for election to the House or Bucopho Committee; or
c. is or was at any time during that period the holder of an office in any organization that sponsors or supports or has at any time sponsored or supported a candidate for election as a member of the House or Bucopho committee.

5. The members of the Commission shall be appointed for a period not exceeding twelve years without the option for renewal.

6. The chairperson, deputy chairperson and the other members of the Commission shall possess the qualifications of a Judge of the superior courts

[684] Katharine Bebington, "Eswatini: the year ahead", ACCORD, 24 February 2023.
[685] "Freedom in the World 2022: Eswatini", Freedom House, section A3.

or be persons of high moral character, proven integrity, relevant experience and demonstrable competence in the conduct of public affairs.

7. The functions of the Commission shall be to –
a. oversee and supervise the registration of voters and ensure fair and free elections at primary, secondary or other level;
b. facilitate civic or voter education as may be necessary in between elections;
c. review and determine the boundaries of tinkhundla areas for purposes of elections;
d. perform such other functions in connection with elections or boundaries as may be prescribed;
e. produce periodic reports in respect of work done.
8. Three members of the Commission including either the chairman or deputy chairman shall constitute a quorum.
9. A member of the Commission shall not enter upon the duties of that Commission until that member has taken and subscribed the oath of allegiance and oath for the due execution of office that are set out in the Second Schedule.
10. The provision of this Constitution relating to the removal of judges of the superior courts from office shall, subject to any necessary modifications, qualifications or adaptations, apply to the removal from office of the chairperson and other members of the Commission.
11. The office of any member of the Commission shall become vacant where that member resigns or circumstances arise that would disqualify that member for appointment as such.
12. If before the Commission has submitted its report under section 92 the office of chairperson or any other member of the Commission falls vacant or the holder of that office becomes unable for any reason to discharge the functions as chairperson or member of the Commission the King shall appoint another person to be chairperson or member as provided under subsection (2).
13. In the exercise of its functions under this Constitution, the Commission shall not be subject to the direction or control of any other person or authority.
14. There shall be a secretariat of the Commission provided by the Ministry responsible for elections.

There are several provisions of the **Election Act 6 of 2013** which are worded with sufficient open-endedness to raise concerns about how they might be applied. [686]

The Election Act contains a part that specifically covers election campaigns (quoted in full in the box below). Section 42 of this Part **prohibiting the use of "foul language"** is much wider than this heading suggests. The prohibition covers incitement to "public [dis]order, insurrection or violence"; statements that are "defamatory or insulting", statements that constitute "incitement to hatred" and statements that "excite or promote disharmony, enmity or hatred against any person".[687] These are very broad

[686] Elections Act 6 of 2013. Note that this Act is variously referred to as Act 6 of 2013 and Act 10 of 2013, with these differing references even appearing on material on the website of The Elections And Boundaries Commission.
[687] Elections Act 6 of 2013, section 42.

prohibitions that invite subjective application. Some have also expressed doubts that the restriction on campaigning during primary elections in section 39(1)) is enforced even-handedly.[688]

ELECTION ACT, 2013

PART VI ELECTION CAMPAIGN

39. CANVASSING FOR VOTES

(1) Canvassing for votes during primary elections is prohibited.

(2) A candidate contesting an election at secondary elections has the right to conduct campaigns freely in accordance with this Act.

(3) A candidate may, during an electoral campaign, publish campaign materials of such a nature and in a manner that may be approved by the Commission.

40. GENERAL CAMPAIGN

(1) The Commission shall prescribe a code of conduct to be complied with by all candidates during an election campaign.

(2) Subject to the provisions of this section and section 39, every candidate has the right to conduct that candidate's campaign freely.

(3) A public officer or public entity shall give and be seen to give equal treatment to all candidates to enable each candidate to conduct that candidate's campaign freely.

41. ORGANISED CAMPAIGN

(1) The Commission may determine the manner in which campaigns shall take place.

(2) In furtherance of subsection (1), the Commission shall give equal treatment to all candidates and enable each candidate to conduct that candidate's campaign freely, and each candidate shall be given an opportunity to address the meeting on matters of national interest and socio-economic development.

(3) The Commission shall ensure that adequate security is provided at campaign meetings organized by the Commission.

42. USE OF FOUL LANGUAGE PROHIBITED

(1) A person shall not, whether in a general or organized campaign, use any language –

(a) which constitutes incitement to public [dis]order, insurrection or violence;

(b) which is defamatory or insulting or which contains incitement to hatred; or

(c) which seeks to excite or promote disharmony, enmity or hatred against any person.

[688] See, for example, Nomfanelo Maziya, "Some current MPs perceived as campaigning in disguise", *Swazi Observer*, 4 July 2023; Delisa Thwala, "EBC half way through their weekend target", *Eswatini Positive News*, 31 May 2023.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding five thousand Emalangeni or to imprisonment for a period not exceeding one year or to both.

43. CLOSE OF CAMPAIGN

A campaign meeting shall not be held within twenty-four hours before the polling day.

Section 78 of the Act concerns **undue influence**. While there is no problem with prohibiting the use of threats of force, violence or restraint to influence another person during an election period, the broader prohibition on threats of any "physical, psychological, mental or spiritual injury, damage, harm or loss" or threats of doing "anything to the disadvantage of any person" could be broadly applied.[689] This provision has been identified by at least one local journalist as being potentially problematic, although the article quoted a differing opinion from a member of the Swaziland Multi-Stakeholder Forum who felt that is legal provision would not prevent attempts to influence people through campaigns such as road-shows, public statements, banners, speeches and other forums, as opposed to influencing people by waylay them and hitting them with a knobkerrie or other use of violence.[690]

ELECTION ACT, 2013, SECTION 78(1)

78. UNDUE INFLUENCE

(1) A person shall not directly or indirectly, by oneself or by any other person –
(a) make use of or threaten to make use of any force, violence or restraint upon any other person;
(b) inflict or threaten to inflict by oneself or by any other person, or by any supernatural or non-natural means, or pretended supernatural or non-natural means, any physical, psychological, mental or spiritual injury, damage, harm or loss upon or against any person; and
(c) do or threaten to do anything to the disadvantage of any person; in order to induce or compel any person –
(i) to register or not to register as a voter;
(iii) to vote or not to vote;
(iv) to vote or not to vote for any candidate;
(v) to support or not to support any candidate; or
(vi) to attend and participate in, or not to attend and participate in, any election meeting, march, demonstration or other election event;
(d) interfere with the independence or impartiality of the Commission, any member, employee or officer of the Commission;
(e) prejudice any person because of any past, present or anticipated performance of a function under this Act;

[689] Id, section 78(1). There is a similar provision on undue influence in the Voters Registration Act 4 of 2013, section 36.
[690] Mfanukhona Nkambule. "2-yr imprisonment for telling people not to vote", *Times of Swaziland*, 14 May 2023, which also quotes the contrary opinion of Sikelela Dlamini, the Secretary General of the Swaziland Multi-Stakeholder Forum.

(f) advantage, or promise to advantage, a person in exchange for that person not performing a function under this Act; or
(g) unlawfully prevent the holding of any election meeting.

ELECTION ACT, 2013, SECTION 79(2)

A person who, before or during an election, publishes any false statement of fact in relation to the personal character or conduct of a candidate in that election, shall be guilty of an illegal practice, unless that person can show that that person had reasonable grounds for believing, and did believe, the statement to be true.

Section 79 on the "**Illegal practice of publishing false statements in respect of candidates**" also contains some problematic aspects. The prohibitions on false claims of a candidate's illness, death or withdrawal from the election are not particularly worrying. However, this section also prohibits publication of "any false statement of fact in relation to the personal character or conduct of a candidate in that election", unless the publisher of the statement can show reasonable grounds for believing, and actual belief, that the statement was true. The maximum penalty for violation of the prohibition is a E20 000 fine or three years' imprisonment, or both.[691] It would be difficult to draw the line between fact and opinion in discussion of a candidate's character and conduct, and there is no defence of fair comment. The only defence articulated requires proof of actual belief of the truth of the statement, which would be difficult to establish in court beyond providing testimony of the accused's state of mind. Thus, this prohibition is likely to inhibit robust discussion of the merits and faults of the various candidates.

Section 81 on "**Illegal practices in respect of public meetings**" makes it illegal during the election period to act or incite others to act "in a disorderly manner for the purpose of preventing the transaction of the business for which the meeting is called". This formulation is also arguably overbroad.

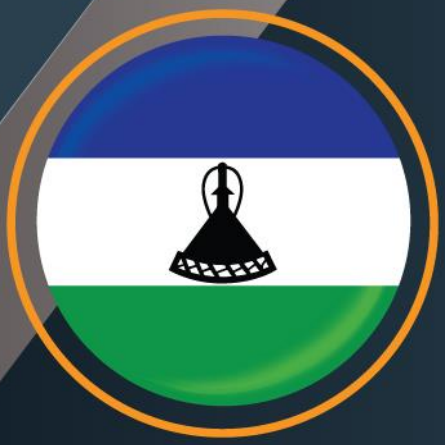
There are **restrictions on certain acts in the vicinity of a polling place on election day**, similar to those found elsewhere. It is illegal to do the following acts within 400 meters of a polling station: canvass for votes, solicit the vote of a specific voter, induce any person not to vote or induce any person not to vote for a particular candidate, It is also prohibited to exhibit any notice or sign within 100 hundred metres of the entrance to any polling station on a poling day (other than official notices relating to the election authorised by an election officer in terms of the Act).[692] These do not seem unreasonable.

No rules were located on fairness in broadcasting or other media coverage during election periods.[693] The **Broadcasting Code 2020** states only that election-related programmes including campaign reports and polling night results must not be sponsored by advertisers.[694]

[691] Id, section 79.
[692] Id, section 83(1)(d)-(e).
[693] The Broadcasting Code 2020 issued by the Eswatini Communications Commission does not cover this topic.
[694] Broadcasting Code 2020, item 5.10.1.3.

CHAPTER 8

LESOTHO



CHAPTER 8: LESOTHO

LESOTHO KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **67th globally; 13th out of 48 African countries** "Press freedom is fragile in Lesotho. Abuses against journalists are not uncommon and the media lack independence."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Lesotho's 1993 Constitution, as amended through 2011 There have been subsequent constitutional amendments, but none appear to have affected section 14. **14. FREEDOM OF EXPRESSION** 1. Every person shall be entitled to, and (except with his own consent) shall not be hindered in his enjoyment of, freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence. 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision – a. in the interests of defence, public safety, public order, public morality or public health; or b. for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting or television; or c. for the purpose of imposing restrictions upon public officers. 3. A person shall not be permitted to rely in any judicial proceedings upon such a provision of law as is referred to in subsection (2) except to the extent to which he satisfies the court that that provision or, as the case may be, the thing done under the authority thereof does not abridge the freedom guaranteed by subsection (1) to a greater extent than is necessary in a practical sense in a democratic society in the interests of any of the matters specified in subsection (2)(a) or for any of the purposes specified in subsection (2)(b) or (c). 4. Any person who feels aggrieved by statements or ideas disseminated to the public in general by a medium of communication has the right to reply or to require a correction to be made using the same medium, under such conditions as the law may establish.

KEY LAWS: • Computer Crime and Cybersecurity Bill, 2022 • As of July 2023, the Bill had been passed by Parliament and was awaiting Royal Assent.[695] • Penal Code Act 6 of 2012 (specific provisions) • Communications (Subscriber Identity Module Registration) Regulations 2021
CRIMINAL DEFAMATION: No[696]
DATA PROTECTION: Lesotho has a data protection law.[697]
ACCESS TO INFORMATION: Lesotho has no access to information law. A Receipt and Access to Information Bill was drafted in 2000 but has not progressed.[698]

8.1 CONTEXT

Newspapers, magazines and other periodical publications are required to register under the **Printing and Publishing Act 10 of 1967**. This law also requires that *all* "printed matter" must display the name and address of the proprietor, publisher and printer.[699] This is one of several laws identified by the Media Institute of Southern Africa (MISA) Lesotho Chapter) as being archaic and in need of repeal.[700]

The telecommunications, broadcasting and postal sectors are regulated by the **Communications Act 4 of 2012**, which replaced the Lesotho Communications Authority Act 5 of 2000.[701] The key regulatory body is the **Lesotho Communications Authority (LCA)**, which is appointed by the relevant minister after public invitations for recommendations or expressions of interest are issued.[702] The Communications Act states that the LCA "shall be independent and not subject to control by any person or authority".[703] However, one analyst notes that the LCA "has never been a particularly independent body", and that amendments to the Communications Act "have deprived it of much of the functional independence it once had and have given a significant number of powers to the minister".[704]

The critical issue of the LAC's lack of independence is under discussion as part of national institutional reforms under consideration in mid-2023, particularly the LCA's ability to discharge its regulatory functions devoid of influence from third parties.

[695] Mathatisi Sebusi, "Press incises 'draconian' cyber law", *Public Eye News*, 1 July 2023. Local observers say that, even at this stage, the bill might still be withdrawn and revised on the basis of recent civil society input.
[696] *Peta v Minister of Law, Constitutional Affairs and Human Rights* (CC 11/2016) [2018] LSHC 3 (18 May 2018).
[697] Data Protection Act 5 of 2012.
[698] "Access to information", MISA-Lesotho, undated.
[699] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 301. The text of the legislation could not be located online.
[700] "Position Paper for Multi-Sectoral Reforms", Media Institute Of Southern Africa (MISA-Lesotho Chapter), undated, page 11.
[701] Communications Act 4 of 2012, section 56.
[702] Id, section 6.
[703] Id, section 3(3).
[704] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 286.

National media reforms under discussion in 2023 include a proposal for the LCA to be transformed into a Lesotho Independent Communications Authority (LICA) which operates under the directon of officials appointed on the basis of merit.[705]

The LCA is responsible for licensing various classes of broadcasting services, and the Act provides that any audio, visual or any other content distributed via the internet may be licenced or regulated as "broadcasting".[706] It has been observed that this provision is overbroad "as it purports to require all content provided over the internet to be licensed by the LCA. It is not clear how these provisions could be enforced, particularly concerning social media content."[707]

There was a recent attempt to impose the LCA's power to regulate "internet broadcasting", when the LCA proposed **draft Lesotho Communications Authority (Internet Broadcasting) Rules, 2020**. These rules would have applied to internet posts accessible to at least 100 internet users in Lesotho, whether individually or in a series, and internet posts by users who have more than 100 followers in Lesotho, requiring "Internet broadcasters" that fell within this description to comply with broadcasting principles and standards.[708] The proposed rules would also have empowered regulators to conduct investigations where "internet broadcasters" were suspected of contravening broadcasting rules and to "direct or facilitate removal of such posts or content".[709] According to the Internet Society in Lesotho, while there is a public interest in the regulation of harmful behaviours on the Internet, the draft rules were an inappropriate instrument for addressing this problem and were "so disproportional that if enforced, will effectively shut down any content production and social media communication in Lesotho".[710] These rules led to many public objections and were ultimately rejected by the National Assembly.[711]

Under the Communications Act, the relevant minister can issue an **emergency suspension order** if the Minister has a reasonable basis to conclude that continued operation by a licensee poses "a substantial, direct and imminent threat to national security or public order" and that an emergency suspension is the only want to forestall the threat. Such an order can remain in effect for up to 72 hours, and longer if extended by a court.[712]

The Communications Act also establishes a **Broadcasting Disputes Resolution Panel (BDRP),** which is also selected by the minister after soliciting nominations and recommendations from the public. The BDRP is charged with preparing a

[705] Personal communication from MISA Lesotho, August 2023.
[706] Communications Act 4 of 2012, section 38(2). See also the Lesotho Telecommunications Authority (Broadcasting) Rules 2004, Legal Notice No. 71 of 2004,
[707] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 308.
[708] "Proposed Internet Broadcasting Rules 2020", Internet Society Lesotho Chapter, 28 October 2020; "Proposed Promulgation of the Lesotho Communications Authority (Internet Broadcasting) Rules, 2020", Internet Society Lesotho Chapter, 28 October 2020.
[709] Tawanda Karombo, "More African governments are quietly tightening rules and laws on social media", *Quartz*, 12 October 2020; "LEXOTA Country Analysis: Lesotho ", last updated July 2022.
[710] "Proposed Promulgation of the Lesotho Communications Authority (Internet Broadcasting) Rules, 2020", Internet Society Lesotho Chapter, 28 October 2020.
[711] Personal communication from MISA Lesotho, August 2023.
[712] Communications Act 4 of 2012, section 20.

broadcasting code of conduct that must address "obscene or offensive content and content that is likely to incite violence to persons or property"; "fairness, accuracy and balance of news broadcasts"; the protection of privacy; political advertising and other advertising and sponsorships.[713] The Act specifically states that, to the extent that the Code imposes any restriction on freedom of expression, such restrictions must be "no broader than necessary to achieve a compelling public interest", and imposed pursuant to transparent procedures in a non-discriminatory manner.[714] The final power to approve the Code rests with the minister.[715] The BDRP also addresses disputes about broadcasting content. Disputes that it cannot resolve within 90 days are referred to the LCA for decision.[716] The national media reforms under discussion in 2023 are also looking at possible changes to the broadcasting regulatory regime, noting that BDRP is not independent as it operates under the LCA, which is itself slated for reform.[717]

The state broadcaster is the **Lesotho National Broadcasting Service (LNBS)**, which is not regulated under any dedicated legislation. There have been discussions about enacting a law that would transform the state broadcaster into a public broadcaster with an independent board, but this idea has not moved forward.[718] The Lesotho News Agency (LENA) currently resorts under the ministry responsible for communications. As with the state broadcaster, proposals to transform this body into an autonomous news service with an independent board, have not materialised.[719]

The national media reforms currently under discussion include a proposed reform of the LNBS, to transform it into a three-tier broadcasting service that encompasses public broadcasting, commercial broadcasting and community broadcasting and is insulated from party-political influence, with Board members appointed on merit who would represent a wide variety of stakeholders.[720]

Institutions for media self-regulation have yet not been established. The Lesotho chapter of the Media Institute of Southern Africa (MISA) proposed the establishment of an independent National Media Council to regulate both print and electronic media, as part of a co-regulatory media system that brings together media self-regulation with a statutory regulatory system that allows for state intervention where self-regulation fails – thus constituting a hybrid of self-regulation and co-regulation. MISA Lesotho sees this approach as preferable to civil defamation actions that can result in exorbitant damages, leading to media self-censorship.[721]

A milestone that took place in 2021 was the adoption of the **National Media Policy 2021** by Parliament, as part of the overarching media reforms that are underway in

[713] Id, sections 39(8)(a) and 40(1).
[714] Id, section 40(2)
[715] Id, section 40 (3)-(5). The Broadcasting Code, 2022 can be accessed here.
[716] Id, section 41.
[717] Personal communication from MISA Lesotho, August 2023.
[718] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, pages 310-311.
[719] Id, page 311.
[720] Personal communication from MISA Lesotho, August 2023.
[721] "Lesotho: Protecting freedom of expression and information in 2020", MISA Lesotho, 3 May 2020; personal communication from MISA Lesotho, August 2023.

Lesotho. This policy was developed by media practitioners and its adoption was heralded by the Lesotho Chapter of the Media Institute of Southern Africa (MISA-Lesotho).[722] The government describes it as a guiding tool for the media fraternity that "aims to ensure that the media operate in a conducive environment".[723] This policy was not yet available online as of August 2023.

8.2 CONSTITUTION

Section 14 of the Constitution on freedom of expression) quoted on the first page of this chapter) is unusual in the region in that it enshrines a right to reply by "any person who feels aggrieved by statements or ideas disseminated to the public", in the same medium of communication where the statements appeared.[724]

The Media Institute of Southern Africa (MISA) in Lesotho and other stakeholders advocate amendments to section 14 of the Constitution to specifically protect media freedom, including the rights of digital users, as well as the right of access to information, the right to academic freedom and freedom of research, and artistic freedom.[725]

In 2003, in the *MO Africa Newspaper* case, Lesotho's High Court held that a newspaper caption relating to a pending criminal case did not violate the ***sub judice* rule** – which is a common law principle that restricts comment on pending court cases to avoid prejudicing the case outcomes. The newspaper caption questioned whether the real culprits had been caught in the case, in which two persons were being prosecuted for the assassination of the previous deputy Prime Minister, in which the army was suspected of being involved. The Court held that the caption in question did not rise to the level of scandalizing or prejudicing the criminal proceedings, which were a matter of public interest, and was thus protected by the constitutional right to freedom of expression. The High Court took the view that, while freedom of expression may be limited by principles such as the *sub judice* rule, such limitations must be narrowly interpreted and the "necessity for any restrictions must be convincingly established."[726]

In 2018, in the *Peta* case, the Constitutional Court declared **criminal defamation in section 104 of the Penal Code Act 6 of 2010** to be unconstitutional.[727] The challenge

[722] "Parliament adopts National media policy", MISA-Lesotho, 30 November 2021.
[723] Lesotho Ministry of Information, Communications, Science, Technology and Innovation website here.
[724] Lesotho's 1993 Constitution, section 14(4).
[725] "MISA Lesotho calls for Constitutional Amendment", MISA Lesotho, 28 April 2022; "Lesotho: Protecting freedom of expression and information in 2020", MISA Lesotho, 3 May 2020; Tsebo Matšasa, Mzimkhulu Sithetho and Dr Bob Wekesa, "The Lesotho National Dialogue and Stabilization Project Media Sector Reforms", 26 August 2019; personal communication from MISA Lesotho, August 2023.
[726] *Moafrika Newspaper: Rule Nisi (Sub-Judice Matter) (In R v. Mokhantso)* [2003] LSHC 24, 17 February 2003; see case summary by Global Freedom of Expression here.
[727] Section 104 of the Penal Code stated that a person "who, by print, writing, painting or effigy, or by any means otherwise than, solely by a gesture, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another, with intent to defame that other person, commits an offence of defamation." Section 101 defined "defamatory matter" as "matter likely to injure the reputation of any person by exposing him or her to hatred, contempt or ridicule, or likely to damage the person in his or her profession or trade by injury to his or her reputation, and it is immaterial whether at the time of the publication of the defamatory matter the person concerning whom the matter is published is living or dead". Penal Code Act 6 of 2012, sections 101 and 104.

was brought by Basildon Peta, the owner and editor of the *Lesotho Times*, who had been charged with the offence of criminal defamation following the newspaper's 2016 publication of a satirical column about the political power of a Lesotho Defence Force commander. The Court found the law to be an unacceptable restriction on freedom of expression because some of its key terms were overbroad and vague, and because it had the effect of criminalizing all satire which by its very nature distorts and exaggerates reality, and because it has a disproportionate chilling effect on media expression. The Court concluded that the offence did not pass the test of being reasonably and demonstrably justified in a democratic society and struck down section 104 of the Penal Code along with its accompanying sections 101-103.[728]

8.3 CASE STUDIES

In May 2023, journalist Ralikonelo 'Leqhashasha' Joki was fatally shot by known assailants as he left the privately-owned radio station *Ts'enolo FM* in Maseru. Joki was the host of a current affairs programme "Hlokoana-La-Tsela" (I Heard It Through the Grapevine) which covered government, agriculture, and corruption and was best known for a 2021 story about five politicians who were illegally trading in alcohol. in the months before the shooting, Joki had received at least three death threats from different Facebook accounts related to his work as a journalist. Although the motive behind Joki's killing remains unclear, many believe that it was related to his reporting.[729]

In 2021, radio journalist Lebese Molati was detained and allegedly choked by police after his report about the disappearance of guns belonging to the police. Molati was reportedly tortured, including attempts to suffocate him with a plastic bag, in an effort to force him to reveal the sources he had interviewed before being released without charge. His station, *357FM*, was suspended by the Lesotho Communications Authority shortly after this month for alleged non-compliance with broadcasting regulations.[730]

Also in 2021, police allegedly raided the studios and offices of radio station *People's Choice* (PCFM) and interrogated journalist Teboho Ratalane about the source of a police union press release that he had referred to on air in connection with a news story concerning the theft of 75 firearms.[731]

---

[728] *Peta v Minister of Law, Constitutional Affairs and Human Rights*, CC 11/2016,. 18 May 2018; see case summary by Global Freedom of Expression here.

[729] "Lesotho journalist Ralikonelo Joki killed after radio show", Committee to Protect Journalists, 15 May 2023.

[730] "Lesotho police arrest a radio presenter, suspend one station's license, and raid another", Committee to Protect Journalists, 14 December 2021; Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane, "Lesotho: Attacks against journalists intensify" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), pages 35-37; "Freedom in the World 2022 – Lesotho", Freedom House, section D1.

[731] "Lesotho police arrest a radio presenter, suspend one station's license, and raid another", Committee to Protect Journalists, 14 December 2021; Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane. "Lesotho: Attacks against journalists intensify", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA); "Freedom in the World 2022 – Lesotho", Freedom House, section D1.

In another 2021 incident, *Lesotho Times* investigative journalist Mohalenyane Phakela was reportedly barred by Lesotho's Chief Justice from covering the courts until his editor made an apology for stories previously published by the newspaper.[732]

In late 2018, military personnel allegedly threatened *Lesotho Times* investigative journalist Pascalinah Kabi, accusing him of infiltrating the Lesotho Defence Force with the intention to spy, endangering the security of the country by publishing information from a restricted military document and fomenting hatred.[733] Kabi had written articles about demands for compensation made by soldiers who had been accused of mutiny but were later reinstated.[734]

In 2018, government authorities laid a complaint of **incitement to violence** against the privately-owned *MoAfrika FM* radio station. The complaint cited four instances when the station aired critical reporting or commentary about government officials which the government claimed may have incited violence. The matter was referred to the Broadcasting Dispute Resolution Panel (BDRP) for resolution.[735]

In a separate 2018 incident, a spokesperson for the Prime Minister reportedly tried to force his way into the MoAfrika studio in Maseru, in reaction to the radio station's criticism of him. He was accompanied by a group of men. The station's editor-in-chief, Sebonomoea RK Ramainoane, then allegedly went on air and called on MoAfrika's "supporters" to come to the studio – and some people, including opposition politicians, did show up at the station. The government spokesperson denied the allegation that he tried to enter the studio forcibly but conceded that he had gone to the studio to ask why he has been "insulted" on air.[736] (The tactic of attempting to intimidate radio presenters or attacking them in their studios is apparently not unusual. It was reported in 2017 that this had happened at *Harvest FM*, *Thaha-Khube FM* and *Tšenolo FM*.[737])

In 2017 the same radio station was shut down by government for 72 hours, on the basis that it had **incited violence**. On that occasion, the station's editor-in-chief was arrested on charges of **criminal defamation**, which were not pursued after the law on criminal defamation was declared unconstitutional.[738]

There have been some past attempts to shut down the Internet:

> *In July 2016, leading up to the 2017 election in Lesotho, the government of Lesotho proposed a social media shutdown over concerns that State secrets were being published. The regulatory body, the Lesotho Communications Authority (LCA), refused*

[732] Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane. "Lesotho: Attacks against journalists intensify", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA).
[733] This may have been intended to reference the crime of sedition, which involves amongst other things bringing the government into "hatred or contempt". Penal Code Act 6 of 2012, section76(5)(a).
[734] "Lesotho military spokesman threatens investigative journalist", Committee to Protect Journalists, 21 December 2018.
[735] "Lesotho authorities accuse MoAfrika FM of incitement for critical reports", Committee to Protect Journalists, 15 August 2018.
[736] Id.
[737] "'Media self-regulation the way to go'", *Lesotho Times*, 5 May 2017.
[738] "Lesotho authorities accuse MoAfrika FM of incitement for critical reports", Committee to Protect Journalists, 15 August 2018.

the proposal and demanded that the government give a lawful written order if they wanted to shut off access to social media. Later that year, in November 2016, the government again pursued a social media shutdown and asked LCA to send a letter to the two main mobile/internet providers to "provide information on whether a temporary restriction of access to Facebook and Twitter usage was possible". The government sent the letter [to] the service providers, who subsequently leaked it to the public. LCA then held a meeting with officials from Facebook. The elections eventually happened on 3 June 2017, and there was no confirmed evidence of an internet shutdown. Because of a mixture of pressure from an independent regulator, civil society, and business interests, a likely internet shutdown was avoided.[739]

8.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) TECHNICAL CYBERCRIME PROVISION IN PENAL CODE

Lesotho currently has one provision on crimes specific to computers in its **Penal Code**. Section 62(2) criminalises unlawful access to a computer or an electronic storage device, where the access is used for certain actions that there is no reasonable cause to believe that the owner of the computer or storage device would authorise –

- to extract information; or
- to interfere with information, with the intention of securing an advantage or causing damage to electronic data or programmes.[740]

B) COMPUTER CRIME AND CYBER SECURITY BILL

As of July 2023, Lesotho's **Computer Crime and Cyber Security Bill** had been passed by Parliament. and was only awaiting Royal Assent. [741] However, local observers say that, even at this stage, the bill might still be withdrawn and revised on the basis of recent civil society input.[742]

In March 2021, a previous version of the cybercrime bill that was introduced into Parliament aroused widespread opposition from local rights groups. As a result, in September 2021, a parliamentary committee returned the bill to the executive with instructions to "reassess" it. This committee recommended further consultation and also expressed concern that the Bill conflated the issues of cybercrime and cybersecurity.[743] Then, after the October 2022 elections ushered in a new administration, the 2021 cybercrime bill resurfaced. On 9 May 2022, the National

[739] "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, pages 10-11.
[740] Penal Code Act 6 of 2012, section 62(2). There is no definition of "electronic storage device"
[741] Mathatisi Sebusi, "Press incises 'draconian' cyber law", *Public Eye News*, 1 July 2023.
[742] Personal communication, July 2023.
[743] "Freedom in the World 2022 – Lesotho", Freedom House, section D4; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 6.

Assembly passed the bill, which still required Senate approval at that stage.[744] In May 2023, after more intensive advocacy, the government again deferred the passing of the bill to allow for further consultations with stakeholders.[745] The analysis below is based on the version of the bill which was current as of mid-2023.

The explanatory statement for the bill includes the following motivation:

> *There are several legislations which provide for criminalisation of different offences such as fraud, extortion, forgery, bribery, genocide, crimes against humanity, war crimes, terrorism and other offences. However, there is no statute which provides for criminalisation of illegal activities committed through the use of electronic devices except for the Penal Code Act, 2012 and the Communications Act, 2012 which criminalise unlawful access to computer or electronic storage devices owned by another person, while the Communications Act criminalises intentional damage of communications facilities belonging to another. There is a need for a comprehensive legislation which adequately prevents computer and internet. related crimes. The Bill provides a list of offences committed through the misuse of electronic devices.*
>
> *The Bill further has provisions on procedural law which prescribe procedural standards relating to search, seizure obligations to assist the investigating officers, production of information, preservation of data, collection and disclosure of data and for interception and the use of forensic tools by law enforcement officers.*
>
> *The Bill provides for limitation of criminal liability of service providers. Cybercrime has no borders and therefore there is a need for international cooperation between States in the fight against cybercrime. The Bill provides that Lesotho should cooperate with other States in the fight against cybercrime.*[746]

The statement accompanying the bill also reports that it complies with both the Budapest Convention and the Malabo Convention.[747]

The bill provides for a **National Cybersecurity Advisory Council** and a **National Cybersecurity Incident Response Team**. It includes a long list of cybercrime offences.

COMPUTER CRIME AND CYBER SECURITY BILL, 2022 - TECHNICAL OFFENCES	
Clause 21: Illegal access	It is an offence, intentionally and without lawful excuse, to access the whole or any part of a computer system. There is an enhanced penalty where unauthorized access is gained by infringing security measures or with the intent of obtaining computer data.

[744] Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, pages 6-7; "Non-State Actors' Solidarity Key To Media Freedom", MNN Centre for Investigative Journalism, 7 June 2023.
[745] "Non-State Actors' Solidarity Key To Media Freedom", MNN Centre for Investigative Journalism, 7 June 2023.
[746] "Computer Crime and Cybersecurity Bill, 2022 Statement of Objects and Reasons", Senate of Lesotho, 19 May 2022.
[747] Id.

	○ Clause 2 defines "access" as "gaining entry to use data, computer program, computer data storage medium, computer system, their accessories or components or any part of the accessories or components or any ancillary device". ○ While some assert that criminalization of "mere access" without more is justified given that it compromises data confidentiality, there is no universal consensus on whether criminalization of mere access to non-protected systems is warranted, or whether this crime should be narrowed by additional conditions.[748] The *SADC Model Law on Computer Crime and Cybercrime* qualifies the offence of illegal access by requiring that it take place "intentionally, without lawful excuse *or justification* or in excess of a lawful excuse or justification".[749] ○ MISA Lesotho asserts that the unclear description of illegal access may give law enforcement agencies a basis for infringing on freedom of expression.[750]
Clause 22: Illegal remaining	It is an offence intentionally and without lawful excuse, by infringing security measures or with the intent of obtaining computer data or other dishonest intent, to remain logged in a computer system or part of a computer system or continue to use a computer system after the expiration of the time allotted for authorized access. ○ The intention requirements help to prevent this offence from being overbroad. ○ It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorized access.[751]
Clause 23: Illegal interception	It is an offence "dishonestly and without lawful authority" to use technical means to intercept a private transmission of computer data from or within a computer system.
Clause 24: Illegal data interference	All of the actions described in this clause are offences only if done "intentionally and without lawful excuse". It is an offence to do any of the following: • alter or damage computer data so as to make it lose its integrity or render it ineffective; • interfere with the lawful use of computer data; • communicate, disclose or transmit any computer data, program, access code or command to any person not authorized to access them; • access or destroy any computer data for purposes of concealing information necessary for an investigation into the commission or otherwise of an offence; or • accept computer data when not authorized to receive it. It is an offence with an even higher potential penalty to do any of the following:

[748] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
[749] SADC Model Law on Computer Crime and Cybercrime, section 4.
[750] "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
[751] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	• create, destroy, mutilate, remove or modify data or a program or any other form of information existing within or outside a computer or computer network; • activate, install or download a program that is designed to do any of these things; • create, alter or destroy a password, personal identification number, code or method used to access a computer or computer network. There is no liability for someone who does any of these things pursuant to legal authority. There is an enhanced penalty where an offence under this clause is committed in relation to data in a critical database or data concerned with national security or the provision of an essential service. For purposes of these offences, it is immaterial whether an illegal interference or its intended effect is permanent or temporary. o The most concerning part of the list of offences is accepting computer data that one is not authorized to receive. This could affect public access to data acquired by a whistleblower or placed in a cache such as Wikileaks. It is not clear if the exception of "lawful excuse" would apply to exposing such information in the public interest – and doubts about the application of this exception could result in self-censorship. o Regarding the enhanced penalties, there is no definition of "critical database", but clause 2 defines "critical information infrastructure" as "computer systems, devices, electronic communication networks, electronic communication facilities, computer programs or computer data so vital to the country that the incapacity or destruction of, or interference with, such systems and assets would have a debilitating impact on national or economic security or public health and safety". However, clause 18(2) give the minister the power to designate computer systems or any other systems as "critical information infrastructure" if their disruption would interrupt a life-sustaining or essential service; have an adverse effect on the country's economy; result in massive casualties or fatalities; result in the failure or substantial disruption of the country's money market; or have an adverse and severe effect on the country's security, including the intelligence and military services. Note that it has been asserted that best practice avoids potential risks arising from an overly broad definition of "critical infrastructure".[752] o Regarding the enhanced penalties, "national security" is undefined. o Regarding the enhanced penalties, clause 2 defines "essential service" as "a service the interruption of which endangers the life, personal safety or health of the whole or any part of the population".
Clause 25: Illegal system interference	It is an offence to input, transmit, delete, alter or suppress computer data, or to disrupt the use of a computer by any person with intent to hinder the proper functioning of a computer system. It is an offence to seize or destroy any computer medium with the intent of preventing proper use of a computer system,

[752] Id, page 15.

	It is an offence to willfully hinder or interfere with a computer system used in critical infrastructure operations, whether exclusively or generally, with the intention of affecting or impacting its lawful use.
	
	o "Hindrance" in relation to a computer system means any action that interferes with the proper functioning of a computer system and includes –
	  o cutting the electricity supply to a computer system;
	  o causing electromagnetic interference to a computer system;
	  o corrupting a computer system by any means; and
	  o inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (clause 2).
	o See the note on the meaning of "critical information infrastructure" in the row above.
	o The inclusion of specific intentions helps to narrow the listed offences.

Clause 26: Data espionage	It is an offence "intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification" to obtain for oneself or another person computer data which is not meant for that person and which is "specially protected against unauthorized access". o Without knowing that would be covered by "justification", it is possible that this offence could inhibit some instances of investigative journalism. o This formulation of the offence raises the question of how a person would know if data is "specially protected", as opposed to merely "protected". o Without more specificity, "unauthorized access" could be interpreted broadly to include data which is not legally protected, but has only been arbitrarily declared to be prohibited from access by a government official. [753] o It has been asserted that "data espionage" offences are unnecessary because they are covered by the general offence of unauthorized access.[754]
Clause 27: Cyber terrorism	It is an offence "willfully and without legal excuse" to use a computer and information system - • to communicate information intended to seriously intimidate a population, or to destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization; • to cause attacks upon persons which may lead to death, intimidation or kidnapping. This offence carries a maximum penalty of twenty years' imprisonment.
Clause 28: Cyber extortion	It is an offence "unlawfully and intentionally" to commit any offence in this law related to illegal access, interception of data or interference with data for purposes of obtaining any advantage from another person, or compelling another person to perform or to abstain from performing any act. This offence carries a maximum penalty of fifteen years' imprisonment

[753] Id.
[754] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	○ MISA Lesotho has commented that the bill is shallow on explaining cyber extortion, which may make it difficult for law enforcement agencies to implement the law accurately.[755]
Clause 29: Misuse of devices and software	It is an offence "intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification" to produce, sell, procure for use, import, export, distribute or otherwise make available any of the following: • a device, including a computer program, that is designed or adapted for the purpose of committing an offence under Part IV of the Act; • a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; • introduce or spread a software code that damages a computer or computer system, with the intent that it be used by any person for the purpose of committing an offence under Part IV of the Act. It is an offence even to possess any of the described items, with the exception of the software code. However, this offence requires the intent that the item in question is to be used by any person for committing an offence described in Part IV of the Act. ○ Clause 2 includes a wide and yet non-exhaustive definition of "device".
Clause 30: Computer-related forgery	It is an offence to input, alter, delete, or suppress computer data, resulting in inauthentic data. "with the intent that it be considered or acted upon for legal purposes as if it were authentic", regardless of whether or not the data is directly readable or intelligible. There is an enhanced penalty if this offence is committed by sending out multiple electronic mail messages from or through a computer system. ○ Clause 2 defines "multiple electronic mail messages" as "a mail message, including electronic mail, electronic text messages and instant messaging, sent to more than one thousand recipients". This is a better definition than that used in some other SADC countries which require only that multiple messages be sent to more than one person.
Clause 31: Computer-related fraud	It is an offence to cause loss of property to another person by any input, alteration, deletion or suppression of computer data, or by any interference with the functioning of a computer system, "with the fraudulent or dishonest intent of an economic benefit for oneself or for another person". ○ The required intent helps to ensure that this offence is properly targeted.
Clause 34: Identity related crimes	It is an offence to use a computer system to transfer, possess, or use a means of identification of another person with the intent to commit or to aid or abet, or in connection with, any unlawful activity that constitutes a crime. ○ The required intent helps to ensure that this offence is properly targeted.

[755] "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).

Clause 38: Unsolicited messages	It is an offence "intentionally without lawful excuse or justification" - • to use a computer system to relay or retransmit multiple electronic messages, with the intent to deceive or mislead, or to use any electronic device that does not reflect the origin of such messages; • to materially falsify header information in multiple electronic messages and intentionally initiate the transmission of such messages. o In contrast to the laws in other SADC countries, here it is specifically NOT a defence if the transmission of multiple electronic messages in question takes place within customer or business relationships. This makes sense here since the formulation of the offence requires the intent to deceive or mislead, hiding the origin of the messages or falsifying aspects of the messages – none of which would be acceptable business practices. o Clause 2 defines "multiple electronic mail messages" as "a mail message, including electronic mail, electronic text messages and instant messaging, sent to more than one thousand recipients".
Clause 44: Cyber squatting	It is an offence to intentionally take or make use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right.
Clause 45: Social engineering attacks	It is an offence to create or operate a website, or send a message through a computer system, with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system.
Clause 46: Interception of electronic messages or money transfers	It is an offence unlawfully or without authority to intercept an electronic message or process through which money or information is being conveyed. o This offence appears to lack an appropriate criminal intent.
Clause 47: Willful misdirection of electronic messages	It is an offence to "willfully and maliciously" misdirect electronic messages.
Clause 48: Inducement to deliver electronic messages	It is an offence to induce any person in charge of electronic devices "to deliver any electronic messages not specifically meant for him".
Clause 49: Intentionally withholding messages delivered erroneously	It is an offence intentionally to hide or detain any electronic mail, message, or payment card which was found by the person or delivered to the person in error and which ought to be delivered to another person. o It is not clear what efforts are required to avoid committing this offence if one receives a message intended for another in error.
Clause 50: Unlawful destruction of	It is an offence unlawfully to destroy or abort any electronic mail or process through which money or information is being conveyed.

electronic message	○ Again, it is not clear what efforts would be required to avoid this offence if one receives a message intended for another in error. It is not clear what the qualifier "unlawful" would capture.
Clause 51: Issuance of false electronic instructions	It is an offence for a person who is authorized to use a computer or other electronic device to issue false electronic instructions "with intent to deceive".
Clause 52: Modification and interference with contents of a message	It is an offence "intentionally and without lawful excuse" to modify or interfere with the contents of any message sent by means of a communication service". ○ A "communication service" is defined in clause 2 as "an operation or provision for transmission of voice, data, text, sound, video and images". ○ This is a very broadly-formulated offence. The phrase "without lawful excuse" is a limiting factor, but it may leave room for doubt as to what is allowed in terms, for instance, of modifying a message received and then forwarding it to someone else without any criminal or malicious intent. ○ This overlaps with section 44(1)(e) of the Communications Act 4 of 2012, which makes it an offence to "intentionally modify or interfere with the contents of any message sent by means of a communications service" – which in that Act refers to a broadcasting, postal or telecommunications service.[756]
Clause 54: Offences against critical information infrastructure or protected computer systems	Where a person commits an offence under this Act in relation to "critical information infrastructure", the maximum penalty is M15 million or 25 years' imprisonment or both. ○ The heading of the offence refers to "protected computer systems", but there is no reference to these in the text and no definition of the term in the bill. ○ As noted above, clause 2 defines "critical information infrastructure" as "computer systems, devices, electronic communication networks, electronic communication facilities, computer programs or computer data so vital to the country that the incapacity or destruction of, or interference with, such systems and assets would have a debilitating impact on national or economic security or public health and safety". However, clause 18(2) give the minister the power to designate computer systems or any other systems as "critical information infrastructure" if their disruption would interrupt a life-sustaining or essential service; have an adverse effect on the country's economy; result in massive casualties or fatalities; result in the failure or substantial disruption of the country's money market; or have an adverse and severe effect on the country's security, including the intelligence and military services. Note that it has been asserted that best practice avoids potential risks arising from an overly broad definition of "critical infrastructure".[757]

[756] Communications Act 4 of 2012, section 44(1)(e) read with the definition of "communications service" in section 2.
[757] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 15.

	○ This overlaps with some other offences which already refer to actions against critical information infrastructure.
Clause 56: General provision on cybercrimes	Any offence under any Act which is committed in whole or in part through the use of a computer, electronic device or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification. ○ This provision appears to be aimed at ensuring that any crime committed with computer tools can be prosecuted under the relevant law for that crime.

The Bill creates eight content-related offences, covering a broad array of topics.

COMPUTER CRIME AND CYBER SECURITY BILL, 2022 – CONTENT-BASED OFFENCES	
Clause 32: Child pornography	There is an extensive set of offences relating to "child pornography". The production of child pornography is an offence regardless of the medium used, but the other acts relating to child pornography are offences only if they involve a computer system or information and communication technologies. The only articulated defense is where the child pornography was for a *bona fide* law enforcement purpose. It is also an offence to knowingly expose children to pornography through a computer system, or to knowingly facilitate a child's access to pornography through a computer system. The maximum punishment for any offence in this section is imprisonment for 20 years. ○ "Child pornography" is defined as "any material that visually depicts a child engaged in real or simulated sexually explicit conduct, or any depiction of the sexual organs of a child, for primarily sexual purposes (clause 32(1)). However, there is no definition of "child", which could create some uncertainty.[758] ○ There are no exceptions for materials that are for genuine artistic, educational, legal, medical, scientific or public benefit purposes, meaning that some innocent material could be considered illegal.
Clause 33: Distribution of data message of intimate image without consent	It is an offence to make available, broadcast or distribute, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give consent. "Intimate image" for this purpose means "a visual depiction of a person made by any means under circumstances that give rise to a reasonable expectation of privacy, and in which the person is nude, or exposing his genital organs or anal region or, in the case of a female, her breast."

[758] "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).

	○ Some other countries apply this offence if the person who shared the images was reckless about the existence of consent. ○ The Bill limits the channels through which the intimate messages are conveyed to "a computer system" – defined in clause 2 as "a device or a group of'inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other related function" - which may not be sufficient to keep up with all the ways in which social media messages are transmitted.[759]
Clause 35: Racist and xenophobic material	It is an offence "intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification" - • to produce racist or xenophobic material for the purpose of its distribution through a computer system; • to offer or make available racist or xenophobic material through a computer system; • to distribute or transmit racist or xenophobic material through a computer system; or • to distribute racist or xenophobic material that may constitute a threat through a computer system. ○ Clause 2 defines "racist and xenophobic material" as "any material, including any image, video, audio, recording or any other representation of ideas or theories which advocates, promotes or incites hatred, discrimination or violence against any individuals based on race, colour, descent or national or ethnic origin as well as religion". ○ Note that this offence, in contrast to the one below, does not require that material based on religion is actionable only if religion is used as a pretext for one of the other grounds. ○ There seems to be an unnecessary overlap between distributing *any* racist or xenophobic material through a computer system, and distributing racist or xenophobic material *that may constitute a threat* through a computer system. ○ As noted above in respect of the provision on child pornography, the limitation of this offence to use of a "computer system" may be too limiting to capture what was intended. ○ This extends the provision in the Penal Code on hate speech to computer systems. However, the Penal Code refers to the expression of "hatred, ridicule or contempt", and it includes the protected grounds of gender and disability that are not included in the cybercrime bill.[760] These provisions should be harmonized.
Clause 36: Racist and xenophobic motivated insult	It is an offence "intentionally and without lawful excuse", publicly and through a computer system to use language that "incites attacks and insults" to a person or a group of persons on the basis of race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors. ○ The Malabo Convention refers to "insult" on any of the prohibited grounds, while this offence refers to inciting attacks or insults from others. The different approach here may have been intended to narrow the proposed offence, but it still seems overbroad.

[759] Id.
[760] Penal Code Act 6 of 2012, section 78.

Clause 37: Genocide and crimes against humanity	It is an offence "intentionally and without lawful excuse" to distribute or otherwise make available through a computer system to the public or to another person "information intended to aid, induce or incite others to commit genocide or crimes against humanity". o There is no definition of "genocide" or "crimes against humanity". o In contrast to similar crimes elsewhere in the region and in the Malabo Convention, this offence is forward-looking rather than backward-looking. The Malabo Convention makes it an offence to deny, approve or justify genocide or crimes against humanity; this offence in contrast, criminalises only the encouragement of others to commit genocide or crimes against humanity.
Clause 40: Cyber-bullying and harassment	It is an offence "intentionally, without lawful excuse" – • to initiate any electronic communication with the intent to coerce, intimidate, harass, abuse, or cause emotional distress to a person; or • to initiate offensive and obscene communication with the intent to disturb the peace, quiet and privacy of another person, whether or not a conversation ensues. It is an offence "intentionally and without lawful excuse" to initiate any electronic communication or use a computer system with the intent to support severe, repeated and hostile behaviour. o These offences seem overbroad since there is no definition of "harass", or of what constitutes "hostile" behaviour. intent to cause emotional distress is also very subjective. For example, this offence might be used against a journalist who repeatedly approaches a political figure seeking comment on charges of wrongdoing – which could cause emotional distress or be perceived as being done with an intent to harass. o It would be useful to provide restraining orders in cases of genuine. well-defined harassment where no prison sentence is imposed.
Clause 41: Violation of intellectual property rights	It is an offence "for commercial purposes" to willfully use any computer or electronic device to violate any intellectual property rights protected under any law or treaty applicable to Lesotho.
Clause 43: Publication of false information	It is an offence to publish "information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to threaten, abuse, insult, mislead or deceive the public". o The inclusion of "insult" is particularly overbroad here. It is extremely difficult to ensure that any information is not "false, deceptive, misleading or inaccurate" in some respect – and no requirement that the falsity be related to a "material" aspect, Even if the formulation were improved, however, this would still be a problematic provision that is prone to abuse. This issue would be better addressed via existing civil defamation law. o This draft provision has inspired the most debate. It has been observed that it has the effect of bringing back criminal defamation, which has already been found unconstitutional (as discussed above). This provision has been identified as being particularly likely to be abused

	and threaten freedom of expression. One person commented: "This section flies in the face of a multiplicity of ordinarily allowed, tolerated, and countenanced ways of society poking fun at itself for comic effect, social commentary and political satire or caricature; and it is likely to be abused by powerful groups against socially constructive exertions of the categories like conventional and social media including citizen journalism, artists and cartoonists, and even mainstream scholars."[761]

In general, **attempt, abetment and conspiracy to commit any of the offences in the Act** – both technical and content-based – is also an offence.[762] It has been asserted that the **penalties** provided in the bill are not proportionate to the various crimes.[763]

With respect to procedural issues in the bill, **searches and seizures** require a warrant from a court (no specific court is specified) based on an affidavit from a law enforcement officer that there are reasonable grounds to suspect that there may be a computer system, device or computer data in a certain place that is either material evidence in proving an offence, or that has been acquired by a person as a result of an offence.[764] A "law enforcement officer" means any officer of the Lesotho Mounted Police Service or the Directorate on Corruption and Economic Offences.[765] A law enforcement officer who is undertaking a search is empowered to seize or secure computer data, take steps to maintain the integrity of preserved data, render remove or make inaccessible the stored data or information from a computer system or a computer storage medium and retain a copy of such data or information.[766] Where a court has issued a warrant, a person who is not a suspect but who has knowledge about the functioning of the computer system or the relevant security measures has a duty to assist law enforcement agents.[767]

A court also has the power, in response to an application by a law enforcement officer, to **issue production orders** to service providers or other persons in control of computer systems.[768] A law enforcement officer may also apply to a court for a **preservation order** in respect of any kind of computer data for an initial period of 14 days, which can be extended for any specified time period by the court.[769] The court can also authorise the collection of **partial traffic data** by law enforcement officers for the purposes of a specific criminal investigation; this applies to traffic data about a specified communication that can identify the internet service provider or the path through which a communication was transmitted.[770] (In some other jurisdictions this step does not require judicial authority.) A court can also authorise the **general collection of traffic data associated with a specified communication during a**

[761] Matšeliso Phulane, "Cyber law slammed, again", *The Reporter*, 15 December 2022, quoting Mokitimi Tšosane of the Transformation Resource Centre (TRC); "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 6.
[762] Computer Crime and Cybersecurity Bill, 2022, clause 42.
[763] Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
[764] Computer Crime and Cybersecurity Bill, 2022, clause 59.
[765] Id, clause 2 (definition of "law enforcement officer").
[766] Id, clause 59(3).
[767] Id, clause 60.
[768] Id, clause 61.
[769] Id. clause 62.
[770] Id, clause 63.

specified period, including the use of "technical means" to collect or record such data. There is no time limit on the period that may be covered by the court authorization.[771]

Furthermore, the court may issue authority for the use of a **remote forensic tool** or a **direct access forensic tool** for monitoring purposes, including the installation of a forensic tool on the suspect's computer system. Such an authority is limited to 3 months, with no mention of renewal.[772]

The bill contains a provision allowing a court to order forfeiture of assets for persons convicted of any offence under the statute. This can apply to any asset, money or property constituting or traceable to the proceeds of the offence, as well as any computer, equipment, software or other technology used or intended to be used to commit or facilitate the offence. The Act also requires in every case that persons convicted of an offence under the statute must forfeit their passport or international travelling document to the State until they have paid any fines or served any sentence imposed. A court may release a person's travel document upon application if travel is required for medical treatment or in the interest of the public. or where the King has pardoned the convicted person.[773]

INTERNAL SECURITY (GENERAL) ACT, 1984

34. Incitement to public violence
A person who, in any place whatever, acts or conducts himself in such manner or speaks or publishes such words that it might reasonably be expected that the natural and probable consequences of his act, conduct or speech or publication will, under the circumstances, be the commission of public violence by members of the public generally or by persons in whose presence the act or conduct took place or to whom the speech or publication was addressed, is guilty of an offence and is liable on conviction to a fine of one thousand Maloti or to imprisonment for a period of five years or to both.

Penal Code Act 6 of 2012

85. Provoking public violence
A person who, in any place acts or conducts himself or herself in such a manner or speaks or publishes such words from which there is a real likelihood that the natural and probable consequence of his or her act, conduct or speech or publication will under the circumstances lead to the commission of public violence by members of the public generally or by persons in whose presence the act or conduct takes place or to whom the speech or publication is addressed, commits an offence.

The proposed provisions for collecting evidence on cybercrimes are supplemented by provisions in the **National Security Services Act, 1997** that empower the relevant minister to authorise the interception of communication on the grounds that an offence has been, is being or is likely to be committed, and that it could constitute a threat to national security or have a bearing on the functions of the National Security Services. An interception authorisation issued by the minister is valid for a period of six months and can be extended if the minister finds it necessary. This Act also gives the minister power to issue a warrant in respect of any property specified in the

[771] Id, clause 67.
[772] Id, clause 68. Clause 2 defines a "remote forensic tool" as "an investigative tool, including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include keystroke logging or transmission of an internet protocol address". A "direct access forensic tool" is not defined.
[773] Id, clause 77.

warrant, in order to obtain information which that is likely to be of substantial value in assisting national security services in discharging any of their functions if the information cannot reasonably be obtained by any other means.[774]

C) OTHER LAWS THAT MAY LIMIT FREEDOM OF EXPRESSION

MISA-Lesotho has identified 14 laws that impact on media freedoms and freedom of expression.[775] These are some of the key provisions of concern:

- The **Sedition Proclamation 44 of 1938** makes it an offence to print, publish, sell, distribute or import any seditious publication. The definition of sedition is very broad and includes inciting "disaffection against the Government" and promoting "feelings of ill-will and hostility" between different classes of the population.[776] This offence is replicated in section 76(2)(c) of the **Penal Code**, discussed below.
- Section 10(1) of the **Printing and Publishing Act, 1967** makes it an offence to import, print, publish, sell, offer for sale, distribute, or reproduce a statement which poses a danger to, among other things, "public safety" and "public order" which can be broadly interpreted.[777]
- Section 4 of the **Official Secrets Act, 1967** makes it an offence for any person to communicate any information regarding a prohibited place or information that is otherwise in contravention of the Act.
- The **Internal Security (General) Act, 1984** contains a number of vague offences related to "subversion" and "subversive activities", including uttering or writing any words with a "subversive intention" – with "subversive" being very widely defined and including anything intended to "incite disaffection" towards any public officer.[778] It also authorises arrest without a warrant of anyone suspected to be involved in "subversive activity".[779]
- Section 34 of the **Internal Security (General) Act, 1984** makes it an offence to, among other things, speak or publish words that might reasonably be expected to result in the commission of public violence,[780] which is replicated by section 85 of the **Penal Code** on provoking public violence.[781] These charges have been utilised against journalists in practice.

---

[774] National Security Services Act 11 of 1998, sections 26-27, discussed in "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 8. (CIPESA mistakenly refers to the Act as being dated 1997.)

[775] African Media Barometer: Lesotho 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 12. See also "Lesotho: National Overview", MISA-Lesotho, 2012 at page 47 which lists 13 laws that have concerning provisions: 1. Obscene Publication Proclamation No. 9 of 1912, 2. Sedition Proclamation No 44 of 1938, 3. Printing and Publications Act, 1967, 4. Official Secrets Act, 1967, 5. High Court Act, 1978, 6. Criminal Procedure and Evidence Act, 1981, 7. Internal Security Act (General) Act, 1984, 8. Emergency Powers Order 1988, 9. National Assembly Elections Order 1992, 10. Constitution of Lesotho 1993 (Article 14(2)), 11. The Parliamentary Powers and Privileges Act, 1994, 12. Police Service Act 1998, 13. Financial Institutions Act, 1999.

[776] African Media Barometer: Lesotho 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 12.

[777] Id.

[778] Internal Security (General) Act 24 of 1984, section 7(a) read with definition of "subversive" in section 3.

[779] Id, section 13.

[780] Id, section 34.

[781] Penal Code Act 6 of 2012, section 85.

- It is also an offence under section 24 of the **Internal Security (General) Act, 1984** to use obscene, abusive, threatening or insulting words or behaviour in a public place, or to swear, shout, scream or otherwise conduct oneself with intent to provoke a breach of the peace, or whereby a breach of the peace is committed or likely to be committed even if that was not the intention of the speaker.[782] This offence is replicated in section 84 of the **Penal Code** on breach of the peace.[783] These offences could clearly be used to constrain freedom of expression during protests.

The **Penal Code** includes a number of provisions that could inhibit free expression. Perhaps the most often used were the sections on **criminal defamation**, which have been held to be unconstitutional.[784] In addition to section 84 on breach of the peace and section 85 on provoking public violence, discussed above, the following are some of the provisions of concern: `

- The crime of **sedition** in section 76 (reproduced in the box below) is broadly defined and applies to words and publications as well as actions, and when it comes to government criticism, there is a fine line between what is permitted and what is prohibited.
- It is an offence to show **disrespect, contempt or irreverence for the national flag or anthem**.[785]
- It is an offence to **violate the dignity or injure the reputation of anyone in the Royal Family** although, interestingly, it is a defence if this was "a genuine response to provocative acts emanating from any member of the Royal Family".[786]
- **Hate speech** is an offence. It is illegal to utter any words or publish any writing expressing "hatred, ridicule or contempt for any person or group of persons, wholly or mainly because of race, ethnic affiliations, gender, disability or colour, commits of an offence".[787]
- It is for a person to make or publish an **untrue statement calculated to bring any judicial officer or court into disrepute** (referring to a statement that the person in question "knows or has reasonable grounds to suspect" is untrue).[788]

[782] Id, section 24.
[783] Penal Code Act 6 of 2012, section 84.
[784] See section 8.2 of this chapter. Sections 101-104 of the Penal Code Act 6 of 2012 were struck down on constitutional grounds.
[785] Penal Code Act 6 of 2012, section 77
[786] Id, section 79.
[787] Id, section 78.
[788] Id, section 90.

PENAL CODE

76. Sedition

(1) A person who, with a number of other people, comes together in an unlawful gathering with the intention of defying or subverting the authority of the Government of Lesotho, but without the intention to overthrow or coerce the Government of Lesotho, commits an offence of sedition.

(2) A person who –
(a) does or attempts to do or makes any preparation to do, or conspires with any person to do, any act with seditious intention;
(b) utters any seditious words;
(c) prints, publishes, sells, offers for sale, distributes or reproduces any seditious publication; or
(d) knowingly imports any seditious publication, commits an offence.

(3) A person who, without lawful excuse, has in his or her possession any seditious publication, commits an offence.

(4) No prosecution for an offence under this section shall be initiated except within six months of the commission of the offence.

(5) A seditious intention is an intention –
(a) to bring into hatred or contempt or to excite disaffection against the person of His Majesty or the Government of Lesotho as by law established;
(b) to incite the people and residents of Lesotho to attempt to procure the alteration, otherwise than by lawful means, of any law in Lesotho;
(c) to bring into hatred or contempt or to excite disaffection against the administration of justice in Lesotho;
(d) to cause discontent or disaffection amongst the people and residents of Lesotho; or
(e) to promote feelings of ill-will and hostility between different classes of the population of Lesotho.

(6) An act, speech or publication is not seditious if its effect is to –
(a) show that the Government has been misguided in or mistaken in any of its measures;
(b) point out errors or defects in the Government or Constitution of Lesotho as by law established or in legislation or in the administration of justice with a view to the remedying of such errors or defects; or
(c) identify and criticise with a view to their discussion or removal of any matters which are producing or have a tendency to produce feelings of ill-will, hostility and enmity between different classes of the population of Lesotho.

(7) In determining whether the intention with which an act was done, any words were spoken, or a document was published, was or was not seditious, every person shall be deemed to intend the consequences which would naturally

flow from his or her conduct at the time and under the circumstances in which he or she so conducted himself or herself.

(8) For the purposes of this section –

(a) "publication" includes all written matter and everything whether of a nature similar to written or printed matter or not, containing any visible representation, or by its form, shape, or in any manner capable or suggesting words or ideas, and every copy or reproduction of any publication

(b) "seditious publication" means any publication having a seditious intent;

(c) "seditious words" means any words having a seditious intent.

D) STATE SURVEILLANCE

According to CIPESA (Collaboration on International ICT Policy for East and Southern Africa):

> *The **National Security Services (NSS) Act 1997** in section 27(2) empowers the minister to give direction for the interception of communication if convinced by an application from an authorised NSS officer that there is an offence that has been, is being or is likely to be committed, and is a threat to the national security or that the information has or could have a bearing on the functions of the NSS. The minister is required to sign the interception authorisation which is valid for a period of six months and can be extended for a similar period if the minister finds it necessary as per section 27(3). With respect to urgent requests, section 27(4) empowers the NSS Director General or an officer authorised by the Director General to sign the authorisation if the minister has expressly authorised its issue. In such a case, the authorisation is valid for two working days.*[789]

E) SIM CARD REGISTRATION

In May 2021, the government proposed regulations that mandated the Lesotho Communications Authority (LCA) to establish and maintain a central database linking personal information to SIM cards, including the holder's physical address and biometrics. These regulations would have given security agencies access to the central database on a written request to the LCA stating the purpose for which the information is requested. These proposed regulations inspired heated public opposition. For example, the Media Institute of Southern Africa (MISA) argued that making personal data easily accessible to security agencies without judicial consent could violate privacy rights and inhibit free expression. As a result, the proposed regulations were amended to require security

[789] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33 (footnote omitted and emphasis added).

agencies to obtain a subscriber's consent or court authorization for access to personal data.[790]

The final **Communications (Subscriber Identity Module Registration) Regulations 2021** require customers to present a national identity document or other identification verification to a service provider to obtain or retain a SIM card. There is no biometric verification. The identifying information is retained by the service provider (as opposed to in a central government database), and third parties may access this data only with the written consent of the customer or a court order.[791]

F) ACCESS TO TRAFFIC DATA

The **proposed Communications (Compliance Monitoring and Revenue Assurance) Regulations 2021** sought to provide procedures for the collection and access of telecommunications traffic data. These regulations would require telecommunications licensees to submit telecommunications traffic data to a central authority on a monthly basis. Law enforcement officials or the national security agency would be able to access this traffic data without a court order or a warrant. The proposed regulations were not approved by Parliament, and consultations with stakeholders are continuing.[792]

G) TAKE-DOWN NOTIFICATIONS

Lesotho's **draft Electronic Transactions and Electronic Commerce Bill 2013** (which appears to still be under discussion as of mid-2023) includes a proposal for the removal of information by a service provider upon receipt of a notification from a complainant alleging that it is the subject of unlawful activity. This notification takes the form of an electronic communication sent to the service provider or its designated agent. A service provider is not liable for a wrongful take-down in a *bona fide* response to a notification of unlawful activity, which mitigates in favour of removal of any allegedly offending material. Expeditious removal or disabling of access in response to receipt of a take-down notification from an aggrieved party would also give protection against liability to a service provider that was merely hosting, caching or providing links to the data in question. There is no provision for notice to the person who put the information online. A person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.[793]

---

[790] "2022 Country Reports on Human Rights Practices: Lesotho", US State Department, section 2A; "Lesotho: Authorities Should Withdraw Communications Regulations", Freedom House, 21 June 2021; "Lesotho: Communications Regulation 2021 (Subscriber Identity Module and Mobile Device Registration)", MISA Lesotho, 8 July 2021; "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 34.
[791] Communications (Subscriber Identity Module Registration) Regulations 2021.
[792] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, pages 8-9.
[793] Draft Electronic Transactions and Electronic Commerce Bill 2013, clauses 45-48.

CHAPTER 9

MADAGASCAR

CHAPTER 9: MADAGASCAR

MADAGASCAR KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **34th globally; 4th out of 48 African countries** "Despite a long media tradition going back more than 150 years, Madagascar's media landscape is highly polarised and politicised, and heavily impacted by corruption."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Madagascar's 2010 Constitution (in English) **ARTICLE 10** The freedoms of opinion and of expression, of communication, of the press, of association, of assembly, of circulation, of conscience and of religion are guaranteed to all and may only be limited by the respect for the freedoms and rights of others, and by the imperative of safeguarding the public order, the national dignity and the security of the State. **ARTICLE 11** Any individual has the right to information. Information under all its forms is not submitted to any prior constraint, except that which infringes the public order and the morality. The freedom of information, whatever the medium, is a right. The exercise of this right includes duties and responsibilities, and is submitted to certain formalities, conditions, or sanctions specified by the law, which are the measures necessary in a democratic society. All forms of censorship are prohibited. The law organizes the exercise of the profession of journalist.
KEY LAWS: • Loi n°2014-006, as amended by Loi n°2016-031: La lutte contre la cybercriminalité • Loi n°2016-029, as amended by Loi n°2020-006: Code de la Communication Médiatisée • Code Pénal, Mis à jour au 31 mars 2005 (selected provisions)
CRIMINAL DEFAMATION: Yes[794]

[794] "Madagascar's 3rd Universal Periodic Review, 34th Session (Oct-Nov 2019), Submission by Southern Africa Litigation Centre", paragraphs 12-17.

DATA PROTECTION: Madagascar has a law on data protection.[795]
ACCESS TO INFORMATION: Madagascar does not have a law on access to information[796] although Article 11 of the Constitution (quoted above) guarantees the right to information.

THIS CHAPTER WAS PREPARED WITH THE AID OF VARIOUS ONLINE TRANSLATION TOOLS.

9.1 CONTEXT

Reporters Without Borders provides the following overview of the media sector:

> *Due to a high rate of illiteracy, radio is the main source of news. The state controls the public media, and state broadcasters RNM and TVM still tend to follow government communication directives. Privately owned radio stations can only broadcast by satellite. The mostly French-language written press remains confined to urban areas. Privately owned media outlets are politicised and polarised between those who support the government and those who support the opposition. This severely limits the availability of objective and independent reporting.*
>
> *The state controls the public media and has the power to appoint or dismiss key officials. The stranglehold of politicians on the media undermines pluralism and journalistic freedom. It is common for media outlets to be controlled directly or indirectly by government ministers, parliamentarians and businessmen with close ties to politicians. The polarisation between pro-government and pro-opposition media is all-pervasive. No media outlet is politically independent.*
>
> *The precariousness of Madagascar's media has had disastrous consequences on their independence and the quality of their reporting. The level of media concentration creates dominant positions and both the current president and communication minister head a media group. […] Very low salaries leave journalists vulnerable to corruption, including the widespread practice of "felaka" (an envelope with a few banknotes given by the organisers of the event to journalists covering it). It is not uncommon for journalists to take on odd jobs and to find themselves in a conflict of interest as a result of working for politicians. Journalists tend to censor themselves mainly to comply with the editorial line imposed by the politician who owns the media outlet they work for, or to comply with a ban on criticising advertisers.*[797]

The US State Department's 2002 Report on Human Rights Practices also notes the tendency towards self-censorship, and the influence of the business and political interests of the owners of media outlets. It observes that organizers of official events

[795] Law No. 2014-038 relating to protection of personal data (Malagasy Data Protection Law). A summary of the law in English can be found here.
[796] "Republic of Madagascar", IMF Country Report No. 23/117, March 2023, paragraph 35.
[797] "2023 World Press Freedom Index: Madagascar", Reporters Without Borders.

often invited only state-owned or pro-government media outlets to attend, and that state broadcasters allegedly received unwritten orders from the minister of communication regarding the content that may be aired.[798]

The African Media Barometer 2021 states that although Madagascar has ratified and domesticated most of the regional and international instruments on freedom of expression and press freedom, it does not necessarily enforce them.[799]

The key legal framework for the communications sector is contained in **Law no. 2016-029: Code of Media Communication**, adopted in 2016 and amended in 2020 by **Law no. 2020-006**.[800] The 2020 amendments were intended to be a response to some of the criticisms of media practitioners.

Several aspects of both the original 2016 law and the 2020 amendments were declared unconstitutional by the High Constitutional Court.[801] In terms of the Constitution, all laws must be submitted by the President to the High Constitutional Court, which decides on their conformity with the Constitution. A provision judged to be unconstitutional may not be brought into force.[802] The Court's opinion on the original 2016 law is discussed in some detail in the section on the Constitution below, because its discussion in that case defined the parameters of constitutional the right to freedom of expression in general terms. Its opinion on the 2020 amendments was less detailed since it made reference to the 2016 opinion on many issues. (Note that some of the findings of the Court in both of these judgements concern matters of detail that are not relevant to this discussion and are therefore not discussed here.)

This law covers communications that take place through written, audiovisual or electronic media, as well as speeches in public places and posters or announcements displayed to the public. This includes radio and television broadcasting, cinema, telecommunications and social media.[803] However, the High Constitutional Court found that the definition of "online press and digital communication" needed clarification because the law should not combine "online press", which refers to articles published by journalists, with "digital communication" which could encompass communications by ordinary citizens in many different forms for many different purposes. It directed a change of wording that would essentially separate professional and non-professional activities.[804]

---

[798] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A. Similarly, BTI states: "In practice, the media are free to publish a variety of opinions, but the government does not hesitate to call them to order if it considers them to have overstepped their role. This means they are often subject to interference or government restrictions, and some journalists consequently practice self-censorship." "Madagascar Country Report 2022", BTI Transformation Index, Bertelsmann Stiftung, 2022.

[799] "African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.

[800] Loi n°2016-029 du 14 juillet 2016: Code de la Communication Médiatisée, often referred to simply as the "Communications Code". It was amended by Loi n°2020-006: portant modification de certaines dispositions de la Loi n° 2016-029 du 24 août 2016 portant Code de la Communication Médiatisée. The 2020 amendments also changed the date of the original law in its title. Loi n°2020-006, Article 1 on the amendment of the law's title: L'intitulé de la Loi n°2016-029 du 14 juillet 2016 sus visée est modifié comme suit : «**Loi n°2016-029 du 24 août 2016** portant Code de la communication Médiatisée».

[801] *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, 12 August 2016; Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant", 31 August 2020.

[802] Madagascar's 2010 Constitution, Article 117.

[803] Loi n°2016-029, Article 1 (see definitions of "media communications", "audiovisual communications" and "communications") and Article 2.

[804] Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant", paragraphs 13-14.

The law **reiterates the constitutional rights to freedom of expression and information**,[805] with the provisions on these basic principles having been generally strengthened in respect of their application to the press by the 2020 amendments:

> ***ARTICLE 5 NEW:*** *The right to freedom of expression is a universal, inviolable and unalterable right, guaranteed by article 11 of the Constitution which is exercised in accordance with the provisions of the International Covenant of Civil and Political Rights, other conventions relating thereto, adopted by the State. It is the right to seek, receive and freely communicate information and opinions regardless of the media used.*
>
> *It focuses on political discourse, commentary on public affairs, electoral propaganda, debate on human rights, journalism, cultural and artistic expression, teaching and religious discourse. It deals with commercial advertising.*
>
> *The press has the mandate, in complete freedom and independence of mind, to express all opinions and report all events or facts likely to interest the public and contribute to its education, subject to the provisions of Articles 15 to 31 of this law [on the media-related offences].*
>
> *No one may limit the freedom of exchange of information which could hinder access to information or infringe the right of citizens to free, pluralistic and transparent information.*
>
> ***ARTICLE 7 NEW:*** *No journalist may be impeded, denied access to sources of information, or harassed in any way whatsoever in the regular exercise of his mission as a journalist.*
> *The journalist has the right of access to all sources of information, including data and statistics. The journalist has the right to obtain information without hindrance on all facts of public interest.*
> *The conditions, methods and procedures relating to access to the administrative documents of public bodies will be defined by regulation.*
>
> *However, the publication of in camera debates, reports or any other document kept or drawn up within the Institutions of the Republic is prohibited.*[806]

One problematic feature here is the prohibition on publication of government documents in the new Article 7.[807] The High Constitutional Court found that this provision violated the right to information in the Constitution as well as Madagascar's international commitments and held that it must be removed.[808]

Another issue identified by the High Constitutional Court as being unacceptable was the reference to subjecting the right of access to information on conditions and procedures established by *regulation*; it held that the Constitution requires that limits on any of the fundamental rights must be expressly set by law and not contained in a

[805] Loi n°2016-029, Articles 5-8.
[806] Loi n°2016-029, Article 5 new and Article 7 new.
[807] In French: "Toutefois, est interdite la publication des débats à huis clos, des rapports ou tout autre document tenus ou établis au sein des Institutions de la République."
[808] *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraph 12.

regulatory act, holding that the phrase "by regulation" must be replaced with the phrase "by legislative means".[809]

The law also establishes the regulatory body, the **National Authority for the Regulation of Media Communication or ANRCM** ("Autorité Nationale de Régulation de la Communication Médiatisée").[810] After the 2020 amendments, ANRCM has 13 members, with more specificity of membership than in the original law, to ensure a wider diversity of representation:

- one representative of the Ministry in charge of Communication;
- one representative of the Ministry in charge of Culture;
- one representative of the Ministry in charge of Telecommunications;
- one representative of the Order of Journalists of Madagascar;
- one magistrate elected by the Superior Council of the Judiciary;
- one representative of national television;
- one representative of the national radio;
- one representative of private radio stations;
- one representative of private television stations;
- one representative of the written press;
- one representative of a civil society platform working in the field of human rights;
- one representative of an online press organ recognized by the Order of Journalists of Madagascar;
- one representative of the advertising sector.[811]

The law does not say exactly how these members will be appointed, but provides that the organization and functioning of ANRCM will be set out in a decree issued by the Council of Ministers.[812] ANRCM'S functions including regulating media activities and arbitrating disputes that arise from media such activities, including the handing of complaints from members of the public.[813] Initially, the ministry responsible for communications was still responsible for granting and withdrawing operating licences,[814] but this responsibility was passed to ANRCM as a result of the 2020 amendments.[815] The 2020 changes removed the word "independent" from the description of ANRCM, but this was found to be unacceptable by the High Constitutional Court, which reiterated its finding about the original 2016 law, where it stated that ANRCM must be able to take measures "in complete freedom and sheltered from all instructions and pressure", and receive "neither orders nor instructions from the government", as well as being independent of both political power and the power of players in the media communications sector.[816]

[809] Id, paragraph 11.
[810] Id, Article 51.
[811] Loi n°2020-006, Article 52 new.
[812] Id, Articles 53 new.
[813] Id, Articles 51*bis* new.
[814] Loi n°2016-029, Article 49, prior to the 2020 amendments.
[815] Loi n°2020-006, Article 51*bis* new.
[816] *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraph 15, referring to *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraph 53.

However, as of May 2023, ANRCM had reportedly not yet been established, due to the fact that the Decree governing its operation has not yet been issued. Its functions are being carried out by the ministries of communication and culture. The leader of the opposition party Malagasy Miara Miainga (MMM) has called for this issue to be addressed as the country heads towards the 2023 elections.[817]

Private radio and television broadcasters must be licenced - including those that broadcast on the internet.[818] **Public broadcasters** are subject to a few duties set out in the law. The Madagascar Radio and Television Office (ORTM) is the state broadcaster. It includes TVM (the national television channel) and RNM (the national radio). ORTM is not independent, being administered by a Board composed entirely of public officials.[819] **Film production and dissemination** both require prior authorisation from the relevant ministries.[820] **Print media outlets** do not require licensing or prior authorisation, but must provide a declaration to the Public Prosecutor that includes identifying details of the publication director (including information on his or her criminal record) and the printer.[821] The same applies to **online press** that is produced on a professional basis.[822]

The professional online press must also employ at least one professional journalist legally registered on the roll of the Order of Journalists (explained below), and provide ANCRM and the ministry responsible for communication with the digital identifier of the site or online medium as well as of its administrator. Online press organs must also maintain a digital archive for a minimum of three months, of which the ministry in charge of communication is "an executor by right". On the personal contribution spaces of Internet users (ie the space for comments on published articles), the publisher must implement appropriate measures to fight against illegal content, including a mechanism that allows anyone to report the presence of such content, upon which the publisher must remove them promptly or make access impossible. The online press also has a duty (amongst others) to ensure that the content they publish "must not be likely to shock the Internet user by a representation of the human person undermining his dignity and decency or presenting violence in a favourable light"[823] More broadly, **Internet access providers and any other online service providers** have a duty to verify the content of the sites they host and to notify ANCRM of any illegal

[817] Frederic Ange Toure, "In Madagascar, criticizing the president can be expensive", *Le Journal de Afrique*, 31 March 2023; "Liberté de presse: la mise en place de l'ANRCM sollicitée", *Newsmada*, 5 mai 2023.
[818] Loi n°2016-029, Article 121, as amended by Loi n°2020-006.
[819] Loi n°2016-029, Articles 157-168; "African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 37. The Board is established by a ministerial order.
[820] Loi n°2020-006, Article 194 new; Loi n°2016-029, Article 198.
[821] Loi n°2020-006, Article 100 new. Identifying information must also appear on every press publication. Loi n°2016-029, Article 102.
[822] Loi n°2020-006, Article 174*bis* new; Loi n°2016-029, Article 175 as amended by Loi n°2020-006.
[823] Loi n°2020-006, Article 74*bis* new. This article defines "online press" as "any communication service to the public on digital media published on a professional basis by a natural or legal person who has editorial control of its content, consisting of the production and making available to the public of 'original content, of general interest, regularly renewed, composed of information presenting a link with current events and having been the subject of treatment of a journalistic nature, which does not constitute a promotional tool or an accessory of an industrial or commercial activity".

activity or content that they discover. They must also collect information on the identity and contact details of customers and website owners.[824]

The Code on Media Communication does not appear to restrict the exercise of journalism, but it establishes a category of professional journalists who must meet certain requirements to obtain a professional identity card issued by a Commission within the **Order of Journalists of Madagascar (OJM**). The OJM is a body of journalists with a statutory duty to regulate the profession and "act as a guardian of the rules of ethics and professional conduct of the profession". However, it cannot be described as a purely self-regulatory body; the law requires that the Commission which issues professional credentials to journalists must be composed of an equal number of government officials, journalists and representatives of employers' organizations in the media sector. The law also states that the organization and functions of the OJM will be set by regulation.[825]

A "**professional journalist**" is a person "whose main and regular occupation is to seek facts from sources and communicate them by appropriate means to the public", and who earns most of his or her income from this occupation. This category includes reporter photographers, reporter cameramen, reporter sound recordists and editors amongst others. To receive a professional identity card from the Order of Journalists, a person must hold a diploma or other qualification from a recognised journalism training institution and must have worked as a professional journalist for at least three years.[826]

The 2020 amendments sought to give the OJM "a right of control" over all the activities of professional journalists who hold professional cards;[827] however the High Constitutional Court found that this was too broad, since the right to freedom of expression can be restricted only by law and only on limited grounds and any form of censorship is prohibited. Thus, this "right of control" must be qualified. [828]

The law lists the **duties and obligations of a journalist**:

The duties of the journalist:

- Respect the facts, whatever the consequences for themselves, because of the public's right to know the truth;
- Only publish information whose origin, veracity and accuracy are established. Otherwise, accompany them with the necessary reservations;
- Not to delete essential information and not to alter words, texts and documents;

[824] Loi n°2016-029, Article 176: "Le fournisseur d'accès internet et tout autre prestataire de service en ligne a le devoir de vérifier le contenu des sites qu'il héberge. Il notifie l'Autorité Nationale de Régulation des Communications Médiatisées de toute activité ou contenu illicite dont il a connaissance. A défaut de notification immédiate, il est sanctionné par une peine d'amende de 1.000.000 à 3.000.000 Ariary. Les clients d'un hébergeur ou les propriétaires de site web doivent lui fournir leur identité réelle et leurs coordonnées exactes."
[825] Loi n°2016-029, Article 53; Loi n°2020-006, Articles 54*bis* new, 54b new, 54c new, 55 new.
[826] Loi n°2020-006, Article 54 new, read with Loi n°2016-029, Article 1 (definition 30).
[827] Loi n°2020-006, Article 56*bis* new.
[828] *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraphs 18-21.

- Defend, in all places and all circumstances, the freedom to inform, comment and criticize, taking scruples and concern for justice as the first rule in the honest publication of his information;
- Not to use unfair methods to obtain information, photographs or documents, nor to confuse its role with that of a police officer;
- Never confuse the profession of journalist with that of an advertiser or propagandist;
- Do not accept any direct or indirect instructions from advertisers, or administrative or political authorities.
- Refuse any benefit in cash or in kind, regardless of the value and the provenance, for services rendered or expected;
- Refuse any pressure and only accept editorial directives from those in charge of the editorial staff. Assume full responsibility for all writings.
- Never reveal the circumstances in which the journalist became aware of the facts he is reporting, for the protection of the source of the information collected;
- Refrain from any violation of social ethics: incitement to tribalism, xenophobia, revolt, crimes and offences; contempt of good morals, apology for crimes, war crimes and crimes against humanity;
- Respect people's privacy. The human right to protection of reputation and integrity must be respected. Avoid posting information that violates privacy;
- Rectify any published information that proves to be inaccurate;
- Recognize only the jurisdiction of his sovereign peers in matters of professional honour.

The obligations of the journalist:

- The journalist verifies the accuracy of his information;
- He keeps sound or visual recordings, in particular to provide proof of what is reported;
- The journalist distinguishes between facts and comments;
- The journalist, in the collection, processing and dissemination of information must act with the maximum possible objectivity;
- The journalist must, in all circumstances, and whatever his own personal convictions, act in his soul and conscience, with honesty;
- The journalist must keep his editorial independence and resist political, social or financial pressures likely to influence his rigor in the treatment of information. He does not accept directives other than those responsible for his editorial staff, his morals or his personal ethics when working alone.
- The journalist informs people who are unfamiliar with the press that their remarks may be broadcast and therefore brought to the attention of a large public;
- The journalist refrains from any plagiarism and quotes the colleagues from whom he takes the information;
- The journalist signs the photos illustrating his article or clearly refers to their source.[829]

[829] Loi n°2016-029, Article 58.

Violation of any of these duties and obligations is grounds for disciplinary action by the OJM.

There are also **other breaches that may warrant disciplinary action**:

- Harmful imputations, personal attacks or insinuations malicious towards a citizen, a group of citizens, an association or a professional body;
- Insulting or outrageous words towards a citizen, a group of citizens, an association or a professional body;
- Defamation which damages the honour of a person;
- The call to disturb public order;
- Publications contrary to modesty and good morals;
- Dissemination of obscene, licentious or pornographic images, photographs, publications or illustrations;
- The publication of false information;
- Unauthorized publications compromising the general interest;
- Failure to sign publications or the use of false names;
- Non-compliance with specified requirements;
- Violations of ethics and fair access to public service media;
- Invasion of the privacy of any citizen.[830]

Possible sanctions following a disciplinary action include warnings, temporary suspension or delisting, notwithstanding the application of the other penalties provided for in the law.[831]

It should also be noted that there are detailed requirements and procedures for a **right of reply and rectification** when a media communication directly damages a person's honour or reputation or reports inaccurately.[832]

The law provides **a degree of protection for journalists' sources**. Both journalists and editorial staff have the right to withhold the identity of their informants as well as any information, recordings and documents that might make it possible to identify the informants. However, the identity of a source can be demanded by a judicial authority if three conditions are all met:

- it is likely to prevent the commission of a serious offence constituting a serious threat to the physical integrity of one or more persons; and
- the information requested is of crucial importance to prevent the commission of these offences; and
- the information requested cannot be obtained in any other manner.[833]

[830] Id, Article 59. The final point on privacy is also discussed in Article 60, which says: "Every journalist claims free access to all sources of information and the right to investigate freely on all the facts which condition public life. The secret of public or private affairs may, in this case, be revealed to the journalist only by way of exception and by virtue of clearly expressed reasons."
[831] Id, Article 59.
[832] Id, Articles 70-ff.
[833] Id, Articles 9-12.

Another potentially helpful provision, at least in theory, states "Any aggression committed by any natural or legal person, by the public authorities, by the police against journalists or a reporting team or a radio and television station that is detrimental to their **working materials and equipment**, is liable to prosecution and sanctions in accordance with the provisions of the Penal Code." This provision also prohibits the alteration and destruction of any data contained in these items.[834]

One controversial aspect of the Code on Media Communications concerns its **offences**. According to the Explanatory Memorandum that accompanies the Code, it was aimed at "decriminalization", not in the sense of removing offences, but rather through the replacement of custodial sentences with fines – although other offences will continue to be governed by the common law, the Penal Code or other specific legal provisions.[835] The Law in some instances cross-references offences in the Penal Code and provides detail about how they are to be applied in respect of communications media.[836] Criminal offences relevant to freedom of expression are discussed below in section 9.4 in combination with specific cybercrime offences.

The original 2016 legislation was strongly criticized by journalists and international media organizations. In fact, before it was passed by National Assembly, 45 media outlets aired special information programs in a continuous loop to raise public awareness of its potentially harmful effects. Key complaints were the vagueness of some provisions and the excessive fines for some offences aimed at journalists.[837] The 2020 amendments, even though they aimed to respond to the demands of media practitioners, were also not viewed as being sufficient to correct the deficiencies, with some fines having increased as imprisonment was removed.[838]

In terms of **Law no. 2005-023** on institutional reform of the telecommunications sector, the **Regulatory Authority of Communication Technologies (ARTEC)** regulates **telecommunications networks** and ensures compliance with regulations in the telecommunications sector. Its Board of Directors is established by a Decree of the Council of Ministers. [839]

9.2 CONSTITUTION

In **Article 10 of the Constitution** (quoted on the first page of this chapter), the grounds for limiting freedom of expression, communication and the press are broadly worded: "respect for the freedoms and rights of others" and "safeguarding the public order, the national dignity and the security of the State". There is no mention of necessity or proportionality, nor any requirement that limitations may be imposed only by law –

[834] Id, Article 69.
[835] Id, Explanatory Memorandum on the first page of the law.
[836] Id, Articles 15, 18, 26-27 and 33, for example.
[837] "Madagascar: Controversial Mass Media Code Approved", Library of Congress, 9 September 2016 (references omitted).
[838] African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.
[839] Loi n°2005-023: portant refonte de la loi n°96-034 du 27 janvier 1997 portant Réforme institutionnelle du secteur des Télécommunications (revising law no. 96-034 of January 27, 1997 on institutional reform of the telecommunications sector). ARTEC replaced the Malagasy Office for the Study and Regulation of Telecommunications (OMERT) as of 1 April 2015. "Madagascar Telecommunications", Logistics Cluster, 2022.

although Article 7 does state that the exercise of the individual rights and fundamental freedoms guaranteed by the Constitution is organized by the law.[840]

In its 2016 **decision on the constitutionality of the Communications Code**, the High Constitutional Court of Madagascar provided some general observations about the import of Article 10. It stated that "freedom of expression and communication represents an important constitutional achievement, all the more precious since its exercise is a condition of democracy and constitutes one of the essential guarantees of respect for other rights and freedoms as well as national sovereignty", as well as contributing to respect for the rule of law. The Court also stated that Article 10 encompasses the right to information and the reception of information, and appears in many respects, "to be one of the most important foundations of a democratic society". [841] Moreover, the Court stated that, given the widespread use of online communication services, and the resulting importance that such communications have in democratic life and the expression of idea and opinions, the freedom of expression and communication guaranteed by Article 10 of the Constitution "implies freedom of access to the internet".[842]

The Court also stated that the limitations clause in Article 10 "emphasizes that these freedoms are neither general nor absolute and must be reconciled with other constitutional requirements"[843] – but noted that any interference with their exercise must be necessary, appropriate and proportionate to an objective of general interest. Limitations on these rights must also be imposed by a law with general applicability and must correspond to measures that are necessary in a democratic society and justified by an imperative social need. [844] Furthermore, considering that freedom of information must be balanced against the notion of public order, democratic standards require that "the notion of public order must be interpreted restrictively".[845] Also, when offences implicate freedom of expression, the "sanctions should never be so severe as to hinder the exercise of the right to freedom of expression" or to deter others from exercising this right.[846]

Against this background, the Court analysed several provisions of the Communications Code against the Constitution and, subject to some conditions, upheld all but a portion of Article 6:[847]

---

[840] Constitution de la Quatrieme Republique: "Article 7.- Les droits individuels et les libertés fondamentales sont garantis par la Constitution et leur exercice est organisé par la loi."
[841] *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraph 15.
[842] Id, paragraph 14.
[843] Id, paragraph16.
[844] Id, paragraphs 20-21.
[845] Id, paragraph 30.
[846] Id, paragraph 60.
[847] The Court explicitly confirmed the constitutionality of the first paragraph of Article 6, provided that public order is interpreted narrowly. It also withheld several other articles, subject to some conditions, including the last paragraph of Article 7 (regarding the limitation of right of access to information by means of conditions, terms and procedures defined by a specific text. provided that these are set by law.), the first paragraph of Article 20 (invasion of privacy) and its reiteration in Article 59, Article 30 (false news), Article 44 (the Ministry's power to permanently close a media company or suspend a journalist for repeated violation of the Code,on the condition that this power is exercised constitutionally), Article 51 (on guarantees for the independence of ANRCM), Article 85 (requiring that a publication director must be the owner or majority shareholder or legal representative of the media entity), Article 157 (on the obligations of public service

> ***ARTICLE 6.-*** *Information in all its forms is not subject to any prior constraint, except where it would undermine public order and good morals.*
>
> *Freedom of information, whatever the medium, is a right. The exercise of this right entails duties and responsibilities and is subject to certain formalities, conditions, or penalties provided for by the laws and regulations in force, which constitute necessary measures in a democratic society.*[848]

With respect to the second paragraph of Article 6, the Court found that the phrase "formalities, conditions and penalties for exercising the right to freedom of information" should be clarified and that specific legislative and regulatory texts should be listed. It held that greater precision was necessary to satisfy the constitutional value of the accessibility and intelligibility of the law, and to protect against applications that could be contrary to the Constitution.[849]

The constitutional right to freedom of expression and its limitations have thus been interpreted in a manner that is consistent with international treaties on this topic, but this understanding is not always applied in practice. According to Freedom House, although the Constitution provides for freedom of the press, this guarantee "has been undermined by criminal libel laws and other restrictions, as well as safety risks involved in the investigation of sensitive subjects such as cattle rustling and the illicit extraction and sale of natural resources".[850]

9.3 CASE STUDIES

According to Reporters without Borders: "Journalists are sometimes publicly verbally attacked by politicians or are victims of smear campaigns on social media. Physical attacks are very rare. Sometimes it is the journalists who have been won over to the government's cause who launch verbal attacks on their colleagues who do not share the same political opinion."[851]

In March 2023, the offices of a publication critical of the President, *La Gazette de la Grande Île*, were **raided.** Fernando Cello, who has had his own run-ins with

radio and television, subject to the condition of political neutrality and the obligation to provide a diversity of views), the differentiated penalties for different offences under the Code and several provisions restricting the broadcast of advertisements for private non-commercial radio and television advertisements in the public interest.

[848] "**Article 6.-** L'information sous toutes ses formes n'est soumise à aucune contrainte préalable, sauf celle portant atteinte à l'ordre public et aux bonnes moeurs.

La liberté d'information, quel qu'en soit le support, est un droit. L'exercice de ce droit comporte des devoirs et des responsabilités et est soumis à certaines formalités, conditions, ou sanctions prévues par les textes législatifs et règlementaires en vigueur, lesquelles constituent des mesures nécessaires dans une société démocratique."

[849] *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraphs 24-28.

[850] "Freedom in the World 2023: Madagascar", Freedom House, section D1.

[851] "2023 World Press Freedom: Madagascar", Reporters Without Borders, "Safety".

government authorities and is now the vice-president of the Federation of Journalists' Associations of Madagascar, identifies this media outlet – reportedly the only one not affiliated with a political party – as also being the only one that denounces injustice and dares to criticize the President and the government. Cello is convinced that the State is behind the intrusion. The owner of the magazine, Lôla Rasoamaharo, was arrested shortly before the raid for charges related to **attempted extortion**, **defamation**, **threats** and **insults** as well as facing a complaint of being in **arrears with water and electricity payments**, in what some view as "judicial harassment".[852]

In February 2022, a prominent opposition figure Mahery Lanto Manandafy was arrested on charges of **"spreading false information"** and **"insulting an institution**" in connection with a Facebook post alleging that the construction of a bridge was structurally flawed. He was given a six-month suspended prison sentence. In September 2022, he was arrested again on similar charges combined with a charge of **defamation**, after a post on his Facebook page denouncing a foreign national for providing ammunition to cattle rustlers in collaboration with a member of the President's staff. He was placed in pre-trial detention and was reportedly still being held in custody at the end of 2022.[853] Press reports indicate that he was summoned by the police cybercrime unit in connection with these charges, so they were likely brought under Article 20 of the cybercrime law which criminalises insult or defamation of government institutions.[854]

In March 2022, police arrested teacher Jeannot Randriamanana for defamation after he posted information on Facebook about irregularities in the distribution of food supplies after cyclone disasters in his region. He was sentenced to two years in prison for **defamation** and the **humiliation of Members of Parliament and civil servants**. His appeal against the conviction was unsuccessful, but his prison sentence was suspended, and he was released.[855] Reports of this incident did not cite the statutory instrument that was the basis for the charge, but it sounds likely that it was Article 20 of the cybercrime law which criminalises insult or defamation of members of Parliament.[856]

In May 2022, the local newspaper *La Gazette* reported that a Member of Parliament made a **death threat** against one of its journalists in connection with a specific article alleging that he had attempted to use his influence to expropriate land. *La Gazette* stated that this was the second time that this MP had threatened one of their journalists and reported that family members of its journalists had also received threats.[857]

Also in May 2022, the police cybercrime unit summoned opposition municipal counsellors Lily Rafaralahy and Clemence Raharinirina for investigation, acting on a complaint of **defamation** after they stated that the mayor was a stakeholder in a

[852] Frederic Ange Toure, "In Madagascar, criticizing the president can be expensive", *Le Journal de Afrique*, 31 March 2023.
[853] "Freedom in the World 2023: Madagascar", Freedom House, section B1; "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
[854] Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
[855] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
[856] Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
[857] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.

company that would soon manage the capital city's parking lots. They were convicted and ordered to pay a fine.[858] This also probably involved **Article 20 of the cybercrime law**, which covers **insult and defamation of various government authorities and institutions**.[859]

In July 2022, Mendrika Razafimahefa was arrested by presidential guards for making a "thumbs down" sign as the presidential motorcade drove by. He was released after several days in custody, and eventually given a one-month suspended prison sentence for a **traffic violation,** based on allegations that he had refused to give way to the motorcade as well as making the negative gesture.[860]

In July 2022, two opposition leaders, Rina Randriamasinoro and Jean-Claude Rakotonirina, were arrested on charges of "**inciting hatred and public unrest**" during a protest by hundreds of people against rising living costs and deteriorating economic conditions in the capital city of Antananarivo. Most of the organisers of the protest were affiliated with opposition parties. [861]

In August 2022, a Malagasy citizen who worked as a driver at the country's UNESCO office in Paris after he published a photograph on social media suggesting that the President received special privileges allowing him to check an overweight bag on the airline. The driver was repatriated to Madagascar after the incident and arrested on charges of **infringement of the life and security of the President and his family,** the **disclosure of confidential information considered to be a state secret**, **offence to the fulfilment of a state mission** and **defamation**.[862]

In February 2021, the president of the National Assembly 'reminded' opposition members of Parliament that, since parliamentary immunity did not apply to statements made by Members of Parliament in public or through the media, they could be sued for such statements. She indicated that this message was in response to the complaints from ministries, politicians, and ordinary citizens regarding the actions of some Members of Parliament.[863]

Also in February 2021, in the town of Ankilimanilike, two journalists from a local private radio station were **detained by community leaders, with the support of the local authorities**. The community falsely accused the journalists of spreading false news reports concerning the disappearance of children in the area. The journalists were **forced to pay a ransom to secure their release** after three days of detention, with their release being secured with the help of advocacy by members of the regional journalists' association.[864]

---

[858] Id.
[859] Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
[860] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
[861] "Madagascar bans public protests ahead of presidential election", *Aljazeera,* 3 April 2023; "Freedom in the World 2023: Madagascar", Freedom House, section B1.
[862] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
[863] Id.
[864] Id.

In May 2021, the union of journalists reported that security forces **forced journalists** from the *Tia Tanindrazana* newspaper and the MBS TV channel **to delete images on their cameras that could discredit the government**.[865]

In June 2021, the police cybercrime division summoned Ravo Nambinina Rasoamanana, for a hearing on charges of **spreading false news** and **defamation** in connection with a Facebook page about anomalies in the management of public funds within the Ministry of Public Health. where he was previously employed. The charge appears to have been based on **Article 92 of the Penal Code**.[866]

Another 2021 incident involved France 24 correspondent and Pulitzer Prize-winning Malagasy journalist Gaelle Borgia. She was "the target of a **smear campaign** by high-ranking politicians and government officials on social media after she filmed and published a documentary showing persons in the southern region of the country cooking and eating cowhides from scraps of shoes due to local famine conditions". The governor of the region issued a statement accusing Borgia of spreading **false news**. The state-owned television channel TVM later published interviews with persons who said that the journalist bribed them into being filmed eating shoes – but then Norgia aired a video a few days later in which the same individuals reported that they had been coerced through threats of violence to speak against Borgia.[867]

In April 2020, the publishing director of the newspaper *Ny Valosoa Vaovao*, Arphine Helisoa, was arrested in April 2020 for **disseminating false news** and **inciting hatred of the President**, in violation of **Article 91 of the Penal Code** after the newspaper published a report critical of the government's response to Covid-19.[868]

The 2019 "Helicopter Case" involved the publication of photographs of a helicopter flying over the Mahamasina Municipal Stadium. Following a complaint filed by the Malagasy Army, the journalists who published the photo were charged under **Article 20 of the cybercrime law**, which makes it an offence to **insult or defame the armed forces**. They were convicted and fined.[869]

One case with many components involved investigative journalist Fernand Cello of *Radio Jupiter*. In August 2016, the local power company turned off *Radio Jupiter*'s power supply after Cello, whose real name is Avimana Fernand, accused it on the air of colluding with Ilakaka's mayor to cheat consumers. The power company justified this move on the grounds of *"defamation of the electricity supply company"* and *"disrespect and contempt towards the authorities."* In December 2016, Cello exposed the existence of an illegal sapphire mine in Ilakaka run by Gondwana, a mining company owned by government allies. The army raided *Radio Jupiter* and confiscated its transmitter after that story aired, and Cello went into hiding for several

[865] Id.
[866] Id. "A court notice published in September [2021] indicated that he was accused of acts that may compromise public security, lead to serious political trouble, or incite hatred of the government or infringement of the laws." This describes Article 91 of the Penal Code.
[867] Id.
[868] "LEXOTA Country Analysis: Madagascar", last updated July 2022; "Madagascar journalist Arphine Helisoa jailed on false news, incitement allegation", Committee to Protect Journalists, 22 April 2020.
[869] African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 12 (footnotes omitted); Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.

months after receiving death threats. On 21 April, the ministry of mining ordered Gondwana to suspend operations for contravening the mining code, and Cello came out of hiding. Cello was then arrested and charged with **defamation**, "**spreading false news**", "**inciting hatred**", "**endangering state security**", "**malicious allegations**" and "**verbal death threats**". An additional charge of **stealing a cheque** was filed against him by an executive of the power company that was implicated in the August 2016 story. After four and a half months in provisional detention, Cello was convicted on the cheque-stealing charge and given a suspended sentence of two year's imprisonment along with a stiff fine. He was acquitted on appeal in 2019, but reportedly still faced charges of defamation, malicious allegations and verbal death threats under the Penal Code.[870]

Looking at the role of **social media** in particular, journalists and others have citizens faced police investigation and prosecution for defamation and infringement of public order in response to posting criticism of government performance and public services on social media.[871] And, when it comes to social media, there are accusations that the government has used it to sow biased views and disinformation. The Media Institute of Southern Africa (MISA) reports that, late in 2021, some of the highest authorities in Madagascar were accused of financing troll farms for this purpose.[872]

9.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) LAW NO. 2014-006 ON THE FIGHT AGAINST CYBERCRIME (AS AMENDED)

Madagascar's cybercrime law is **Law no. 2014-006 on the fight against cybercrime**[873] as amended by **Law no 2016-031**.[874] The law defines "cybercrime" as "any illegal act committed by means of a computer system or network or any other physical network connected or in relation to an information system".[875]

It contains three chapters: (1) crimes related to information systems; (2) attacks on individuals through information systems, and (3) responsibilities of operators and service providers. Amongst other things, this law criminalises online defamation and

[870] "Madagascar: municipal authorities short-circuit overly critical radio station", Reporters Without Borders, 9 August 2016; "Madagascar goes after Jupiter", IFEX, 10 May 2017; "Journalist freed after receiving suspended sentence", Reporters Without Borders, 28 September 2017; "Southern Africa: Media freedom muzzled as journalists are targeted for telling the truth", Amnesty International, 3 May 2019. Note that the Amnesty International source states that Cello spent two years in jail, while Reporters Without Borders and IFEX refer to a suspended sentence of two years.

[871] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.

[872] Lizette Feris, "The State of Media and Information Literacy in Southern Africa", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 65, citing "Facebook 'troll farms' play outsized role in Madagascar's politics", France 24, 5 October 2021. A "troll farm" refers to a body that employs people to make deliberately offensive, provocative or false online posts to cause conflict, discredit certain individuals or institutions or manipulate public opinion.

[873] Loi n°2014-006 du 17 juillet 2014: sur la lutte contre la cybercriminalité.

[874] Loi n°2016-031 du 14 juillet 2016 et du 15 juillet 2016: modifiant et complétant certaines dispositions de la loi n°2014-006 du 17 juillet 2014 sur la lutte contre la cybercriminalité. The amending law provides a new section 20 and also provides for regulatory texts to be adopted, as necessary, for the application of the law.

[875] Loi n°2014-006: Article 1.

spreading 'false information". Freedom House reports that these offences have been applied in practice against social media users.[876]

In the tables below, titles have been added for ease of reference. The provisions in the cybercrime law do not have titles.

LAW NO. 2014-006 ON THE FIGHT AGAINST CYBERCRIME (AS AMENDED) - TECHNICAL OFFENCES	
Article 6 read with Article 3: Fraudulent access	It is an offence to access all or part of an information system intentionally, without legitimate excuse or justification, or beyond a legitimate excuse or justification. This offence is punishable only by a fine. The possibility of imprisonment is added for fraudulent access that damages, erases, deteriorates, modifies, alters or deletes computer data contained in the system, or hinders or alters the operation of all or part of the system. o The provision of the possibility of a legitimate excuse is a positive element.
Article 4 read with Article 4: Fraudulent remaining	It is an offence to remain connected to a computer system or a part of an information system of information, or to continue to use an information system, intentionally, without legitimate excuse or a higher justification. This offence is punishable only by a fine. The possibility of imprisonment is added for fraudulent remaining that damages, erases, deteriorates, modifies, alters or deletes computer data contained in the system, or hinders or alters the operation of all or part of the system. o It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorized access.[877]
Article 7: Fraudulent data interference	It is an offence to fraudulently introduce, damage, erase, deteriorate, modify, alter or delete computer data, or to act fraudulently in such a way as to modify or delete a method of data processing or transmission.
Article 8: Fraudulent use of computer data	It is an offence to fraudulently use computer data that is deliberately damaged, erased, deteriorated, modified or altered.
Article 9: Computer-related forgery	It is an offence to fraudulently introduce, alter, erase or delete computer data, to generate non-authentic data, with the intention that the data be taken into account or used for legal purposes as if it were authentic, whether or not the data is directly legible and intelligible.
Article 12 read with Article 11: Breach of integrity of an information system	It is an offence to fraudulently hinder or alter the operation of all or part of an information system. Altering the operation of an information system means any action that distorts the operation of an information system to make it produce a result other than that for which it is normally designed and used.

[876] "Freedom in the World 2023: Madagascar", Freedom House, section D4.
[877] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

	Hindering the operation of an information system means any action having the effect, object or purpose of paralyzing an information system by the introduction, transmission, damage, deletion, modification, alteration or deletion of computer data.
Article 13: Fraudulent data interception	It is an offence to fraudulently intercept computer data by technical means, during non-public transmissions, to, from or within an information system. This includes the interception of electromagnetic emissions from an information system that are transporting such computer data.
Article 14: Fraudulent devices	It is an offence to fraudulently produce, import, hold, offer, transfer, distribute or make available - • equipment or a device, including a computer program or any data, that is designed or adapted mainly to enable the commission of one or more of the offences provided for in Articles 3, 4, 7, 8, 11 and 12; • a password, an access code or similar computer data allowing access to all or part of an information system to commit one or more of the offences provided for in Articles 3, 4, 7, 8, 11 and 12. This offence is punishable by the same penalties as the offence for which it was used or intended to enable. It is not an offence where the prohibited acts were *not* carried out for the purposes of the offences referred to, such as in the case of authorized testing, research or protection of an information system. o The required intention helps to narrow the offence appropriately.
Article 15: Computer-related fraud	It is an offence to cause a loss of property to another person, with the intention of obtaining a benefit without right, by - • entering, altering, erasing or deleting computer data; • any form of interference with the operation of an information system. o The required intention helps to narrow the offence appropriately.

Conspiracy and **aiding or abetting** the crimes set out in Articles 3, 4, 7, 8 and 11 are also criminalised.[878]

Looking at **penalties**, access that does not cause any damage to data is punishable only by a fine. All of the other technical offences are punishable by imprisonment and a fine, *or by one of these penalties only*. In other words, imprisonment is not an inevitable consequence of conviction on any of the technical offences. In contrast, most of the content-based offences are punishable by a minimum term of imprisonment *and* a fine.

[878] Loi n°2014-006, Article 10.

LAW NO. 2014-006 ON THE FIGHT AGAINST CYBERCRIME (AS AMENDED) - CONTENT-BASED OFFENCES	
Articles 16-18: Threats for purposes of extortion	It is an offence to use a computer or electronic medium to transmit a threat of assassination, poisoning or any other attack against persons that would constitute a serious crime for the purpose of ordering the person in question to deposit a sum of money in a specified place or to fulfil any other condition. This applies to any crime that is punishable by death, life imprisonment with hard labour, or deportation. If the threat is made by means of anonymous or signed writing, image, symbol or emblem, the minimum penalty is two years' imprisonment and a fine (Article 16). If the threat is made verbally ("*verbale*"), the minimum penalty is six months' imprisonment and a fine (Article 17). If the threat is made against a person or a group of persons on the grounds of origin, sex, ethnicity, nationality, race or religion, real or supposed, the minimum penalty is two years' imprisonment and a fine, regardless of the form the threat took (Article 18). In any of these cases, the culprit may be deported ("*l'interdiction de séjour*") (Article 18). o The prohibited grounds set out here for the imposition of enhanced penalties do *not* include disability, even though disability *is* part of the similar list under Article 20. o This offence overlaps to some extent with Articles 305-308 of the Penal Code.[879]
Article 19: Identity offence	It is an offence to knowingly usurp the identity of any natural or legal person on a computer or electronic medium, with a view to disturbing the tranquillity of the person being impersonated or someone else, or to undermine the honour of the person being impersonated or that person's reputation with others. The minimum penalty is six months' imprisonment and a fine. o Impersonation on its own, without the required intention, is not an offence.
Article 20: as replaced in 2016:[880] Insult or defamation	Insult or defamation is an offence. Where this offence is committed against constituted bodies, courts, tribunals, armed forces, public administrations, members of the Government, Parliamentarians, public officials, depositaries or agents of public authority, citizens charged with a public service or mandate, assessors or witnesses by reason of their depositions. This applies when the insult or defamation is made by means of – • speeches, cries or threats uttered in public places or meetings

[879] Code Pénal, Mis à jour au 31 mars 2005 (as amended to 31 March 2005). There have been some subsequent amendments on trafficking in persons that do not affect the provisions discussed in this chapter.
[880] Loi n°2016-031, which amended Loi n°2014-006, contains a new Article 20.

	• by writings, printed matter, drawings, engravings, paintings, emblems, images or other conveyance of writing, words or images that are sold, distributed, put for sale or exhibited in public places or meetings; • by placards or posters exposed to public view; or • by means of a computer or electronic medium, The penalty is a fine of 2 million to 100 million Ariary. Where the insult is committed against any individual through a computer or electronic medium, and not preceded by provocation, the penalty is a fine of 100 000 to 10 million Ariary. Where this form of the offence is committed against a person or a group of persons on the grounds of origin, sex, disability, ethnicity, nationality, race or specific religion, the penalty is a fine of 2 million to 100 million Ariary. In the event of a conviction for an insult in either of these two categories, the court may order the display or dissemination of its decision. o Note that many of the means of communication on the list of means of insulting or defaming public figures or bodies do *not* involve cyber communication at all, which is odd in cybercrime law. o The provision on public figures and bodies refers to both "insult and defamation" by a range of means of communication, while the provision on other individuals refers only to "insult" through a computer or electronic medium. o Note that the option of requiring dissemination of the court's conviction does not apply to the insult or defamation of public officials and entities. o The amendment of Article 20 removed prison sentences for the offences of insult or defamation, but the fines that can be imposed in the amended version are stiff. o According to Reporters without Borders, "the law's failure to define what is meant by 'insult' or 'defamation' leaves room for very broad interpretation and major abuses."[881] o This provision overlaps with Articles 23 and 24 of the Code on Media Communications.[882]
Article 21: Genocide and crimes against humanity	It is an offence to use a computer or other electronic medium to disseminate or otherwise make available to the public material that denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law. The minimum penalty is six months' imprisonment and a fine.
Article 22: Child pornography	It is an offence to fix, record, produce, procure or transmit an image or representation of a child which is of a pornographic nature, with a view to its distribution by means of a computer or electronic medium. The minimum offence is two years' imprisonment and a fine. Attempt to do this is punishable by the same penalties. It is also an offence, punishable by the same penalties to offer or disseminate such an image or representation, by means of a computer or electronic medium, or to import or export it.

[881] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A. The original source is not indicated.
[882] Loi n°2014-006, Articles 23 and 24 (discussed below).

	It is also an offence to – • habitually consult an online public communication service that makes such images or representations available; or • possess such an image or representation in any form whatsoever. The minimum offence is two years' imprisonment and a fine. The penalties for child pornography offences are increased when the child involved is under age 15. o "Child pornography" is defined in this section 3 to mean "any representation, by any means whatsoever, of a child engaging in explicit, real or simulated sexual activities or any representation of the sexual organs of a child, primarily for sexual purposes. o "Child" means a person under the age of 18. o "Online public communication service" means "any transmission of digital data not having the character of private correspondence, by an electronic communication process using the Internet network allowing a reciprocal or non-reciprocal exchange of information between the issuer and the receiver". o These offences also apply to pornographic images of a person who appears to be a minor, unless it is established that the person was at least age 18 on the day the image was fixed or recorded. o "Pornographic image" includes – o the image or representation of a minor engaging in sexually explicit behaviour o the image or representation of a person who appears to be a minor engaging in sexually explicit behaviour o the realistic image representing a minor engaging in sexually explicit behaviour, with "realistic image" referring in particular to the altered image of a natural person created in whole or in part by digital methods. o There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose. o This offence overlaps with Article 346 of the Penal Code[883] and Articles 18 and 146 of the Code on Media Communications.[884]
Article 23: Using a computer or other electronic medium in aid of debauchery, corruption or child prostitution to	It is an offence to use a computer or other electronic medium to attack morals, by exciting, favouring or facilitating debauchery, corruption or child prostitution (involving children of either sex) to satisfy the passions of others, punishable by hard labour, in two situations: • when the acts are committed in teaching or educational establishments or in the premises of the administration, or in the vicinity of these establishments or premises during the entrances or exits of pupils or the public or in a time very close to these (punishable by hard labour for a specified period); or

[883] Code Pénal, Mis à jour au 31 mars 2005 (as amended to 31 March 2005), Article 346: It is an offence to fix, record or transmit the image of a minor, with a view to its dissemination, when this image presents a pornographic character. The minimum offence is two years' imprisonment and a fine. The penalties are increased when the child involved is under age 15.
[884] Loi n°2014-006, Article 18: The import, distribution, export, production, publication, exhibition and sale of pornographic materials involving children are punishable by the penalties provided for in Article 346 of the Penal Code. Article 146: All production, filming and distribution of cinematographic work of a child pornography nature or incitement to debauchery in any form of violence are prohibited. Any breach of this provision is liable to the penalties provided for in the various laws in force and the confiscation of the materials used in the commission of the offence.

satisfy the passions of others	• when the acts have been committed in an organized gang (punishable by hard labour for life). **Art.23.-** Quiconque aura attenté aux moeurs, par l'utilisation d'un support informatique ou électronique, en excitant, favorisant ou facilitant, pour satisfaire les passions d'autrui, la débauche, la corruption ou la prostitution enfantine de l'un ou de l'autre sexe, est puni des travaux forcés à temps, dans chacun des deux cas suivants : 1° Lorsque les faits sont commis dans des établissements d'enseignement ou d'éducation ou dans des locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux; 2° Lorsque les faits ont été commis en bande organisée, les coupables seront punis des travaux forcés à perpétuité. o Cybercrime law appears to provide heavier penalties in certain circumstances, where the means of communication used is a computer or other electronic medium. The circumstances articulated seem somewhat unclear but could refer to using such media in the places described to display violence or pornographic material. The lack of clarity could be a problem of translation, so the original text is quoted above. o Even in the original French, broad terms such "*la débauche*" and "*la corruption*" are not defined. Note that "debauchery" may encompass same-sex conduct.[885] o This offence overlaps with Article 346 of the Penal Code. The Penal Code covers messages of a violent or pornographic nature or of a nature to seriously undermine human dignity, in any circumstance where the message is likely to be seen by a minor. The minimum penalty is two years' imprisonment and a fine. The Penal Code offence also provides that where the means used to communicate the message is the written or audiovisual press, the specific provisions of the laws which govern those matters are applicable as regards the determination of the persons responsible. This appears to refer to Article 146 of the Code on Media Communications. [886]
Article 24: Grooming	It is an offence for an adult to use an electronic means of communication to make sexual proposals to a minor or to a person presenting himself as a minor. The minimum penalty is two years' imprisonment and a fine. The minimum period of imprisonment is increased to five years when the proposals were followed by a meeting.
Article 25:	It is an offence to manufacture, transport, disseminate by any means and via any medium, a message of a violent or pornographic nature, of a racist or xenophobic nature, or of a nature that seriously violates human dignity,

[885] See "2021 Country Reports on Human Rights Practices: Madagascar", US State Department, section 6: "The Ministry of Interior ordered the cancellation of an evening event that members of the LGBTQI+ community organized in an Antananarivo bar for July 3 to celebrate Pride Month. The event had taken place in the same location during previous years. Authorities cancelled the event because they claimed it was an incitement to **debauchery** and **offense to morals**."

[886] Loi n°2014-006, Article 146: All production, filming and distribution of cinematographic work of a child pornography nature or incitement to debauchery in any form of violence are prohibited. Any breach of this provision is liable to the penalties provided for in the various laws in force and the confiscation of the materials used in the commission of the offence.

Racist and xenophobic material	or to trade in such a message, *when this message is likely to be seen or perceived by a minor*. The minimum punishment is two years' imprisonment and a fine. Where the offences provided for in Article 346 of the Penal Code or in this Article are committed by means of communication to the general public online, the specific provisions of the laws which govern these matters are applicable. o The prohibited materials are not defined in this law and are worded in a very broad fashion. o It is not clear how a person would ascertain if the message "is likely to be seen or perceived by a minor".

B) LAW NO. 2014-006 ON THE CODE ON MEDIA COMMUNICATIONS (AS AMENDED)

The content-based cybercrime offences need to be read together with the offences in the Code on Media Communications.[887]

CODE ON MEDIA COMMUNICATIONS – KEY CONTENT-BASED OFFENCES	
Article 19: Prohibited publication	The unauthorized publication of debates *in camera*, reports or any other document held by or drawn up within the institutions of government that could **compromise public order or national security** is prohibited. Whether or not material falls within this category is to be assessment by the courts. The penalty is a fine.
Article 20: as replaced in 2020,[888] read with Articles 21-22: Right to image and invasion of privacy	The "right to image" is the right for any person to oppose both the capture of his image and his property and the dissemination thereof, without his prior and express consent. The **right to image and private life** relates to the protection against any attack on the right to the name, the image, the voice, privacy, honour, reputation, state of health, sentimental life, reputation, religious practice, family relationships, and everything that relates to a person's intimate and personal sphere. There are exceptions: • The image and/or private life of a person and their property may be captured and disseminated, without their prior and express consent where the person in question is linked to a historical event or a current event, under the principle of citizens' right to legitimate information subject to respect for the dignity of the human person and the respect due to the deceased; • There is no breach of privacy when the acts were carried out in full view of the interested parties without their opposing them when they had an opportunity to do so. • Although a journalist must refrain from infringing on the privacy of individuals, even when these individuals assume political functions or

[887] Id, as amended by Loi n°2020-006.
[888] Loi n°2020-006, Article 20 new.

	roles, the journalist can reveal information when this compromises public morals if the public interest justifies it. • Consent for use of an image is not required when the image is public information.[889] • Any image taken, published or broadcast in the context of any public event, including official ceremonies, sports meetings and shows of all kinds does not constitute an infringement of image rights. The disclosure of the intimate private life of a person is an invasion of privacy in these circumstances: • the capture, recording, storage, transmission or publication, without the consent of their author, of spoken words, images, photos or videos that were made on a private or confidential basis; • the publication, by any means whatsoever, of a montage made with the words or the image of a person, without his consent, if it is not obvious that it is a montage. Any invasion of privacy committed by one of the means listed above is punishable by a fine of 1 million to 6 million Ariary, without prejudice to the application of Law No. 2014-006 on cybercrime. In the event of violations of privacy and image rights, a judge may also order: • seizure or sequestration of the publication, deletion of contentious passages or publication of an insert; • ordering the offender to pay damages, whether it is a television channel, a press magazine, a photographer, or an unknown person; • the removal of illegal content, in particular videos, photographs, or any other medium involved in the infringement; • the return of any original photographs; • the prohibition of the rebroadcasting of disputed content; • the publication or insertion of the court decision in the press. o Given the broad protection for privacy, it would likely be difficult for a journalist to anticipate in advance when a publication that would violate the right to image or privacy would be justified in the "public interest". o It has been asserted that, despite the amendments to this provision, it still acts as a "sword of Damocles" hanging over the heads of social media users", because of the heavy fines involved, with some worrying that even publishing satirical or parodic images might result in exorbitant fines. [890]
Article 23 read with Article 25: Defamation	Any allegation or public imputation of an incorrect fact which undermines the honour or esteem of a person, or the presumption of innocence which a person enjoys before final conviction of an offence, or a body to which the fact is imputed, constitutes defamation where it results in personal and direct harm to the person or body concerned.

[889] "*Pour l'information du public, le consentement du sujet n'est pas requis*".
[890] African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.

	Toute allégation ou imputation publique d'un fait incorrect qui porte atteinte à l'honneur ou à la considération d'une personne, à la présomption d'innocence dont elle bénéficie avant toute condamnation définitive, ou d'un corps auquel le fait est imputé constitue une diffamation à condition qu'il en résulte un préjudice personnel et direct à la personne ou au corps visé. Both direct publication and republication are punishable as defamation, even if it is reported in doubtful form or even if it targets a person or a body not expressly named, but who can be identified by other clues. The penalty is a minimum fine of 1 million Ariary. The maximum fine is higher where the defamation was made against the State, a State institution, a court, a tribunal or the armed forces. Defamation can be committed against the memory of a deceased person if committed with the intention of attacking the honour or reputation of the deceased's heirs.
Article 24 read with Article 25: Insult	Any offensive expression, terms of contempt or invective uttered against a person that does not involve an imputation of fact but does constitute an insult is an offence. Toute expression outrageante, termes de mépris ou invectives qui ne renferment l'imputation d'aucun fait et proférés contre une personne, constitue une injure. The penalty is a fine of 1 million to 2 million Ariary, with a higher fine applicable in cases where the insult incites discrimination, hatred or violence against a person or a group of people on the basis of nationality, origin, race or religion. Insult can be committed against the memory of a deceased person if committed with the intention of attacking the honour or reputation of the deceased's heirs.
Article 26: Incitement	It is an offence to use media communication - • to incite hatred between genders or religions; • to incite violence, murder, attack on bodily integrity, xenophobia or discrimination • to glorify crimes, war crimes and crimes against humanity, or • to undermine morality and the integrity of the national territory; or • to jeopardize national unity. The penalties are as provided in the Penal Code, but no specific provisions are referenced. o This crime is widely-worded, which could contribute to subjective application.
Article 27: Incitement to crime	It is an offence to use a wide range of means, explicitly including electronic publications, to incite someone to commit a crime, regardless of whether or not the crime actually takes place. The penalties are as provided in the Penal Code, but no specific provisions are referenced.

Article 28: Provocation of armed forces	It is an offence to provoke members of the armed forces, to divert them from their duties and from the obedience they owe to their commanders in the execution of the laws and regulations that govern them. The penalty is a fine.
Article 29: Provoking collective refusal of tax	It is an offence to use communications or other means to organize or attempt to organize the collective refusal of tax. The penalty is a fine.
Article 30: as replaced in 2020:[891] (1) Publication of false information (2) Hindering public holiday celebrations (3) Publications that affect public finance	It is an offence to deliberately publish, disseminate or produce by any means whatsoever false information, or material where parts or facts have been doctored, altered, falsified or falsely attributed to third parties, where such information or material has misled the public or disturbed public order. The penalty is a fine ranging from 5 million to 10 million Ariary. The same applies when the publication, distribution or reproduction is likely to shake the discipline or the morale of the armed forces or to hinder civil peace. La publication, la diffusion ou la production de manière délibérée par quelque moyen que ce soit d'informations mensongères, de pièces ou faits trafiqués, altérés, falsifiés ou mensongèrement attribués à des tiers et laquelle aura induit le public en erreur, troublé l'ordre public, est punie d'une amende de 5 000 000 à 10 000 000 d'Ariary. Les mêmes faits sont punis de la même peine lorsque la publication, la diffusion ou la reproduction faite est de nature à ébranler la discipline ou le moral des armées ou à entraver la paix civile. The same penalty applies to any hindrance by any means whatsoever to the celebration of national holidays or any incitement, by any audiovisual medium, to abstain from participating in national holiday celebrations, whether or not this incitement has been followed by effect. The penalty applies to a publication, distribution or republication that is likely to undermine public confidence in the soundness of the currency, to cause withdrawals of funds from public coffers or establishments required by law to make payments to public funds, to incite the public to sell public securities or effects, or to divert them from the purchase or subscription of these securities or effects, whether or not these allegations or provocations have been followed by results. o "It is not clear how to determine whether information is "false" or the scope of something that is likely to undermine the discipline or the morale of armed forces, obstruct civil peace; undermine public confidence in the strength of currency, or cause withdrawals of public funds. Article 30 therefore fails to provide clear guidance for individuals and provides an overly wide degree of discretion to those charged with the enforcement of this law."[892] o Journalists have criticized the high fine imposed for any interference in the celebration of national holidays.[893]

[891] Loi n°2020-006, Article 30 new.
[892] "LEXOTA Country Analysis: Madagascar", last updated July 2022.
[893] "Madagascar: Controversial Mass Media Code Approved", Library of Congress, 9 September 2016 (references omitted).

Article 31: Outrage against public decency	It is an offence to outrage public decency ("*l'outrage aux bonnes moeurs*") by means of media communications, or through any exhibition of drawings, engravings, paintings, emblems or obscene images via any audiovisual medium. The penalty is a fine ranging from 2 million to 5 million Ariary. o This is another vague prohibition.

With respect to liability under the Code on Media Communications, Article 32 provides that responsibility falls first on the director of the publication, then on the editor-in-chief, then on the author of the publication. The Code also provides a number of procedural directives in relation to criminal offences, particularly for prosecution for defamation and insult.[894]

In the case of a conviction for any offence under the Code, the judge can order permanent confiscation of any equipment used in the commission of the offence.[895] Also of particular note is that this law authorises the suspension of programmes or sections of a publication, or in the case of a repeat offence, permanent closure of the media outlet altogether and/or the removal of the journalist involved in the offences.[896] Concerns have been cited about these far-reaching powers to suspend media licenses and seize the property of media outlets for as few as two infractions of the law.[897] It has also been pointed out that, in effect, the law allows the authorities to close media outlets or ban programmes deemed likely to disturb public order.[898]

According to CIVICUS, the adjudication of the provisions of this law that affect expression is also cause for concern; CIVICUS states that "the Code of Media Communications Law imposes heavy fines for offences such as contempt, defamation and insult against a government official. In addition, flaws in the criminal justice system allow the judiciary to rule under the influence of the executive. Pre-trial detention including of human rights defenders and journalists is prevalent and used as a strategy to force them to self-censor."[899]

While both the cybercrime law and the Code on Media Communications remove custodial sentences for most content-based crimes, they still criminalise and impose heavy fines for defamation, insult and other similar crimes. The crimes of insult and defamation in the cybercrime law appear to be even more onerous than their counterparts in the Code on Media Communications, in their formulation and in the higher maximum fines that can be imposed.

According to the Southern Africa Litigation Centre: "These laws have a chilling effect on journalists', human rights defenders' and every citizen's freedom of expression. It will raise incidents of self-censorship for those who fear heavy fines and other punishments. This law poses a great risk to freedom of expression which is protected

[894] Loi n°2014-006, Articles 36-46.
[895] Id, Article 43.
[896] Id, Articles 44-45
[897] "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
[898] "2023 World Press Freedom Index: Madagascar", Reporters Without Borders, "Legal Framework".
[899] "Madagascar: Journalist acquitted but severe civic space restrictions persist", CIVICUS, 13 March 2020.

by Article 10 of the Constitution of Madagascar and Article 19 of the ICCPR [International Covenant on Civil and Political Rights].[900]

C) OFFENCES RELATING TO EXPRESSION IN THE PENAL CODE

Another provision that is used in practice to stifle free expression is **Article 91 of the Penal Code**, which criminalises acts likely to compromise public security, cause serious political disturbances, provoke hatred of the Malagasy Government or infringe the laws of the country. This crime is punishable by imprisonment for at least one year and at most five years – a significant point since other provisions on defamation and insult are now punishable only by fines. According to LEXOTA:

Article 91 of the Penal Code broadly criminalises any acts that are likely to compromise public security, cause serious political unrest, or provoke hatred of the government. It is unclear what types of statements would be included within the scope of this provision, or what threshold would need to be reached for an act to be likely to compromise public security, cause serious political unrest, or provoke hatred of the government. Article 91 has been used to restrict and punish those critical of the government under the guise of false news.[901]

CODE PENAL, ARTICLE 91	PENAL CODE, ARTICLE 91
[…] Les autres manoeuvres et actes de nature à compromettre la sécurité publique ou à occasionner des troubles politiques graves, à provoquer la haine du Gouvernement malgache, à enfreindre les lois du pays, seront déférés aux tribunaux correctionnels et punis d'un emprisonnement d'un an au moins et de cinq ans au plus. […]	[…] Other manoeuvers and acts likely to compromise public security or to cause serious political unrest, to provoke hatred of the Malagasy Government or to infringe the laws of the country, will be referred to the criminal courts and punished by imprisonment for at least one year and at most five years. […]

D) INVESTIGATION TOOLS AND STATE SURVEILLANCE

In terms of procedure, the **Law on the Fight against Cybercrime** provides that **service providers can be ordered not to erase or anonymous certain technical data for a period of up to one year**, for the purposes of criminal investigation or for the provision of information to the judiciary. The categories of data covered, and the duration of their conservation may be set by decree. The data covered by these provisions relates exclusively to the identification of the persons using the services in question, the technical characteristics of the communications and location information; the law forbids the application of such **preservation orders** to the content of the

[900] "Madagascar's 3rd Universal Periodic Review, 34th Session (Oct-Nov 2019), Submission by Southern Africa Litigation Centre" March 2019, paragraph 16.
[901] "LEXOTA Country Analysis: Madagascar", last updated July 2022.

correspondence exchanged or the information consulted. Service providers otherwise have a legal duty to erase or anonymise all traffic data.[902]

Anyone with knowledge of a **secret agreement for the decryption of encrypted communications**, made for purposes of preparing, facilitating or committing an offence, also commits a crime if they refuse to provide this information to appropriate authorities.[903]

The **Code on Media Communications** states that investigation measures such as excavations, searches, seizures, telephone tapping and recordings that attempt to uncover **journalists' sources** are permitted only where this information is likely to prevent the commission of the offences involving a serious threat to the physical integrity of one or more persons, is of crucial importance to preventing that offence and cannot be obtained in any other way.[904]

The **Code of Criminal Procedure** empowers judges to issue **warrants**, valid for a maximum of three months, authorising police to intercept communications for purposes of criminal investigation if the communications concern bank accounts or historical data about phone conversations. Service providers are not required to disclose intercepted data in the absence of a warrant. No warrant is required in emergency situations, but only limited types of data can be disclosed in these circumstances.[905]

An investigating judge can order the surveillance of bank accounts, access to systems and phone tapping during an investigation of **money laundering or financial crimes**.[906]

In 2014, three lawyers of former President Marc Ravalomanana were reportedly subject to phone surveillance, at a time when Ravalomanana was under house arrest and only being allowed to communicate with his lawyers.[907]

There have been no official reports of the government monitoring online activity in recent years.[908]

---

[902] Loi n°2014-006, Articles 25-27 and 31.
[903] Id, Article 40.
[904] Loi n°2016-029, Articles 11-12.
[905] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, pages 36-37, citing the Code of Criminal Procedure, Articles 103, 129-130. The primary source has not been checked. Note that the text of the secondary source refers incorrectly to the Penal Code, but footnotes the Code of Criminal Procedure.
[906] Id, pages 36-37, citing Article 9 of Law No. 2016-017, which modified and amended some provisions of the Code of Criminal Procedure (which the secondary source mistakenly refers to as the Penal Code). See the Explanatory Memorandum for Loi n° 2016-17, which states that Article 9 of this amending law concerns additions to the Code of Criminal Procedure to enable the fight against money laundering and other financial offences, incuding a new article 260.1 that extends the jurisdiction and power of the investigating judge to order the placement under surveillance of bank accounts, access to these systems and telephone tapping. The primary source was not checked.
[907] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 37.
[908] See, for example, "Freedom in the World 2023: Madagascar", Freedom House, section D4; "Freedom in the World 2022: Madagascar", Freedom House, section D4.

E) SIM CARD REGISTRATION

Law no. 2005-023 on telecommunications obligates operators to comply with the conditions for providing the information necessary for the production of the general directory of subscribers, which are to be set by decree.[909] The Decree on this topic was not located online, but according to other sources, Madagascar has introduced mandatory SIM card registration.[910]

F) TAKE-DOWN NOTIFICATIONS

In terms of the Code on Media Communications. which applies to online materials as well as print publications and broadcast media, a **judge may order the removal of illegal content in the event of violations of privacy and image rights**.[911]

The Code also mandates, as noted above, that there must be a **mechanism in respect of the online press that allows anyone to report the presence of illegal content in the comments made by the internet audience**, upon which the publisher must remove them promptly or make access impossible.[912]

There may be other provisions on the removal of illegal or allegedly illegal content which we have not located. No provision analogous to the take-down notification procedures provided in most other SADC countries was found.

9.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Presidential elections are scheduled for 9 November 2023, with a second round of voting on 20 December if required. President Andry Rajoelina will be seeking a second 5-year term of office. Rajoelina initially came to power through a 2009 military coup that displaced the democratically elected government of Marc Ravalomanana. Rajoelina stepped down in 2014 as part of a negotiated post-coup transition. Hery Rajaonarimampianina served as Madagascar's President from 2014 to 2018. Rajoelina was then elected President in 2018. In 2023, Rajoelina will be competing against both Ravalomanana and Rajaonarimampianina. [913]

[909] Law 2005-023, Article 7(1).
[910] See, for example, "Africa: SIM Card Registration Only Increases Monitoring and Exclusion", Privacy International, 5 August 2019; "Access to Mobile Services and Proof of Identity 2021: Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19". GMSA, April 2021, page 55.
[911] Loi n°2020-006, Article 20 new.
[912] Loi n°2020-006, Article 74*bis* new.
[913] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).

This overview looks at the country's longer electoral history:

> *Since its independence in 1960, Madagascar has organized 12 presidential elections, 12 legislative elections, eight senatorial elections, seven referendums and several local elections, and it has experienced four republics. The country is one of the few countries in sub-Saharan Africa that has gone through several electoral transitions (1993, 1996, 2001 and 2018). However, the regimes elected in the run-offs tend to be hegemonic, as one party "takes it all" and installs authoritarian governance practices. These practices and the lack of credibility and transparency in the organization of the electoral process have led to various problems. These include violent protests in the post-election phase, the mobilization of power outside the institutions, and the seizure of power through public demonstrations and a coup d'état in 2009. The latter caused a political crisis for almost five years and the international isolation of the country. Internal and external mediation efforts suffered serious challenges but ultimately led to the organization of elections as a necessary condition to end the crisis in 2013.*
>
> *The presidential election of December 2018 led to a change of power with the election of Andry Rajoelina. His opponent, Marc Ravalomanana, accepted defeat and called for reconciliation and solidarity and for the demonstrations to stop.*
>
> *In May 2019, a legislative election was held with the participation of several political parties, just like the local elections of December 2019. These elections were generally free, fair and transparent with regard to registration and media access. The question of electoral campaigning is always problematic as certain political parties and candidates run a disguised campaign before the official date, and the financing of electoral campaigns are also an issue. The presidential party won the majority in the two elections.*[914]
>
> *Andry Rajoelina has a majority in all institutions after his victory in the national and local elections. Given this domination, national reconciliation is not one of the priorities of the current government even though there are clear tensions. Indeed, the opposition, which created a coalition led by Marc Ravalomanana, emphasizes that reconciliation is necessary for the development of the country and asks the government to be more open. The opposition therefore boycotted the [2020] senatorial elections. It accused the regime of authoritarian practices accentuated during the lockdown due to the COVID-19 pandemic.*[915]
>
> *Madagascar's political institutions are inefficient, partly due to the lack of a stable pattern of political-party organization, which in turn is an expression of the parties' shallow roots in society. Nearly all presidents have created their political parties after their elections. With about 195 registered political parties in March 2019, the system is highly fragmented, volatile and polarized.*
> *However, polarization changes according to power relations. Politicians will easily change party according to where they have their interests met, and most will try to belong to the party in power. […] This situation confirms the winner-takes-all nature of Malagasy politics and illustrates the prevailing reluctance of politicians to play an opposition role.*[916]

[914] "Madagascar Country Report 2022", Bertelsmann Transformation Index (BTI), Bertelsmann Stiftung, "Political Participation".
[915] Id, "Executive Summary".
[916] Id, "Political and Social Integration".

In the last presidential election in 2018, because the incumbent government controlled much of the formal media space, campaigns on social media were considered by many parties to be useful and cost-effective - even though internet penetration at that stage was not very wide.[917] On the other hand, Russia reportedly used the media to try and influence the outcome of the 2018 elections through disinformation and paying journalists to write flattering stories, as well as hiring young people to attend political rallies.[918]

Elections are supervised by the **Independent National Electoral Commission (CENI)**. Freedom House states that the CENI, although ostensibly independent, is subject to some influence by the executive, which controls member nomination and budget allocation processes. It also reports that CENI's independence and credibility have been seriously undermined by its lack of resources and expertise, particularly in database management and information technology.[919]

The main **Election Law** is Law no. 2018–008, which replaced the previous 2012 Election Law.[920] It contains a number of provisions on "electoral and referendum propaganda", which refers to public meetings, parades, processions, rallies, advertisements in audiovisual, written and electronic media, as well as any other activity aimed at inducing voters to support and vote for a candidate or a list of candidates". Ensuring compliance with these provisions is the duty of **ANRCM, acting in consultation with CENI.**[921] It is explicitly stated that the prohibitions and restrictions on electoral propaganda are applicable to any message having the character of electoral propaganda disseminated by any means of communication to the public, including electronic means.[922]

The Election Law states that **the various means of propaganda used by candidates must respect the limits of freedom of expression** – meaning that election propaganda must not include offensive or defamatory matter. It is also forbidden to bring to the attention of the public a new element of electoral controversy at a time when political opponents do not have a chance to answer the allegations meaningfully before the end of the electoral campaign. It is further prohibited to promote and use a brand or commercial products for propaganda purposes.[923] Some of these prohibitions are vague and could lead to selective enforcement.

Electoral propaganda put forward by candidates or their supporters **must not constitute a means of pressure on voters** that is likely to alter their free choice.[924] Again, it would be hard to have clarity here, in respect of what constitutes pressure.

---

[917] Madagascar election: campaigns on social media, AfricaNews, 5 November 2018.
[918] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
[919] "Freedom in the World 2023: Madagascar", Freedom House, section A3.
[920] Loi n° 2018-008, relative au regime general des elections et des referendums (Organic Law no. 2018–008 relating to the general regime of elections and referendums). which repealed Organic Law no. 2012-005 on the Electoral Code.
[921] Id, Article 92.
[922] Id, Article 95.
[923] Id, Article 93.
[924] Id, Article 94.

There are also certain **time limits on election propaganda**. The electoral campaign period ends a midnight on the day before the ballot. After that, the following are prohibited –

- to distribute newsletters, circulars and other documents;
- to disseminate any message having the character of electoral propaganda to the public by any means of electronic communication;
- to send automated telephone calls to voters seeking their support for a candidate.[925]

Campaign events including public electoral meetings, parades, processions and rallies may take place freely, but a prior written declaration addressed to the relevant State authorities for the area concerned, at least 48 hours before the event. These State authorities must provide copies of these declarations to CENI for monitoring purposes. Campaign events may not be held in places of worship, workplaces, administrative buildings or barracks. The catch is that the State authorities are empowered to prohibit, suspend or cancel a campaign event that carries a risk of "undermining public order". There is, however, a right of appeal to an electoral court in such a case.[926] A "risk of undermining public order" would be hard to determine, particularly in a decision that must be made in advance of the event which is considered to constitute the risk.

Political posters are prohibited during the 6-month period before the official opening of the campaign period. After the campaign opens, CENI regulates the placement of **campaign posters**, which must be far from polling stations. In each location approved for posters, there must be an equal area allocated exclusively to each party – with specific positions determined by lot. Regulations on poster size and the methods of affixing the posters will be set by regulation. It is an offence to remove, deface or obscure campaign posters. No campaign posters may be put up after the election campaign period closes. CENI has the power to enforce the rules on posters, but there is a right of appeal to an electoral court against its decisions. [927]

From the publication of the official list of candidates until the opening of the official electoral campaign, ANRCM guarantees the **right of access to all radio and television services (public and private)** for all candidates and contending parties. During this period, all radio and television services must ensure fair representation of all. under comparable programming conditions. The principle of fairness must be applied to both speaking time and airtime but the principle of airtime equity "does not apply to broadcasts conveying editorial lines". For purposes of equity in speaking time, speeches falling within the exercise of a public function are not counted[928] - which gives an obvious advantage to incumbents. The same principles of equity apply once the official election campaign period begins. **Free airtime** is allocated during this period, with slots chosen by lot. Every audiovisual media outlet must keep a record of the speaking time of political personalities and the airtime granted to each candidate

[925] Id, Article 96; see also Article 116.
[926] Id, Articles 97-99.
[927] Id, Articles 100-109.
[928] Id, Article 110.

and party, which is submitted to ANRCM for monitoring purposes. ANRCM has the authority to impose various sanctions for failure to comply with the rules, with a right of appeal to an electoral court. Commercial advertising for election propaganda purposes is prohibited, with the exception of soliciting donations from the public.[929]

The Election Law states that the use of **new information and communication technologies** or any other **social network resources** is permitted during the electoral period, subject to compliance with the principles of plurality, equity and transparency and under the control of ANRCM.[930] However, enforcement of these principles online would surely be very difficult to achieve.

The **publication of the results of opinion polls directly or indirectly linked to the elections** is prohibited during the election campaign period and also during the period of electoral silence that begins on the day before the polling day.[931]

Another interesting point relates to the **processing of personal data in the context of election campaigns.** This is not forbidden, but electoral authorities are charged to ensure that the collection of such data is lawful and fair. Any file created for political communication purposes cannot be used for any other purpose, and propaganda files compiled for the needs of a particular electoral campaign must be destroyed at the end of the electoral period concerned.[932]
There are also several offences contained in the Election Law with particular relevance for freedom of expression. These are some of the keys such offences:

- It is an offence **during the election campaign, to incite fights that have disturbed public order and safety** by means of speeches or publications, punishable by a prison sentence or a fine, or both.[933]
- The **distribution of defamatory materials during the election campaign** by any other means, including digitally, is an offence punishable by a fine.[934]
- **Insult to authorities or institutions of the Malagasy State during an electoral campaign**, is an offence punishable by imprisonment for 6 months to 3 years and a fine, or by only one of these two penalties.[935] This offence could be applied to give the ruling party an advantage by muffling criticism of its past performance.
- **Violation of any of the rules on election propaganda** is an offence, punishable by imprisonment or a fine, or both.[936]
- It is an offence **to make a public statement in favour of or against a candidate or party on the polling day or the day before**, punishable by a fine.[937]

[929] Id, Article 111-115.
[930] Id, Article 117: "L'utilisation des nouvelles technologies de l'information et de la communication ou de toute autre ressource des réseaux sociaux est admise dans le cadre de la période électorale. Elles demeurent assujetties au respect des principes de pluralité, d'équité et de transparence, sous le contrôle de l'Autorité nationale de régulation de la communication médiatisée."
[931] Id, Article 118. This is an offence under Article 228, punishable by a stiff fine.
[932] Id, Article 119.
[933] Id, Article 218.
[934] Id, Article 221.
[935] Id, Article 222.
[936] Id, Article 224.
[937] Id, Article 227.

According to Freedom House, almost 200 political parties are registered in Madagascar even though the law on political parties imposes a high financial barrier for political candidacy. Freedom House also states that political leaders "frequently use religion, ethnicity, and caste as instruments to mobilize voters".[938]

In the 2018 election, ANCRM was not operating effectively, which reportedly placed a burden on CENI to regulate the media during the election period on top of its other duties. Also, in the 2018 election campaign, regulatory powers did not extend to private broadcasters, which lead to significant disparities in treatment between the candidates.[939] Both of these problems have been remedied since then.

Freedom House reports that authorities at times decline requests for protests and rallies in the name of public security, and that several meetings of opposition parties were banned or forcefully dispersed by the police during 2022.[940] Indeed, in April 2023, the government banned "public meetings of a political nature" in the open air, although such meetings may still take place in closed rooms where the words spoken are not heard outside. The government claimed to be relying on a 1960 ordinance aimed at maintaining public order. In addition, Parliamentarians are to speak about the adoption of laws only at the end of each session, and only within their constituencies, and mayors and their deputies have been ordered to limit their public statements to reports on their activities. These moves have led to widespread local and international criticism. Even though the rules apply to all political parties, including the ruling party, it will not concern the President and members of the government where they express themselves "in their function for the implementation of the general policy of the State". One diplomat commented that members of the ruling party will be able to crisscross the country to campaign for the sitting President while opposition parties "will have to make do with small audiences behind closed doors". Some opposition parties have referred to the developments as a "coup against democracy", while the leader of the opposition party Malagasy MMM called them a move "towards dictatorship".[941]

[938] "Freedom in the World 2023: Madagascar", Freedom House, sections B1-B2.
[939] "Recueil de Recommandations", CENI/PADEM, 13 October 2021, page 56.
[940] "Freedom in the World 2023: Madagascar", Freedom House, section E1.
[941] "Madagascar Bans Public Protests Ahead of Presidential Election", ICTJ, 4 April 2023; Laurence Caramel, "A Madagascar, le président Andry Rajoelina confine l'opposition", *Le Monde Afrique*, 6 April 2023.

CHAPTER 10

MALAWI

CHAPTER 10: MALAWI

MALAWI KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **82nd globally; 19th out of 48 African countries** "Political influence over the media restricts journalistic freedom in Malawi. Reporters are still subjected to threats and cyber-harassment."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Malawi's 1994 Constitution, as amended through 2020 **34. FREEDOM OF OPINION** Every person shall have the right to freedom of opinion, including the right to hold, receive and impart opinions without interference. **35. FREEDOM OF EXPRESSION** Every person shall have the right to freedom of expression. **36. FREEDOM OF THE PRESS** The press shall have the right to report and publish freely, within Malawi and abroad, and to be accorded the fullest possible facilities for access to public information. **37. ACCESS TO INFORMATION** Every person shall have the right of access to all information held by the State or any of its organs at any level of Government in so far as such information is required for the exercise of his or her rights. **38. FREEDOM OF ASSEMBLY** Every person shall have the right to assemble and demonstrate with others peacefully and unarmed. **44. LIMITATIONS ON RIGHTS** 1. No restrictions or limitations may be placed on the exercise of any rights and freedoms provided for in this Constitution other than those prescribed by law, which are reasonable, recognized by international human rights standards and necessary in an open and democratic society.

2. Laws prescribing restrictions or limitations shall not negate the essential content of the right or freedom in question and shall be of general application.
KEY LAWS: • Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*] • Penal Code [*Chapter 7:01*] (selected provisions) • as amended by the Penal Code (Amendment) Act 8 of 2023
CRIMINAL DEFAMATION: constitutionality of "criminal libel" being challenged in court as of mid-2023[942]
DATA PROTECTION: Malawi does not have a data protection law, but a draft is being reviewed by the Ministry of Justice.[943]
ACCESS TO INFORMATION: Malawi has access to information law.[944]

10.1 CONTEXT

Newspapers (and any periodical published at least monthly) must be registered under the **Printed Publications Act 18 of 1947**.[945]

Under the **Censorship and Control of Entertainments Act 11 of 1968**, no one may direct or even take part in the making of any film in Malawi without a film permit; violation of this rule is a criminal offence.[946] The showing of films requires a theatre permit, even where this does not take place on a commercial basis. as well as a certificate of approval for the film (which may set age ratings or impose conditions on the exhibition of the film).[947] Plays, concerts, art exhibitions and other public entertainments require an entertainment permit, which can similarly be issued subject to conditions.[948] Failure to obtain the necessary permits, which are issued by a board appointed by the relevant minister, constitutes a criminal offence.[949]

The Communications Act 34 of 2016, which repealed the Communications Act 41 of 1998, regulates broadcasting, telecommunications and postal services in Malawi.[950] The key regulatory body is the Malawi Communications Regulatory Authority (MACRA). The Board of this body is made up of *ex officio* government officials alongside other members appointed by the President, subject to confirmation by the

[942] *Mbele v R* (Misc. Criminal Case No. 04 of 2022) 2022 MWHC 74 (20 June 2022) (issue of unconstitutionality referred to Chief Justice for certification as a constitutional matter to be heard by a three-judge panel); "Supreme Court rebuffs State on Army General Nundwe's defamation case against Chisa Mbele", *Nyasa Times*, 18 September 2022.
[943] Data Protection Bill, 2021. There are some provisions pertaining to data protection in the Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].
[944] Access to Information Act 13 of 2016.
[945] Printed Publications Act 18 of 1947 [*Chapter 19:01*].
[946] Censorship and Control of Entertainments Act 11 of 1968 [*Chapter 21:01*], sections 19-ff.
[947] Id, sections 9-ff.
[948] Id. sections 14-ff.
[949] Id, section3 (appointment of Board of Censors); on offences, see the sections on each type of permit read with section 32.
[950] Communications Act 34 of 2016 [*Chapter 68:01*], section 2; definition of "communications service" in section 3.

Public Appointments Committee of Parliament.[951] Although, the Communications Act states that MACRA "shall be independent in the performance of its functions",[952] its independence is compromised by the absence of a public nomination process for Board members and by the fact that a third of its members are *ex officio* representatives of the executive.[953] The Act contains regulations for content services that cover topics such as the right of reply, fair comment, the duty to present news truthfully, accurately and objectively, and the duty to provide balance in respect of "controversial issues of public importance".[954] Broadcasting licensees must are also required to ensure equitable treatment of all political parties, election candidates and electoral issues during an election. It should be noted that this regulation says that content licensees must not "broadcast any material that is indecent or obscene or offensive to public morals, including abusive or insulting language, or offensive to religious beliefs of any section of the population, or likely to prejudice the safety of the Republic or public order and tranquillity".

Failure to comply with the Act can lead to suspension or revocation of a licence.[955]

The state broadcaster, the Malawi Broadcasting Corporation (MBC), is also regulated by the **Communications Act 34 of 2016**.[956] It is governed by a Board composed of four *ex officio* government officials, and five other members appointed by the President subject to confirmation by the Public Appointments Committee of Parliament.[957]

Online content is regulated by the **Electronic Transactions and Cybersecurity Act 33 of 2016**, discussed below.

The media has a self-regulatory body called the **Media Council of Malawi (MCM**). It is reported that the MCM, which was initially established in 1995, was dormant from 2010 until its re-launch on 31 December 2019. The MCM has a Code of Ethics and Professional Conduct (the Code) which governs the conduct and practice of journalists in Malawi which date from the period before its dormancy.[958]

[951] Id, sections 5 and 8.
[952] Id, section 5(3).
[953] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 370-371.
[954] Communications Act 34 of 2016 [*Chapter 68:01*], Second Schedule.
[955] Id, section 43(1)(a).
[956] Id, Part XIV.
[957] Id, sections 111-112.
[958] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 406-ff. The Media Council of Malawi Code of Ethics and Professional Conduct is available here. The MCM's own website could not be accessed in mid-2023 as it was infected with a computer virus.

10.2 CONSTITUTION

The sections of the Malawi Constitution most relevant to this discussion are reproduced in the table on the first page of this chapter.

Unlike many other constitutions in the SADC regions, the grounds for limiting the freedom of expression and other fundamental rights are not specified with reference to concerns such as national security or public morals. Section 44 requires only that restrictions or limitations on rights and freedoms must be -

- prescribed by laws which are of general application and do not negate the essential content of the right or freedom in question;
- reasonable;
- recognized by international human rights standards; and
- necessary in an open and democratic society.

Section 36 of Malawi's Constitution is notable for explicitly guaranteeing to the press "the right to report and publish freely, within Malawi and abroad". It has been observed that this provision is important because it explicitly protects both the reporting and publishing rights of the press, and extends those rights to national and international media reporting on Malawi both inside and outside the country. It also recognises the political role of the press in providing information to the public, by stating that the press must be provided with access to public information.[959]

It is also unusual that Section 37 of the constitution on the right of assembly specifically protects the right to "demonstrate with others peacefully and unarmed", given that demonstrations are an important form of political expression.

In 2002 the President of Malawi issued an **oral directive at a political rally banning all forms of demonstrations against a proposed constitutional amendment** which would remove the limitations on the terms of office of the President and Vice-President. The Law Society and other concerned civil society groups approached the High Court seeking an order that the directive violated their constitutional rights to freedom of association, assembly and demonstration, expression, conscience and opinion. In *Malawi Law Society v The President*, the Court found the oral directive unconstitutional on the grounds that it did not amount to "law", and that the ban was also unreasonably wide and incapable of enforcement. Thus, it did satisfy the criteria in section 44 for restrictions on constitutional rights and freedom.[960]

The right to demonstrate peacefully was considered by the Supreme Court of Appeal (Malawi's highest court) in the 2019 case of *Attorney General v Trapence*. In the aftermath of Malawi's disputed 2019 Presidential election, the election results were challenged by opposition leaders who alleged vote-counting irregularities. The Malawi Human Rights Defenders Coalition organized a series of demonstrations calling for the dismissal of the chairperson of the Electoral Commission. A first round of protests was marred by violence. The Attorney General then sought an **injunction**

[959] Id, page 347.
[960] *Malawi Law Society v The President* (2002) AHRLR 110 (MwHC 2002); see the case summary by Global Freedom of Expression here.

preventing future demonstrations on the election result until the issue of violence had been resolved and the opposition leaders' court challenge had been finalized. The issue concerning demonstrations about a matter that was *sub judice* was moot by the time the Supreme Court ruled on the injunction, but it held that the concerns about possible violence did not warrant the requested injunction. While demonstrators, individually and collectively, have a duty to ensure that protesters are unarmed and that there is no violence during demonstrations, this is not their sole responsibility; police also have a duty to act to address violence and criminality, and their assertion that they lacked the resources to do this was not persuasive to the Court.[961]

In the aftermath of the disputed 2019 election, there was intense public debate on many platforms, including radio and television. Live call-in radio shows where listeners aired their opinions on the electoral process proved to be particularly popular. In June 2019, the Director-General of MACRA issued a **public announcement banning call-in radio shows** on the basis that these shows were a platform for callers to incite the public to violence. The relevant minister then issued the **Communications (Broadcasting) Regulations, 2019**, which **banned all live radio phone-in programmes unless the broadcasters utilised a delay machine to allow sufficient time to remove any prohibited content**. Both measures were challenged by the National Media Institution of Southern Africa (NAMISA) and two affected radio stations.

The High Court found that the Director-General's "ban" had no proper legal basis. It also found that the regulations were issued without following the statutory requirements for stakeholder consultations. The Court stated: "Whereas the intentions of ensuring that a potentially volatile political climate does not degenerate into social disorder through unwholesome radio content cannot be gainsaid, such measures have to be both proportionate and appropriate promulgated".[962] It went on to say that "the broad extent of the proposed measures amounted to illegal censorship of publication of legitimate opinions and the communication of diverse points of view. Freedom of expression and its corresponding right to hold and share opinions need to be jealously guarded especially within the context of a contest electoral process […]."[963] However, the Court also indicated that requiring a few seconds delay by broadcasters might be an acceptable way to avoid the publication of "unsavoury and even inflammatory opinions" if proper procedures for issuing such regulations were followed – while finding it unnecessary to decide in this case whether a properly-promulgated regulation to this effect would be a justifiable limitation of the constitutional rights that were implicated.[964]

In the 2022 *Mbele* case, the High Court found merit in the contention that the offence of **criminal libel** is unconstitutional. Section 200 of the Penal Code provides: "Any person who, by print, writing, painting, effigy, or, by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory

[961] *Attorney General v Trapence*, Supreme Court of Appeal, MSCA Civil Appeal No. 55 of 2019, 30 September 2019l see the case summary by Global Freedom of Expression here.
[962] *S v MACRA; Ex Parte The Registered Trustees of National Media Institute of Southern Africa & 2 Others* (Constitutional Reference 3 of 2019) [2020] MWHC 193 (29 May 2020), paragraph 26.
[963] Id, paragraph 27.
[964] Id, paragraphs 33-35.

matter concerning another person, with intent to defame that other person, shall be guilty of the misdemeanour termed 'libel'."[965] The penalty for libel is an unspecified fine or imprisonment for up to two years. The High Court found that a *prima facie* "discordance" between this offence and the constitutional right to freedom of expression. It considered jurisprudence on criminal defamation and freedom of expression under the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights, and concluded that there was merit in a consideration of whether the Malawi law on criminal libel constituted a limitation on the right to freedom of expression that met the requirements of reasonableness, recognition by international human rights standards and necessity in an open and democratic society. The High Court thus referred the case to the Chief Justice for certification as a constitutional matter to be heard by a three-judge panel.[966] As of mid-2023, the Supreme Court had not yet issued a ruling on this case.

10.3 CASE STUDIES

According to Reporters Without Borders:

> *The disputed elections of 2019 had a negative impact on press freedom. Several TV channels were vandalised, and radio phone-in programmes were banned when the results were being announced. Malawi has not yet adopted a whistleblower protection law, and journalists are sometimes subjected to threats and online intimidation. Several cases of physical attacks on journalists, especially by political party activists or police, have been reported in recent years. Journalists are still sometimes arrested arbitrarily […].*[967]

Freedom House gave this overview of internet freedom in Malawi in 2022:

> *Internet freedom in Malawi declined during the coverage period, as state authorities retaliated against journalists who published corruption allegations against the government. The arrests and detentions of journalists who cover political leaders or discuss corruption in their online content has [sic] resulted in increased self-censorship. Online news outlets have been subject to government manipulation via unofficial directives in recent years, though there were no reported cases of censorship or forced removal of content during the coverage period.*[968]

[965] Penal Code [*Chapter 7:01*], section 200. The Penal Code was recently further amended by the Penal Code (Amendment) Act 8 of 2023, which does not affect this section, but (as discussed below) did repeal some other provisions of the Penal Code relevant to expression.
[966] *Mbele v R*, Misc. Criminal Case No. 04 of 2022, High Court of Malawi, 20 June 2022.
[967] "2023 World Press Freedom: Malawi", Reporters Without Borders, "Safety".
[968] "Freedom on the Net 2022: Malawi". Freedom House, "Overview". See also section B4.

The International Press Institute noted in 2021 that the current Malawi government, which has been in office since June 2020, has made several efforts to position itself in a good light in terms of media freedom – citing as one example the inclusion of journalists among the priority group of people to be first in line for the Covid-19 vaccine; yet, on the other hand, journalists are still often the target of attacks, both by the police and the public.[969]

In 2023, *Maravi Post* journalist Dorica Mtenje was charged with **criminal libel** and **offensive communication under the cybercrime law** following a complaint by the Director of the National Intelligence Service about an article concerning his suspension for alleged gross incompetence and misappropriation of funds**.** She was detained for about 12 hours. Police reportedly confiscated her phone but returned it upon her release. The article in question did not carry a byline, and Mtenje asserted that she did not write or publish it.[970]

In 2022, the privately owned news website *Platform for Investigative Journalism* published an article alleging police corruption in connection with a contract for the procurement of water cannons. A few days later, Gregory Gondwe, the managing director of this news site, was detained for about six hours while police questioned him, in the presence of his lawyer, about the sources for that article. Police also searched the news office under a warrant issued in connection with the alleged offence of **spamming, pertaining to the illegal transmission of information online, under section 91 of the Electronic Transaction and Cyber Security Act, 2016.** Police confiscated Gondwe's cell phone and laptop and forced him to disclose his passwords. The devices were returned the next day. Gondwe was not formally charged, but police indicated that they were still investigating the case. The Attorney-General apologised for Gondwe's detention and questioning, stating that he had no knowledge that police would take this route, and committing to a government review of archaic laws that restricted media freedom. A police spokesperson said that Gondwe had not been arrested but merely "interviewed" in connection to an ongoing investigation into the news article and related issues.[971] Not long after this incident, the *Platform for Investigative Journalism* reported that its website had been hacked and compromised; the Media Institute of Southern Africa (MISA) in Malawi claimed that the hacking was an intentional act committed by state authorities.[972]

In 2022, Chidawawa Mainje was arrested and charged with the offence of **cyber harassment under section 86 of the Electronic Transactions and Cyber Security Act, 2016** for allegedly insulting the President in a WhatsApp conversation. This arrest raised concerns that authorities were monitoring private electronic communications despite

[969] Antonio Prokscha. "Malawi: Recent detentions of journalists overshadow positive press freedom image", **International Press Institute, 12 April 2021.**
[970] "Malawi police detain, charge journalist Dorica Mtenje over story she did not write", Committee to Protect Journalists, 22 February 2023.
[971] "Malawi journalist Gregory Gondwe detained, questioned about sources for article on alleged corruption", Committee to Protect Journalists, 8 April 2022.
[972] Freedom on the Net 2022: Malawi", Freedom House, section C8; Lameck Messina, "Malawi Police Accused of Hacking Website of Investigative Media Group", *VOA*, 17 April 2022; "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.

their encryption, without appropriate legal authority and without any notice to those being monitored.[973]

In 2022, a man was arrested for posting a message on Facebook saying that a Member of Parliament had siphoned maize meant for his constituency. He was charged with **cyberstalking under the Electronic Transactions and Cyber Security Act** before being released at the request of the MP in question.[974]

In 2022, social media influencer Joshua Chisa Mbele was charged with **criminal libel** and **publication of offensive communication in violation of section 87 of the Electronic Transactions and Cyber Security Act**. According to one account, this was in connection with posts alleging that a Malawi Defence Force commander had accepted bribes from a corruption suspect.[975] According to another source, the arrest related to a Facebook post where he shared a list of government officials who allegedly had offshore bank accounts, although he deleted the post after realising that he had fallen for misinformation.[976] Mbele's case led to the challenge to the constitutionality of criminal libel, discussed in the section above.

In 2021, Ignatius Kamwanje plead guilty to a charge of **spamming in violation of the Electronic Transactions and Cyber Security Act** in connection with a Facebook post in which he alleged that money was being stolen from customers at the National Bank of Malawi. Bank employees filed a complaint with the police, contesting this allegation.[977]

It was also reported in 2021 that police in the capital city Lilongwe interrogated Watipaso Mzungu, chief reporter of the privately-owned news website *Nyasa Times*, about an article quoting a local activist who referred to the President as "a joker" and a "time waster" in relation to a proposed Cabinet reshuffle. Mzungu was asked by police to come to police headquarters for questioning, where he was told that the article constituted a **criminal insult of the President and an attempt to undermine the authority of the head of state.** The interrogation lasted about two hours, with Mzungu being asked about his motivations for writing the report and whether he had manipulated the activist's statements to attract public attention. Police also demanded the unedited draft of the news story, as well as the activist's original statement. Mzungu was released without charge after this questioning. The police later stated that Mzungu had merely been "invited for an interview" in connection with an ongoing investigation, and that he had cooperated with the police.[978]

---

973 "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 1F; "Malawi 2022", Amnesty International, "Freedom of expression".
974 "Freedom on the Net 2022: Malawi", Freedom House, section C3.
975 "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A. See also Duncan Mlanjira, "Law Professor Accuses Army General of Abusing his Power in Social Media Activist Arrest", *Nyasa Times*, 2022.
976 "Freedom on the Net 2022: Malawi", Freedom House, section C3. See also "Malawi Police arrest social media activist", *Malawi24*, 11 January 2022/
977 "Freedom on the Net 2022: Malawi", Freedom House, section C3.
978 "Malawi police question journalist Watipaso Mzungu over article calling president 'a joker'", Committee to Protect Journalists, 14 April 2021.

In another 2021 incident, police detained Enock Balakasi, a reporter for the privately owned broadcaster *Joy Radio*, for more than two hours after he photographed police who had responded to an attempted suicide in a suburb of Lilongwe. Police allegedly accused him of photographing them without permission, and deleted photos from his phone. He was initially charged with **conduct likely to cause a breach of peace**, **obstructing police officers on duty**, and **working without permission from the police**, but the charges were dropped after police questioning.[979]

In 2021, Irene Chisulo Majiga was arrested for publishing a voice note on WhatsApp, which later went viral, alleging that a person detained on rape charges was released under questionable circumstances. She plead guilty to a charge of disseminating false information in violation of **section 60(1) of the Penal Code** and paid a fine. The State Prosecutor argued that the post had created public unrest, but it is not clear that there was any clear, objective public harm. [980]

Raymond Siyaya, a journalist from *Chanco Community Radio*, was also arrested in 2021 for allegedly reporting "fake news" on his Facebook page in violation of **section 60(1) of the Penal Code**, by claiming that government officials had mismanaged COVID-19 emergency relief funds. He was later released the charges against him were dropped.[981]

Also in 2021, **police officers beat and briefly detained** Oliver Malibisa, a reporter with *Likoma Community Radio*, as he tried to cover a student demonstration. Malibisa alleged that a police officer hit him in the chest with a gun and told him to stop filming the demonstration. When the journalist continued to film the event, police used pepper spray on him and detained him. He was held at the Likoma Police Station for about two hours before being released without charge. His phone was taken but returned upon his release. [982]

It was reported in 2020 that Tumpale Mwakibinga was arrested and charged with **offensive communication under the Electronic Transactions and Cyber Security Act** for a Facebook post in which he mocked the former First Lady. He was released on bail pending trial, subject to a bail condition prohibiting him from posting anything on social media related to the former First Lady.[983]

In 2020, three journalists were detained for two hours at Kamuzu International Airport in Lilongwe, after attempting to cover the arrival of an EU delegation due to present their final report on the disputed election. Their equipment was confiscated and their footage deleted, and they were locked in a police cell in the airport. Police first charged the three with "**conduct likely to cause breach of the peace**," but the charge was changed to **disorderly conduct under the Aviation (Airport Security) Regulations issued in terms of the Aviation Act**. A police spokesperson stated that the

[979] Id.
[980] "LEXOTA Country Analysis: Malawi", last updated December 2022.
[981] Id.
[982] "Malawi police beat, detain radio reporter Oliver Malibisa", Committee to Protect Journalists, 21 July 2021.
[983] "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020].

journalists were arrested because they had not sought the necessary permission to "cover airport activities", which requires a permit in terms of the aviation regulations.[984]

These incidents indicate that the application of cybercrime offences against journalists and persons who post on social media is taking place in practice. This could be in part due to the fact that Malawi's cybercrime law has been in force longer than those in some other jurisdictions, or it could be due to overbroad drafting of some of the offences covered by the law or targeted application of the laws to dampen criticisms of public figures.

There is some indication that the Malawian government considered an internet shutdown in connection with its 2019 elections, although in the end there was only some temporary disruption of debatable origin:

> *Leading up to the election on 21 May 2019, there were rumours swirling that the government of Malawi was considering shutting down the internet on the day of the election. Several meetings between the government, the Malawi Communications Regulatory Authority (MACRA), and civil society occurred during the weekend before the election. Lawyers from MACRA resisted efforts by the government to shut down the internet and stated that while they believed Malawian law gave them the authority to shut off internet access, they did not think that it was necessary. There were also reports that the government was directly pressuring individual ISPs within the country to shut off access.*
>
> *On the day of elections, there were reports that several of the major internet arteries between Blantyre and Lilongwe were cut. NetBlocks reported a 20% decrease in internet activity in the three hours following the closure of the polls. The government stated both that there was no internet shutdown, and that vandals had cut lines that caused some services to be down temporarily.*[985]

10.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT 33 OF 2016

Malawi's **Electronic Transactions and Cyber Security Act 33 of 2016** is an omnibus piece of legislation that covers electronic transactions, e-commerce, certain data protection issues, management of domain names and e-government as well as cyber security and cybercrime.[986] The Act has three key objectives:

---

984 "Malawi detains, charges 3 journalists seeking to cover EU delegation's return", Committee to Protect Journalists, 10 January 2020.
985 "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, page 8 (footnote omitted).
986 Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].

- to set up a responsive information and communication technology (ICT) legal framework to facilitate competition and development in the sector and "the participation of Malawi in the information age and economy";
- to protect ICT users from undesirable impacts, including the spread of pornographic material, cybercrime and digital fraud;
- to put in place mechanisms that safeguard ICT users from fraud, breach of privacy, misuse of information and immoral behaviour brought by the use of ICT.[987]

The Act is administered by the **Malawi Computer Emergency Response Team** (Malawi CERT, or MCERT) which is set up as a unit within MACRA.[988] MACRA also has the power to appoint cyber inspectors with certain monitoring and investigative powers.[989]

The Act's reach is very broad, as many of its provisions apply to "online public communication" which means "any transmission of digital data, signs, signals, texts, images, sounds or messages, of whatever nature, that are not private correspondence, by electronic communication means that enable a reciprocal exchange of information between an issuer and a receiver".[990]

In general, the Act states that online public communication may be restricted in order to –

- prohibit child pornography;
- prohibit incitement of racial hatred, xenophobia or violence;
- prohibit justification for crimes against humanity;
- promote human dignity and pluralism in the expression of thoughts and opinions;
- protect public order and national security;
- facilitate technical restriction to conditional access to online communication; and
- enhance compliance with the requirements of any other written law.[991]

Freedom House notes concerns about the approval of restrictions to "protect public order and national security", on the grounds that this is a broad provision that is open to abuse. It also expresses concerns about restrictions to "facilitate technical restriction to conditional access to online communication", on the basis that this is "an unclear statement that could be interpreted to enable network shutdowns or blocks on social media platforms".[992]
The cybercrime offences in the law are as indicated in the tables below. They "are informed by the **SADC framework** and other international principles".[993]

[987] Id, section 2
[988] Id, sections 5-6.
[989] Id, sections 69-70.
[990] Id, section 3 (definition of "online public communication").
[991] Id, section 24(2).
[992] "Freedom on the Net 2022: Malawi", Freedom House, section A3.
[993] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 26.

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016 - TECHNICAL OFFENCES	
Section 84: Unauthorized access, interception or interference with data	It is an offence – • to intentionally **access** or **intercept** any data without authority or permission to do so, or to exceed the authorized access (subsection (3)); • to intentionally and without authority to do so, **interfere** with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective (subsection (4)). The Minister shall, by regulations, come up with specific cases where unauthorized access to, interception of, or interference with, data may be permitted in specific conditions set out in the regulations (subsection (2)). It is an offence - • to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any **device**, including a computer program, a component or a phone, which is designed primarily to overcome security measures for the protection of data, or to perform any of these acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item (subsection (5)); • to utilise any device or computer program referred to above in order to **unlawfully overcome security measures** designed to protect "such data or access thereto" (subsection (6)); • to commit any act described in this section with the intent to interfere with access to an information system so as to constitute a **denial, including a partial denial, of service** to legitimate users (subsection (7)); • to **communicate, disclose or transmit any data, information, program, access code or command** to any person not entitled or authorized to access it (subsection (8)(a)); • to knowingly **introduce or spread a software code that damages** a computer, computer system or network (subsection (8)(b)); • **to access or destroy any files, information, computer system or device** without authorization, or for the purposes of concealing information necessary for an investigation into an offence (subsection (8)(c)); or • to **damage, delete, alter or suppress any communication or data without authorization** (subsection (8)(d)). It is also an offence for a person to **knowingly receive data** which that person is not authorized to receive (subsection (9)). There is an **enhanced penalty** where an offence is committed in relation to data concerned with "national security" (which is not defined) or the provision of an "essential service" (not defined) (subsection (10)). o "Access" is not defined. o While some assert that criminalisation of "mere access" without more is justified given that it compromises data confidentiality, there is no universal consensus on whether criminalization of mere access to non-protected systems is warranted, or whether this crime should be narrowed by additional conditions.[994] The *SADC Model Law on Computer Crime and Cybercrime* qualifies the offence of illegal access

[994] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.

	by requiring that it take place "intentionally, without lawful excuse *or justification* or in excess of a lawful excuse or justification".[995] o There are overlaps between the offences of unauthorised access in section 87(3), overcoming computer security measures designed to protect the security of data in section 87(6) and hacking in section 89. o Regarding the statute's reference to illegal interception of data (section 84(3)), one analysis comments: "Malawi's definition is unnecessarily skeletal and basic. The definition would have been improved by merely looking at how other countries both regionally and internationally have drafted their own offences on data interference. Moreover, the requirement that the interception must be to non-public transmission of data has not been included, and omission that renders the offence overly broad."[996] o Interfering with data is covered generally in section 84(4), but this overlaps with other provisions that talk about destroying damaging, deleting, altering or suppressing data (sections 86(8)(b)-(c)). o Section 84(6) is unclear because it references section 86(5) which uses the word "data in two different senses (once to refer generally to information that is protected, and once to refer to "a password, access code or any other similar kind of data" - and then ambiguously refers to "such data". o Regarding the offences relating to devices covered by sections 86(5) and (6), It has been noted that limiting these offences to devices *designed to overcome security measures for the protection of data* means that the offence does not apply to devices that can be used to commit other cybercrimes.[997] o The offence of communicating or disclosing data or information to any person not entitled or authorized to access it in section 86(8)(a) could impede whistleblowers. o Making it an offence to knowingly receive data which one is not authorized to receive (section 86(9)) could affect public access to information acquired by a whistleblower or placed in a cache such as Wikileaks. There is no exception for lawful excuse or acting in the public interest. o The conditions which lead to an enhanced penalty are unclear since the key terms ("national security" and "essential service") are general and undefined.
Section 89: Prohibition of hacking, cracking and introduction of viruses	It is an offence to hack into any computer system, or knowingly introduce or spread a virus into a computer system or network. o "Hacking" and "cracking" are not defined, and the term "cracking" appears only in the heading of the provision and not in the text. This makes the prohibited conduct unclear. It has also been noted that the use of the technical term "hack" in the definition "violates one of the best practices in the drafting of cybercrime legislations, viz., that as much as possible, and whilst not compromising on the clarity of the law, 'technology–neutral language' must be preferred when defining

[995] SADC Model Law on Computer Crime and Cybercrime, section 4.
[996] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 17. Note that some of the section numbers referred to by Bande in respect of the Malawi law are incorrect.
[997] Id, page 22.

	cybercrime offences. This is necessary to ensure that the criminalization covers both existing and future technologies."[998] o This offence appears to overlap with section 87(3) on unauthorized access, and section 87(6) which makes it an offence to utilise a device or computer program to unlawfully overcome security measures designed to protect computer data or access to it.[999] o Note that no malicious intention is specified for any of the acts listed, and that hacking is not specifically required even to take place knowingly – although this may be implied by the generally-understood meaning of the term "hack". The general principles of criminal liability would require some degree of *men's rea* (criminal intent).
Section 90: Unlawfully disabling a computer system	It is an offence to wilfully or maliciously render a computer system incapable of providing normal services to its legitimate users. o "Anything that renders a computer system incapable of providing normal services to legitimate users is covered. A literal reading of the provision would include both technical and non-technical activities. In practice, however, most activities that would hinder a computer system from providing normal services would be technical in nature."[1000] o This offence overlaps with section 87(8)(b), which makes it a crime to introduce or spread a software code that damages a computer, computer system or network. One commentary suggests that these two offences should have been combined into one because "they target various modes of interfering with a computer's system", while it would have been better to enact "a single offence of system interference, which would capture the various ways of committing that offence."[1001]
Section 91: Prohibition of spamming	It is an offence to transmit any unsolicited electronic information to another person for the purposes of illegal trade or commerce, or other illegal activity. o Note that the use of spam is not criminalised unless it relates to some illegal activity; spamming by legitimate businesses is not covered here. o As the case studies in section 103 of this chapter indicate, this offence has been applied in practice to inhibit freedom of expression. Since this offence has to be underpinned by some other "illegal activity," these applications of it must have been supported by the offence of criminal libel – which is currently the subject of a constitutional challenge.
Section 92: Prohibition of illegal trade and commerce	It is an offence to use the internet as a medium for any illegal activity or trade, fraudulent transaction or as a means of procuring any internet-related fraud.

The cybercrime law includes only four content-based offences, as summarised in the table below.

Unusually, **the law does not include any offences relating to the publication of racist**

[998] Id, page 15 (reference omitted).
[999] Id, page 24.
[1000] Id, page 19.
[1001] Id, page 20.

or xenophobic material or material relating to genocide and other crimes against humanity, via electronic means or otherwise. This seems odd, given that the Act explicitly states that online public communication may be restricted in order to prohibit incitement of racial hatred, xenophobia or violence and justification for crimes against humanity (amongst other things).[1002] No other laws covering publication of materials about these topics were located, other than a provision in the Penal Code prohibiting commission of the crime of genocide.[1003]

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016 - CONTENT-BASED OFFENCES	
Section 85: Child pornography	There is a range of offences relating to "child pornography in an electronic form". For the sake of protecting children from pornography, establishments serving the public, and places open to the public proposing access to the Internet, are required to use adequate pornography filtering software as defined by subsidiary legislation made under the Act. o "Child pornography" is defined in section 2 to mean "visual and pornographic material that depicts, presents or represents a person under the age of eighteen engaged in sexually explicit conduct or an image representing a person under the age of eighteen engaged in sexually explicit conduct". "Pornography" is defined in section 2 as "visual material that depicts images of a person engaged in sexually suggestive or explicit conduct". Thus, the reference to "pornographic material" in the definition of "child pornography" seems circular. o There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose. o The provision requiring filters in places where the Internet can be accessed by the public is fairly uncommon in the SADC region.
Section 86: Prohibition of cyber harassment	It is an offence to use any computer system and continue - • making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or • threatening to inflict injury or physical harm to the person or property of any person; or • knowingly permitting any electronic communications device to be used for any of the abovementioned purposes. o Many of the key terms in this offence are not defined ("obscene, lewd, lascivious or indecent"). o The reference to continued acts indicates that cyber harassment requires repeated acts of the kind described. However, if this is correct, it should be made more clear. o The acts that constitute cyber harassment are narrower than in many other SADC cyberlaws, as there is no mention of insult or annoyance. Here, the harassment requires either suggestions of a sexual nature or threats of harm. The reference to "injury or physical harm" indicates that

[1002] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 24(2)(b) and (c).
[1003] Penal Code [*Chapter 7:01*], section 217A.

	psychological or emotional injury is covered by the word 'injury" - a point which should be clarified.
Section 87: Prohibition of offensive communication	It is an offence wilfully and repeatedly to use electronic communication to disturb or attempt to disturb the peace, quietness or right of privacy of any person with no purpose of legitimate communication. "Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quietness or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues, commits a misdemeanour and shall, upon conviction, be liable to a fine of K1,000,000 and to imprisonment for twelve months." o This has been identified as a provision "that public officials could exploit to punish critical speech by online journalists or internet users" [1004], or put another way. "To clamp down on dissenting voices."[1005] This provision has in fact been used against journalists in Malawi.[1006]
Section 88: Prohibition of cyber stalking	It is an offence to wilfully, maliciously, and repeatedly use electronic communication to harass another person *and* to make a threat with the intent to instil reasonable fear in that person for his or her safety or that of a member of his or her immediate family.[1007] o It is a limiting factor that this offence requires, not just vague "harassment" but also the making of threats with an intent to instil reasonable fear for personal safety. It is also a limiting factor that this form of harassment must take place repeatedly and maliciously.

While some of these offences might be used to restrict speech, it has also been reported that cyberbullying is being increasingly used as a tool to silence critics of the government, with online trolls using pseudonyms targeting columnists and journalists who are deemed to be too critical of the current government.[1008]

In general, **attempting, aiding or abetting any of the offences in the Act** – both technical and content-based – is also an offence.[1009]
The law's provisions on **encryption** have given rise to come concern. It requires providers of cryptography services or products to register with MACRA and to provide the regulator with "the technical characteristics of the encryption means as well as the source code of the software used".[1010] Freedom House notes that this provision potentially affects services with end-to-end encryption, such as WhatsApp.[1011] The

[1004] "Freedom on the Net 2022: Malawi". Freedom House, section C2.
[1005] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 29.
[1006] See, for example, "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020] and the case studies in section 10.3 of this chapter.
[1007] The wording on this point a somewhat ambiguous: "…makes a threat with the intent to instil reasonable fear in that person for his safety or *to a member of that person's immediate family*". It is not entirely clear if this refers to making *a similar threat to an immediate member of the family*, or making *a threat to a person that instils fear in that person for the safety of immediate family members*.
[1008] Teresa Temweka Chirwa-Ndanga, "New Access to Information Law Brings Hope" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), page 39.
[1009] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 93.
[1010] Id, sections 52 and 67 (quoted on the box in the text).
[1011] "Freedom on the Net 2022: Malawi". Freedom House, section C4.

result could be to compromise the privacy of those who engage in online communication, which in turn may inhibit freedom of expression.

ELECTRONIC TRANSACTIONS AND CYBER SECURITY ACT, 2016

52. Encryption

(1) A person shall not provide cryptograph services or products in Malawi without registration under this Part.

(2) Registration for provision of cryptograph services or products shall be made -
(a) to the Authority.
(b) in the prescribed manner and form; and
(c) upon payment of applicable fees.

(3) The Minister in consultation with the Authority shall issue regulations -
(a) in respect of use, importation and exportation of encryption programmes and encryption products; and
(b) prohibiting the exportation of encryption programmes or other encryption products from Malawi generally or subject to such restrictions as may be prescribed.

(4) For the avoidance of doubt, subject to any regulations made under sub regulation (1), it is lawful for any person to use encryption programme or product provided that it has lawfully come into possession of that person.

67. Provision of encryption services

(1) A person who provides encryption services shall declare to the Authority the technical characteristics of the encryption means as well as the source code of the software used.

(2) Regulations made under this Act shall define the conditions for making declarations referred to in subsection (1), and may define encryption services whose technical characteristics or conditions of supply are such that, with regard to national defence or internal security interests, their provision shall not require any prior formality.

(3) An encryption services provider shall be bound by professional secrecy.

(4) Unless it is proved that no intentional wrongful conduct or negligence was involved, a provider of encryption services for confidentiality purposes shall be liable, notwithstanding any contractual provision to the contrary, for the damage suffered by the persons that entrusted the management of their confidential conventions to them in case of violation of the integrity, confidentiality or availability of the data object of such convention.

Privacy is also implicated in the requirement that **online content providers must display on their website the full name, domicile, telephone number, and email address of the editor**. Legal entities that provide online content must display their corporate name, postal and physical address of their registered office, telephone number, email address, authorized share capital, and registration number, of the editor.[1012] Failure to display the required information is a criminal offence.[1013] This provision has been called "unworkable" since many platforms are operated by global entities that Malawi cannot regulate – such as, for example, a Facebook page that is not required under the Facebook platform rules to list the actual legal name of an individual or a corporate entity; "This kind of regulation of the internet is typical of authoritarian governments which hope to encourage self-censorship by creating an atmosphere that discourages freedom of expression."[1014] According to Freedom House, "[e]ven though the government does not actively enforce this provision, its presence in legislation undermines citizens' rights to privacy and anonymity and may encourage self-censorship".[1015]
Regarding enforcement of the Act, as noted above, MCERT has the power to appoint **cyber inspectors** whose powers include the following:

- to monitor and inspect any website database with critical data or activity on an information system in the public domain and report any unlawful activity to the Authority;
- to investigate the activities of suppliers of encryption and of encryption service providers
- to search premises and information systems under the authority of a search warrant
- the information system;
- to access and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is, or has been used in, connexion with the commission of any offence.

A cyber inspector may be accompanied by a police officer when carrying out these functions.[1016] **Search warrants** may be issued by a court on the application of a cyber inspector.[1017]

The Act includes a provision for **take-down notifications**. Any complainant may notify a service provider of "any content which is unlawful or infringes, or may infringe, on such person's rights". It is an offence to make a false notification, punishable by a fine of K1,000,000 and imprisonment for twelve months. The service provider is not liable for hosting or caching material that is promptly removed in response to such a notification – nor is the service provider liable for a takedown in response to a wrongful or false notification. As in most such systems, this approach mitigates in favour of

[1012] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 31(1).
[1013] Id, section 95.
[1014] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, page 376.
[1015] "Freedom on the Net 2022: Malawi". Freedom House, section C4.
[1016] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 70.
[1017] Id, section 83.

removal. However, the Malawi framework offers some helpful elements that are not commonly seen in the region:

- A service provider offering access to online public communication services must inform its subscribers of the existence of any technical means which permit restriction of access to certain services – ie filtering mechanisms.
- A service provider must set up "an easily accessible and visible system" for reporting content which is unlawful or infringes on a person's rights.
- A service provider must promptly inform MACRA of any illegal content reported to it by a member of the public and "make public the means taken to fight against the dissemination of such illegal content" – a requirement which would, in theory, enable MACRA to play a monitoring role.[1018]

B) OTHER LAWS THAT MAY IMPACT FREEDOM OF EXPRESSION

In 2023, the **Penal Code** was amended to repeal some crimes that previously impacted freedom of expression. This amendment removed the provisions of the Penal Code on **sedition** – which had previously criminalised speech and publications intended to incite hatred, contempt or disaffection against the President, the Government or the administration of justice; to inspire the public to try to alter any matter by unlawful means; to raise discontent or disaffection amongst citizens; or to promote feelings of ill-will and hostility between different classes of the population.[1019]

However, some provisions that remain are still problematic in respect of freedom of expression.

[1018] Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 30 read with sections 27-28. These requirements technically apply to the "intermediary service provider". which is the person or entity "that provides electronic communications services consisting of the provision of access to communications networks, storage, hosting or transmission of information through communication networks" (definition in section 2).

[1019] The Penal Code (Amendment) Act 8 of 2023 repealed sections 50-53 of the Penal Code [*Chapter 7:01*]. Note that sections 46-49 of the Penal Code, which previously prohibited the importation or re-publication of publications which the minister believed to be contrary to the public interest, were repealed by Act 24 of 2012. Penal Code [*Chapter 7:01*].

- Section 60 of the Penal Code criminalises **the publication of false information that is likely to cause fear and alarm to the public or to disturb public peace.**[1020] It has been observed that this provision is vague and fails to provide clear guidance, which gives an overly wide degree of discretion to those charged with the enforcement of this law.[1021] This crime has been used against individuals in practice in respect of online publications.[1022]
- Section 61 of the Penal Code makes the **defamation of foreign dignitaries** a misdemeanour, where this takes place with intent to disturb the peace and friendship between Malawi and the Republic and the country in question.

PENAL CODE

60. PUBLICATION OF FALSE NEWS LIKELY TO CAUSE FEAR AND ALARM TO THE PUBLIC

(1) Any person who publishes any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace shall be guilty of a misdemeanour.

(2) It shall be a defence to a charge under subsection (1) if the accused proves that, prior to publication, he took such measures to verify the accuracy of such statement, rumour or report as to lead him reasonably to believe that it was true.

- Section 88 of the Penal Code on the offence of **intimidation** covers, in addition to threats of personal harm or property damage, words that threaten another with any injury to his reputation or to the reputation of any other person where this is done with intent to cause alarm or to influence a person's actions. The offence applies to the publisher, editor or printer of any newspaper, pamphlet or other document containing any such threat. This offence is related to criminal libel.
- Section 130 of the Penal Code makes it an offence **to speak or write words with the intention of wounding religious feelings**. This offence also applies to sounds and gestures. However, it has been reported that this provision is not enforced.[1023]
- Section 181 of the Penal Code makes it an offence to publicly conduct oneself in a manner likely to cause a **breach of the peace**. This offence is so broad and vague that it could capture many forms of freedom of expression.

PENAL CODE

200. DEFINITION OF LIBEL

Any person who, by print, writing, painting, effigy, or by any means otherwise than solely by gestures, spoken words, or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, shall be guilty of the misdemeanour termed "libel".

- Section 182 of the Penal Code makes it an offence to use **insulting, abusive, indecent or threatening language** or otherwise conduct oneself in a manner likely to provoke any person to breach the peace. This offence's overbroad formulation makes it vulnerable to selection enforcement.
- Section 200 of the Penal Code concerns **criminal libel**. As has been discussed above, this provision is currently the subject of a constitutional challenge.[1024]

[1020] Penal Code [*Chapter 7:01*], section 60.
[1021] "LEXOTA Country Analysis: Malawi", last updated December 2022.
[1022] See section 10.3 of this chapter.
[1023] "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A.
[1024] See section 10.2 of this chapter.

Section 3 of the **Preservation of Public Security Act 11 of 1960** empowers the minister to make regulations that prohibit the publication and dissemination of any matter that appears to the minister to be "prejudicial to public security".[1025] **The Public Security Regulations** issued under this Act prohibit any person from publishing anything likely to prejudice public security, undermine public confidence in the Government, promote a feeling of ill-will or hostility between any sections or classes or races of people in Malawi, or promote industrial unrest.[1026] One commentary states that the "vague construction of this law fails to provide sufficient guidance to individuals and gives an overly wide degree of discretion to those charged with the enforcement of this law."[1027] Another analysis states that the criteria for this prohibition given are based on opinion rather than being objective, making this provision inconsistent with international best practice.[1028]

Section 4 of the **Protected Flag, Emblems and Names Act** makes it an offence to do any act, utter any words or publish any writing "calculated to or liable to insult, ridicule or to show disrespect to" the President, the National Flag or other specified national emblems.[1029]

Section 83 of the **Prisons Act** makes it an offence to publish in whole or in part a letter or document written by a prisoner which has not been endorsed by a prison officer.[1030] This could obviously inhibit the exposure of abuse of prisoners or prison conditions.

C) SIM CARD REGISTRATION

The **Communications Act 34 of 2016** requires registration of "generic numbers" and SIM cards. Individual subscribers must provide their full names, identity card (or other document proving identity), and residential or business address. Legal entities must provide a certificate of registration or incorporation; a business licence; and, where applicable, a taxpayer identification certificate number.[1031] In terms of the Communications (SIM Card Registration) Regulations, 2023, the service provider must confirm the subscriber's identity by means of fingerprint verification with the National Registration Bureau, and must keep subscribers' records based on the details electronically retrieved from the National Registration Bureau. Registrations by companies and institutions are verified against the fingerprint of a representative of the entity.[1032] This removes the ability to communicate anonymously via mobile phones.[1033]

[1025] Preservation of Public Security Act 11 of 1960 section 3(2)(a).
[1026] The Public Security Regulations (reproduced below the text of the act on this website), regulation 4 read with regulation 14.
[1027] "LEXOTA Country Analysis: Malawi", last updated December 2022.
[1028] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 284-285.
[1029] Protected Flag, Emblems and Names Act [*Chapter 18:03*], section 4.
[1030] Prisons Act [Chapter 9:02], section 83(3)-(4).
[1031] Communications Act 34 of 2016 [*Chapter 68:01*], section 92.
[1032] Communications (SIM Card Registration) Regulations, 2023, regulation 5.There are additional details for other categories of registrations, including minors, foreigners, refugees and diplomatic institutions.
[1033] Freedom on the Net 2022: Malawi". Freedom House, section C4.

D) STATE SURVEILLANCE

No legal authority for interception of communications by government or law enforcement officers was located, nor any authority for the retention of traffic data by service providers for access by government authorities – but there are indications that state monitoring of communications takes place in practice, as evidenced by arrests related to online activities.[1034]

Freedom House reports:

> *Government surveillance of ICT activities is strongly suspected in Malawi, particularly in light of the regulatory authority's January 2018 implementation of the Consolidated ICT Regulatory Management System (CIRMS), which is known locally as the "spy machine". […] MACRA described the system as a tool for monitoring the performance of mobile phone companies and improving the quality of service. However, news reports said that the system would also allow MACRA—without judicial oversight—to obtain data from telephone operators, including the time, duration, and location of calls; short-message service (SMS) messages sent and received; the type of handset used; and other subscriber details.*[1035]

In one 2011 commercial court case,[1036] a telecommunications subscriber complained about a violation of privacy after MACRA issued a directive to four telecommunication providers to provide it with information about who called which number; details of calls received; time and duration of calls; the location where the call was made or received; SMSs sent and received; type of handset used and other detailed subscriber information. The telecommunication companies (Access Malawi Limited, Airtel Malawi Limited, Telekom Networks Malawi Limited and Malawi Telecommunications Limited) initially raised concerns that this directive violated the constitutional right to privacy, but eventually acquiesced to the request. The Court found that providing the information did indeed violate the right to privacy, which can only be limited by law where the limitation is reasonable, recognized by international human rights standards and necessary in a democratic society. The Court also emphasised that "a limitation does not become legal merely because it comes from MACRA or any other regulatory body.[1037]

E) TAKE-DOWN NOTIFICATION

This is discussed above since it is contained in the combined **Electronic Transactions and Cyber Security Act 33 of 2016**.

[1034] Personal communications, July 2023.
[1035] Id, section C5 (references omitted).
[1036] *Kimu v Access Malawi Limited and Others* (Commercial Case No. 54 of 2011) [2012] MWComm C1 (02 May 2012).This judgment could not be located online.
[1037] Case description and quotes as reported in Jimmy Kainja, "Mapping Digital Surveillance and Privacy Concerns in Malawi", Media Policy and Democracy Project, November 2021, pages 9-10; "Navigating Litigation During Internet Shutdowns In Southern Africa", Southern Africa Litigation Centre, June 2019, pages 47-49.

CHAPTER 11

MAURITIUS

CHAPTER 11: MAURITIUS

MAURITIUS KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **63rd globally; 10th out of 48 African countries** "Mauritius may be hailed as one of Africa's model democracies, but its media landscape is highly polarised. Online attacks against journalists have increased."
MALABO CONVENTION: Party
BUDAPEST CONVENTION: Party since 2013; Mauritius was the first African country to accede to the Convention
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Mauritius's 1968 Constitution, revised 2016 Amendments made since 2016 do not affect Article 12. **12. PROTECTION OF FREEDOM OF EXPRESSION** 1. Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence. 2. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision. a. in the interests of defence, public safety, public order, public morality or public health. b. for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting, television, public exhibitions or public entertainments; or c. for the imposition of restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.[1038]

[1038] The placement of the last clause of Article 12(2) is crucial to the Article's meaning. The 1968 Constitution published by constitute.org (which is hyperlinked here because it is updated to 2016) joins this clause to paragraph c, as does the 1968 Constitution published by the Mauritius Director of Public Prosecutions. This placement is supported by Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 9: Mauritius", Konrad Adenauer Stiftung, 2021, page 9.

However, the 1968 Constitution published by the Attorney-General of Mauritius places this clause *below* paragraph c, *which makes it applicable to paragraphs a-c and not just to paragraph c*. This placement of the clause is supported by Geoffrey Robertson QC, "Media Law and Ethics in Mauritius: Preliminary Report", 2013, paragraph 24. It is also the version found in Amos Jenkins Peaslee and Dorothy Peaslee Xydis, *Constitutions of Nations: Volume I, Africa*, Brill, 1974, page 525. It is also how the provision is quoted in the 1999 Privy Council case of *Gilbert Ahnee v The Director of Public Prosecutions*.

KEY LAWS: • Cybersecurity and Cybercrime Act 16 of 2021 (which replaced the Computer Misuse and Cybercrime Act 22 of 2003) • Information and Communication Technologies Act 44 of 2001 • Criminal Code (selected provisions)
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: Mauritius has a law on data protection.[1039]
ACCESS TO INFORMATION: Mauritius does not have a law on access to information, although this has been a topic of discussion and debate for some years now.[1040]

11.1 CONTEXT

Reporters Without Borders provides this overview in this 2023 World Press Freedom Index:

> *The media scene in Mauritius consists of two very distinct sectors. On the one hand, there are highly politicised media, including the national radio and TV broadcaster and other pro-government media, which are often guilty of propagandising, and media that supports the opposition, which are at risk of being sidelined by the government. On the other hand, there are media outlets that are very outspoken but sometimes veer towards sensationalism and undermine the quality of their reporting. Independent, serious and reliable media struggle to find a place in this landscape.*
>
> *The government has total control over the Mauritius Broadcasting Corporation (MBC), whose director general is appointed by the prime minister.*
>
> *The media regulator's lack of independence does not help foster quality journalism. Its sanctions very often target pro-opposition media outlets, as in December 2020, when it banned a radio station from broadcasting for 72 hours after a unionist called Indian Prime Minister Narendra Modi a "racist" on the air.*[1041]

Turning to the legal framework, the **Newspapers and Periodicals Act 6 of 1837** makes it an offence to print or publish a newspaper or a periodical that is "devoted in whole or in part to news or politics" without first depositing a notice with the Accountant-General specifying its title, the physical locations of the printer and publisher, the

The original publication is in the Schedule to the "Mauritius Independence Order 1968" published in Mauritius Government Notice No. 54 of 1968, which could not be located online.

The latter placement seems to be correct, based on the balance of sources, as well as being the version that ties in best grammatically with the reference to "provision" in the opening clause of Article 12(2). This placement of the closing clause is the one reproduced here.

[1039] Data Protection Act 20 of 2017. This Act came into force in 15 January 2018, replacing the Data Protection Act 2004. "Mauritius: Cybercrime policies/strategies", Octopus Cybercrime Community, Council of Europe, undated.

[1040] See Chelvin Ramsamy, "A Long-Awaited Freedom of Information Act for Mauritius. But When?", blog post on Friedrich Ebert Stiftung website, 6 January 2023.

[1041] "2023 World Press Freedom Index: Mauritius", "Media landscape" and "Political Context".

names and addresses of the printer, the editor and one of the principal proprietors who resides in Mauritius, and the extent of their interests in the publication. This law also requires that an imprint with the names and addresses of the printer and editor must appear on every issue.[1042]

There is a broad **right of reply that applies specifically to newspapers** in the **Criminal Code**. Any person named or referred to in a newspaper has the right to reply on the topic in connection with which they were mentioned, This reply is free of charge and must be published in the same place and the same type as the original article. It can be up to twice the length of the original article – and longer, if the person replying pays for the excess at normal advertising rates. The newspaper owner or editor can be criminally fined for failure to afford this right of reply, as well as being ordered to insert the reply.[1043]

Radio and television are regulated by the **Independent Broadcasting Authority Act 29 of 2000**. This law establishes the **Independent Broadcasting Authority (IBA)** which has regulatory functions and powers that include licencing, setting standards for programmes and advertising, considering public complaints and taking "any action it thinks appropriate", and ensuring that broadcasting services do not "encourage or incite crime or racial hatred leading to disorder or offending public feeling".[1044]

The Chairperson of the IBA Board is appointed by the President after consultation with the Prime Minister and the Leader of the Opposition. There are five other members who represent various government agencies, and three to five members appointed by the minister on the basis of their expertise in the field.[1045] The Board appoints the Director who services as the chief executive officer.[1046] The Act states that the IBA is not subject to the control of any person, body or authority in the exercise of its functions – but it also states that the minister may issue such directions to the IBA in relation to "national security and public order", and the IBA must comply with those directions.[1047]

[1042] Newspapers and Periodicals Act [*Cap 37*].
[1043] Criminal Code amended to 2006, section 289. The amendments made to the Criminal Code after the date of this consolidated copy do not affect this section.
[1044] Independent Broadcasting Authority Act 29 of 2000. This version of the Act includes amendments made through December 2021.
[1045] Id, section 6.
[1046] Id, section 11.
[1047] Id, section 3.

THE **CODE OF CONDUCT FOR BROADCASTING SERVICES**

Appears as the Second Schedule to the Independent Broadcasting Authority Act 29 of 2000, while the **Code of Ethics**, dated 2011, can be found here. Both deal with sensitivity to public morals, privacy and the need to be impartial, accurate and objective when reporting news, amongst other things. The Code of Ethics also gives guidelines on journalistic news-gathering techniques such as doorstepping, telephone interviews, and the need for sensitivity when reporting on personal tragedies.

The Act prohibits the issue of a broadcasting licence to any political party or association or any person actively engaged in politics, or to any religious group.[1048] Persons who have been "found liable for defamation or sedition" are also prohibited from being issued with a broadcasting licence.[1049] Internet service providers who are licenced under the Information and Communication Technologies Act (discussed below) can also be licenced under this Act for television broadcasting or rebroadcasting services.[1050] The 2021 amendments reduced the licence period for radio broadcasters from 3 years to 1 year, while leaving the 5-year period for television broadcasting licences unchanged – and the amendments require the IBA to take into account past conduct, any pending judicial processes and any sanction imposed by it on a licensee in the course of considering an application for renewal.[1051] Some believe that these 2021 amendments targeted a specific private radio station that regularly broadcasts content critical of the ruling party, to enable a report to non-renewal of its licence is a form of punishment for having exposed government wrongdoing.[1052] The 2021 amendments also removed previous provisions for community radio or TV licences which were considerably cheaper than commercial licences.[1053]

The IBA has broad powers to issue regulations for the broadcasting sector,[1054] including a Code of Ethics, a Code of Advertising Practice and other Codes "as it may determine".[1055] A requirement of public consultation in respect of these Codes was removed by the 2021 amendments.[1056] The IBA also has the power to suspend or revoke licences for violations of laws and regulations and discretionary power to do this whenever "it is in the public interest to do so".[1057]

A controversial aspect of the 2021 amendments to the law was the introduction of administrative penalties that can be imposed on licensees by the IBA after disciplinary proceedings before the IBA if there is reason to believe that a licensee has contravened the Act, the regulations, the Codes, or a licence condition, has failed to

[1048] Id, section 19(3)(c)-(e).
[1049] Id, section 19(3)(g).
[1050] Id, section 19(3B).
[1051] Id, section 22.
[1052] Ambareen Beebeejaun, "Media Regulation in Mauritius: A Critical Analysis" in David Crowther and Shahla Seifi, *Preparing for a Sustainable Future*, Springer, 2023, page 55 (reference omitted); Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.
[1053] Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.
[1054] Independent Broadcasting Authority Act 29 of 2000, section 38.
[1055] Id, section 6(6).
[1056] Ambareen Beebeejaun, "Media Regulation in Mauritius: A Critical Analysis" in David Crowther and Shahla Seifi, *Preparing for a Sustainable Future*, Springer, 2023, page 54.
[1057] Independent Broadcasting Authority Act 29 of 2000, sections 24-25.

comply with any other laws of Mauritius; or is not a fit and proper person for holding a licence, amongst other grounds. There is a right to appeal to a three-person Independent Broadcasting Review Panel appointed by the Minister, which has the discretionary power to hold its hearings in private. An administrative penalty may not exceed 500,000 rupees.[1058] This is a five-fold increase over the previous maximum fines.[1059]

One particularly controversial provision that was added to this Act in 2021 allows a Judge in Chambers to require journalists to reveal their sources or "produce any record, document or article where this is needed for the IBA's exercise of its regulatory powers on the basis of an *ex parte* application (where the journalist is not involved).[1060] This jeopardises the confidentiality of journalists' sources without any legal safeguards.[1061] A Senior Lecturer in Media and Communication at the University of Mauritius made the following observations about this new provision:

> *This is against journalistic standards that require utmost respect for the confidentiality of their sources. […] Hopefully our judges will resist any frivolous requests and consider only very exceptional circumstances such as if our national security is at stake (which has never happened so far to our knowledge). Nonetheless, such a provision constitutes a red flag for journalists and potential whistleblowers. In other words, a chilling effect! It will require strong will and commitment for journalists to engage in serious investigative work despite the looming threat of a potential order to disclose their raw documentary sources, leading to self-censorship. It will be even more difficult for them to promise the utmost protection of anonymity to their sources as the latter may fear to be identified through the journalists' raw documents.*
>
> *There has been much discussion about the fact that the application to a Judge in Chambers would be made ex parte, that is, done by and for only one party (here the IBA) such that the journalists would not necessarily be able to defend their case against granting of the application. The PM [Prime Minister] has stated that the Judge in Chambers may actually call journalists to counter argue and that they should be trusted to assess requests in all fairness. This seems to be a valid point.*
>
> *However, even if journalists were indeed called by the Judge in Chambers to explain why the application should not be granted, this process still puts the burden on them for proving why the anonymity of sources should be protected, which appears to be in contradiction with Article 10 of the European Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights […].*[1062]

[1058] Id, sections 29-30L.
[1059] "Mauritian parliament imposes tougher regulations on broadcast media", Reporters Without Borders, 1 December 2021.
[1060] Independent Broadcasting Authority Act 29 of 2000, section 18A.
[1061] "Mauritian parliament imposes tougher regulations on broadcast media", Reporters Without Borders, 1 December 2021.
[1062] Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.

Information and communication technologies are regulated under the **Information and Communication Technologies Act 44 of 2001**.[1063] This Act establishes an **Information and Communication Technologies Authority (ICT Authority or ICTA)** as the licensing and regulatory body for the information and communication services.[1064] Amongst its many functions are:

- to advise on national policies on ICT;
- to exercise licensing and regulatory functions, including authorisation, approval or clearance of information and communication services in Mauritius, including the determination of types and classes of licences and tariffs;
- to regulate the registration of SIM cards;
- to take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services;
- entertain complaints from consumers in relation to any information and communication service in Mauritius and, where necessary, refer them to the appropriate authorities;
- control the importation of any equipment capable of being used to intercept a message;
- determine which facilities are essential facilities.[1065]

The ICTA is governed by a Board headed by a chairperson appointed by the Prime Minister after consultation with the Leader of the Opposition. The Board includes the Chairperson of the IBA and 4 other members representing specific government bodies, as well as 4 other members appointed by the relevant minister.[1066] The Board appoints the Executive Director, with the approval of the minister.[1067]

The Act provides for an **ICT Appeal Tribunal** to decide appeals against decisions of the Authority regarding information and communication technologies.[1068] After consultation with the Board, the minister must also appoint an **Internet Management Committee**, which advises the ICT Authority on Internet and related policies, provides a forum for stakeholders to discuss issues relating to the administration of the Internet and administers domain names.[1069] The Act also establishes a **ICT Advisory Council**, made up primarily of ministerial representatives and ministerial appointees, which advises the minister on a range of ICT issues.[1070]

The Centre for Law and Democracy takes the view that the key bodies established under the Act are not adequately independent:

[1063] Information and Communication Technologies Act 44 of 2001 (as amended to December 2021). The most recent amendments to the Act are contained in section 5 of The Judicial and Legal Provisions (No. 2) Act 14 of 2018 and section 39 of The Finance (Miscellaneous Provisions) Act 15 of 2021. For purposes of comparison, the Act as it stood prior to these two amending laws can be found here and here.
[1064] Information and Communication Technologies Act 44 of 2001, section 16.
[1065] Id, section 18(d), (f), (j), (m), (o), (u), and (aa).
[1066] Information and Communication Technologies Act 44 of 2001, section 5.
[1067] Id, section 14.
[1068] Id, sections 36 and 39.
[1069] Id, sections 12-13.
[1070] Id, sections 34-35.

It is a key international law standard regarding media freedom that any bodies that exercise regulatory powers over the media should be independent of political actors. The main reason for this is fairly obvious; if a regulator is controlled by a political actor, it will make decisions which favour that actor rather than in the public interest. It is still appropriate for government to set general policy directions but specific regulatory decisions which affect individual media outlets, such as licensing and deciding upon complaints, need to be taken by an independent body. […]

The two regulatory bodies under the ICT Act – the ICTA and the Tribunal – are not adequately protected against political interference, or in other words are not sufficiently independent – to meet international standards in this area. As a preliminary point, the ICT Act lacks any general provision indicating that the regulatory bodies it creates are independent. Such provisions are good practice because they set the tone for the rules, as well as the culture of regulatory bodies. Also, in the event of litigation that involves the ICT Act, such provisions provide guidance to the court on the importance of interpreting the law so as to safeguard the independence of those bodies. In terms of specific provisions, government control over the ICTA is the starkest in section 19, which authorises the minister to give binding "directions of a general character" to the ICTA's board that are not inconsistent with the objects of the ICTA if the minister believes it is in the "public interest" to do so. This grants the minister very broad discretion to give orders to the board. While it is not inappropriate, as noted above, for the government to set policy, this power goes far beyond that.

A keyway of guaranteeing the independence of regulatory bodies is through the membership of the board and the manner in which members are appointed, by insulating this from political, commercial or other types of influence. The appointments process for the ICTA Board falls well short of international standards in this regard because the process is largely controlled by the government. According to section 5(3) of the ICT Act, the Chair of the board is appointed by the Prime Minister after "consultation" with the leader of the opposition, four of the other nine members are representatives of different ministries, while the remaining four are appointed directly by the minister. This effectively gives the government full control over the board with the only minor qualification on this being the requirement to consult with the leader of the opposition in relation to the chair. This control does not end with the board. Highly exceptionally, the board may only appoint the executive director with the approval of the minister (section 14(1)(b)). This drives political control right into the core work of the ICTA without any justification whatsoever.

Better practice would be to involve a much wider range of actors in the process. Members of civil society, academia and other non-governmental actors should, for example, be given the power to nominate members while a multiparty body such as parliament or a committee thereof should also play a role, for example by appointing members or confirming nominations.[1071]

The Centre for Law and Democracy has also criticised the law's overly broad approach to licensing, with licences being required for "any service involving the use of information and communication technologies including telecommunication

[1071] "Note on Mauritius' Information and Communication Technologies Act 2001", Centre for Law and Democracy, May 2021, pages 3-4 (hereinafter "Centre for Law and Democracy Note on the ICT Act", May 2021).

services"[1072] - noting that this would impose licensing requirements on any online service, such as an online booking system for a hairdresser. The Centre states that the law should utilise licensing only where important public policy issues are involved, such as management of a frequency spectrum, ensuring competition or promoting diversity within an industry, with no licencing requirements for Internet services unless such issues come into play.[1073] The Centre also points to the problem of vague conditions for licences, such as requiring the ICTA to into account "the public interest and the likelihood of unfair practice" and "any element of national security".[1074] These criteria leave give the ICTA too much discretion to deny licences.[1075]

The Act includes a number of technical and content-based cybercrimes, which will be discussed below.[1076] It also provides for a magistrate to issue warrant to authorised officers of the ICTA to carry out searches and seizures whenever there is a reasonable ground to suspect that a person is contravening the Act, or the regulations made under it.[1077]

The ICTA states that it is currently in the process of "consolidating regulation across sectors that are converging, such as telecommunications, broadcasting and IT".[1078] However, in November 2020, the government backtracked on a plan to merge the IBA and the ICTA.[1079]

As part of its duty to curtail harmful and illegal internet content, in 2011 the ICTA implemented a central filtering system that blocks access to child sexual abuse sites for all Internet users in Mauritius. According to the ICTA, Mauritius is the first African country to implement such an approach.[1080]

A few years ago, the government tasked the Law Reform Commission to propose a way to address the problem of fake news on social media. The Law Reform Commission's response was that -

> *the main danger in enacting such legislation is that it poses a threat to freedom of expression, as it can be used, among other things, to gag dissenting voices. Indeed, decreeing a legal duty of 'truth' would create a dangerous instrument to control journalistic activities allowing public officials to decide what amounts to truth is equivalent to accepting that the forces in power have a right to silence views they disagree with, or beliefs they do not share. Such laws can preclude the discussion of ideas which challenge the norm, restraining public debate and restricting criticism of societal attitudes or of those in power. Under such laws, journalists or human rights*

[1072] Information and Communication Technologies Act 44 of 2001, section 20(1).
[1073] "Centre for Law and Democracy Note on the ICT Act", May 2021, page 7.
[1074] Information and Communication Technologies Act 44 of 2001, section 24(5)(a)-(b).
[1075] "Centre for Law and Democracy Note on the ICT Act", May 2021, page 8.
[1076] Id, section 46.
[1077] Id, section 25.
[1078] ICTA website, "Internet: Overview", 2023.
[1079] Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
[1080] ICTA website, "CSA filtering", 2023.

> *activists could be sent to prison on accusations of disseminating untrue statements about alleged wrongdoings.*[1081]

Yet the Act as it stood in 2016 already made it an offence to send "false or misleading" messages.[1082] Then the 2018 amendments actually tightened control over social media messages. Prior to the 2018 amendments, the Act made it an offence to use telecommunication equipment –

- to send messages that are obscene, indecent, abusive, threatening, false or misleading, or *likely to cause distress or anxiety* (section 46(ga)); or
- *for the purpose of* causing annoyance, inconvenience or needless anxiety to any person (section 46(h)(ii)).[1083]

The 2018 amendments made it an offence to use telecommunication equipment –

- to send messages that are obscene, indecent, abusive, threatening, false or misleading, or *likely to cause annoyance, humiliation, inconvenience, distress or anxiety to any person* (section 46(ga)); or
- in a way that is *likely to cause annoyance, humiliation, inconvenience, distress or anxiety* (regardless of intention) (section 46(h)(ii)).[1084]

In short, prior to 2018, the offence required to prove that a person was in fact inconvenienced or annoyed by a message on social media and that the person sending the message did so for that purpose; after the 2018 amendments, one can commit the offence of annoying or inconveniencing someone without even having the intention to do so.[1085]

Then, in May 2021, in the *Seegum* case, the Supreme Court, considering a prosecution under section 46(h)(ii) for Facebook posts uploaded in 2012, found that the *pre-2018* version of that section was unconstitutionally vague due to its use of the broad and undefined term "*causing annoyance*", which did not give sufficiently clear guidance on what conduct was prohibited. The Attorney General reacted to the *Seegum* case by releasing a statement asserting that the case did not affect the amended version of the law[1086] – although the 2018 amendments actually added new broad and undefined terms to section 46(h)(ii): "*humiliation*" and "*distress*".[1087]

[1081] As quoted in Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
[1082] This is covered by all the versions of section 46(ga) – as it stood before the 2018 amendments, after the 2018 amendments and after the 2021 amendments.
[1083] The Act as it stood prior to the 2018 and 2021 amendments can be found here and here. See section 46(ga) and (h)(ii).
[1084] See the amendments made by The Judicial and Legal Provisions (No. 2) Act 14 of 2018, section 5.
[1085] Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021.
[1086] The judges said in the *Seegum* case that "we are not hereby making any pronouncement as to the constitutionality of the new redrafted section 46 (h)(ii), as amended by Act No 14 of 2018", as quoted in ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021.Note that section 46(ga) was not at issue in the *Seegum* case.
[1087] *Seegum J v The State of Mauritius* 2021 SCJ 162, as summarised here by Denton's, the law firm that represented the appellant, on 1 June 2021; Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021; Jillian C York, "Amendments to Mauritius' ICT Act Pose Risks for Freedom of Expression", Electronic Frontier foundation, 6 December 2018.

After the *Seegum* judgment, the Act was once again amended, with section 48(h) being entirely repealed and section 46(ga) being replaced, so as to now make it an offence to use telecommunications or ICT technologies to communicate a message that is –

> *"Obscene, indecent, offensive, abusive, threatening, menacing, false or misleading, which is likely to cause or causes harm to a person".*[1088]

The undefined terms in this version still leave something to be desired. The addition of causing harm or being likely to cause harm could be viewed as helping to narrow the offence somewhat, particularly since the provision now provides a list of factors to consider in assessing whether harm has occurred - although the law does not fully define "harm" other than to say that it "includes serious emotional distress".[1089] Furthermore, this provision fails to require any *intent* to cause harm by the offending content.

In another 2021 development, the ICTA put forward controversial proposals aimed at social media. It released a document proposing a system whereby all social media traffic to and from Mauritius would be to be routed through a central proxy server run by the ICTA. The ICTA would establish systems to break any encryption provided by social media platforms and conduct official surveillance of all of this traffic with data analysis software to enforce content restrictions in the ICT Act. It proposed a National Digital Ethics Committee with powers to block offending social media content and "fake profiles".[1090] According to one press report: "After a firestorm of criticism from the public, global media giants such as Mozilla, Google and Facebook and even the Mauritius Banker's Association that warned of the potential of compromising the secrecy of internet banking transactions, the government dropped the proposals in the document."[1091]

The state broadcaster is the **Mauritius Broadcasting Corporation (MBC)** which is governed by the **Mauritius Broadcasting Corporation Act 22 of 1982**. Its seven-member Board consists of a chairperson appointed by the relevant minister, two *ex officio* government officials, and four other members appointed by the minister.[1092] Amongst MBC's duties are:

- to ensure that its broadcasting programmes do not offend against "decency, good taste or public morality" or encourage crime, disorder or violence.
- to strike a fair balance in the allocation of broadcasting hours among various educational, cultural, political and religious standpoints; and

[1088] Information and Communication Technologies Act 44 of 2001, section 46(1)(ga).
[1089] Id, section 46(2)-(3).
[1090] "Comments on Proposed Amendments to the Mauritian Information and Communications Technologies Act", Centre for Law and Democracy, May 2021; "Mauritius: Proposals to Monitor and Control All Social Media Traffic Very Repressive" Centre for Law and Democracy, 12 May 2021; Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
[1091] Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit*, 1 June 2021.
[1092] Mauritius Broadcasting Corporation Act 22 of 1982, section 6.

- to observe neutrality and impartiality on current affairs, matters of public policy and controversial matters relating to culture, politics, religion or any other subject aside from broadcasting.[1093]

The Act includes a potential **right of reply** in respect of any person who alleges that his honour, character, reputation or goodwill has been adversely affected by any matter broadcast by the MBC. Corporation. The aggrieved person must make a written application for a right of reply within 5 days of the broadcast. *If the Board is satisfied* that the honour, character, reputation or goodwill of the applicant has indeed been adversely affected, it must grant a right of reply *on such terms and conditions as it thinks fit*.[1094] This approach clearly involves a great deal of discretion on the part of MBC.[1095]

The **Media Trust Act 9 of 1994**, which receives government funding, creates a Media Trust tasked with running a media and documentation centre, organising seminars, conferences, workshops and training courses, and fostering relationships with international media. This law defines "media" to mean print and broadcast media (newspaper, periodical, television and radio).[1096]

The Media Trust is complemented by the government-funded Mauritius Digital Promotion Agency established by the **Mauritius Digital Promotion Agency** Act 4 of 2023 to boost the growth of the ICT sector through skills development and innovation; achieve basic ICT proficiency among all population groups; and advise the Minister on the formulation of national policies in respect of the promotion, development of ICT and its application. (This Act does not refer to online media specifically.)[1097]
Mauritius has no self-regulating body for the media.[1098]

11.2 CONSTITUTION

The constitutional right to freedom of expression in article 12 (quoted in the table on the first page of this chapter) has several threads - the right to both receive and impart ideas and information without interference, and protection for privacy of correspondence. The Supreme Court of Mauritius has held that this right also encompasses freedom of the press.[1099]

The wording of the limitations clause has been criticised for requiring that any restrictions must be "*reasonably justifiable*" in a democratic society; as opposed to applying the more stringent standard that they must be "*necessary*" in a democratic society, on the theory that the more stringent wording would reflect the modern view

[1093] Id, section 4(d), (f) and (g).
[1094] Id, section 19.
[1095] The right of reply in respect of newspapers in the Criminal Code, section 289 (discussed above), has considerably more teeth.
[1096] Media Trust Act 9 of 1994, sections 2-4.
[1097] Mauritius Digital Promotion Agency Act 4 of 2023, sections 3-4 and 20.
[1098] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 9: Mauritius", Konrad Adenauer Stiftung, 2021, page 64.
[1099] *Duval v The Commissioner of Police* 1974 MR 130.

"that freedom of speech is a fundamental value and should only be overridden in response to a pressing social need".[1100]

However, this seems to be how the Mauritian courts have applied the constitutional wording. In the 1992 case of *DPP v Boodhoo*, the Supreme Court discussed the permissible limitations to freedom of expression:

> *These limitations are incorporated in express terms in section 12(2)(a), (b) and (c) of our Constitution which sets out the specific aims of those limitations, but which subjects those limitations themselves to the governing norm of what is reasonably justifiable in a democratic society. The necessity for any constitutionally permissible limitations must [...] be narrowly construed and must respond to what has generally been understood to be a "pressing social need". Thus, the application in practice of limitations which are permissible in principle must be closely monitored so as to ensure that they stay, in any particular case, within the limits proportionate to the legitimate aim pursued.*[1101]

One of the leading cases on the constitutional right to freedom of expression is the 1999 case of ***Ahnee v The Director of Public Prosecutions***.[1102] In this case, an article in the newspaper *Le Mauricien* questioned the impartiality of the Chief Justice of the Supreme Court and alleged that two other Supreme Court justices would be hearing a case in which they would also be witnesses. Mr Ahnee, the writer of the article, and Mr Grimaud, the reporter who had actually attended the hearing, were both found guilty of contempt ("scandalising the court"). Mr Ahnee conceded that the allegations that were printed were factually wrong, but argued before the Judicial Committee of the Privy Council that the offence of scandalising the court violated the constitutional right to freedom of expression, as well as being legally faulty on several other grounds. The Judicial Committee of the Privy Council stated:

> *Given that freedom of expression is the lifeblood of democracy, this is an important issue. And there is no doubt that there is a tension between freedom of expression and the offence of scandalising the court. But the guarantee of freedom of expression is subject to qualification in respect of provision under any law (1) "for the purpose of … maintaining the authority and independence of the courts" and (2) shown to be "reasonably justifiable in a democratic society".*[1103]

In considering whether the offence met this test, it was noted that the offence is narrowly defined, being applicable only to comment on the conduct of a judge in relation to the judge's performance on the bench and thus "exists solely to protect the administration of justice rather than the feelings of judges". The charge is applied

[1100] Geoffrey Robertson QC, "Media Law and Ethics in Mauritius: Preliminary Report", 2013, paragraph 24. No final version of the report was ever published. Christina Chan-Meetoo, "On the subject of Media Regulation in Mauritius", 24 November 2021.
[1101] *DPP v Boodhoo* (1992) MR 284, as quoted in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 3.
[1102] *Gilbert Ahnee & Ors v The Director of Public Prosecutions (Privy Council)* (1999) MR 208 (Judgment of the Lords of the Judicial Committee of the Privy Council, 17 March 1999.
[1103] Id, discussion in the judgment of issue 2(a).

only where there is "a real risk of undermining public confidence in the administration of justice". It is also narrowed by the need in a democratic society "for public scrutiny of the conduct of judges, and for the right of citizens to comment on matters of public concern"; one of the defences to the charge is the right to criticise, in good faith, a public act done in the seat of justice. For example, the exposure of judicial misconduct would be in the public interest and would not result in a conviction. So, given the narrow scope of the offence of scandalising the court, it was held to be an acceptable basis for limiting the constitutional right to freedom of expression.[1104]

In the 2013 ***Soornack*** case, the Supreme Court considered the balance between the right to privacy and the right to freedom of expression in a request for an injunction against future newspaper publications about the private life of a businesswoman who was also a political activist and her family. The publications companioned of alleged that the woman had, apparently through her intimate connections with a high-profile politician, obtained financial favours from state-controlled agencies. The Court considered that was no chance that she would succeed in getting a perpetual injunction against future publications about her business and private life. Mindful of the impact of prior restraints on freedom of the press, the court took the view that harassment or defamatory and insulting remarks should be compensated by damages, if proved, rather than supporting a broad prohibition on future publication. The Court was however, prepared to restrict future publication about the woman's minor child which had no relation to the public debates under discussion.[1105]

The 2021 *Seegum* case has been discussed above. It relied primarily on the principle of legality to find a content prohibition in the Information and Communication Technologies Act 44 of 2001 unconstitutionally vague. However, it also made the following comments on freedom of expression in the digital age:

> *We are fully alive to the fact that, with the advent of information and communication technology and its rapid growth, it has become a challenge to regulate communications on the internet and especially on social media platforms. The ease with which material may be published online, or shared via social networks has brought into sharp focus the abuse of the right to communicate freely on the internet and on social media platforms. Although our Constitution protects the right to freedom of expression, it does not mean that it gives carte blanche for the transmission of communications which contravene the basic standards of our society; a person may obviously exercise his right to communicate freely on the internet and on social media platforms, but in so doing he should ensure that he is in no way infringing the rights of others. Just as in the offline world a person cannot insult or defame others with impunity under the guise of exercising his right to freedom of expression, in the online context too there are certain parameters which need to be respected. It is of utmost importance that those parameters be clearly defined, the more so when those parameters are meant to restrict freedom of expression.*
>
> *It is undeniable that a number of challenges have been posed on the existing criminal law by the exponential growth of online communication and we certainly agree that it*

[1104] Id.

[1105] *Soornack Nandanee v Le Mauricien Ltd & Ors* 2013 SCJ 58. The *Ahnee* and *Soornack* cases were identified by the government as being particularly significant cases on Article 12 of the Constitution in the media context. "General Assembly Resolution 72/175 on 'The safety of journalists and the issue of impunity': Inputs of the Government of Mauritius", undated. paragraph 4

> *is imperative that those who make an abuse of their right to freedom of expression be taken to task by subjecting them to appropriate legislation enacted for that purpose. Although the legislator may […] have been actuated by the laudable goal of addressing abusive and offensive online communications, he should have ensured that the said section which is a criminal provision has the quality of predictability and certainty, the more so when it limits the right to freedom of expression. Nor, dare we say, should the said provision have been drafted so as to criminalize online conduct when such conduct is perfectly legal in the offline world.*[1106]

The Mauritian courts have been asked on several other occasions to consider the constitutionality of several offences that have the potential to restrict freedom of speech. These will be discussed below.

11.3 CASE STUDIES

According to Reporter Without Borders: "Threats and acts of intimidation against journalists have increased, after being relatively rare in recent years. At least four journalists critical of the government were subjected to cyber-harassment in November 2022. Two of them were also targeted during a wave of arrests by law enforcement."[1107]

Freedom House reports in 2022: "One of the main newspapers, *L'Express*, has faced verbal attacks by authorities, who have also reduced public advertising with the outlet. Its journalists have faced legal and other harassment, though no reporter has been imprisoned and most are broadly perceived as operating freely. *L'Express* and other media outlets have been barred from or marginalized in state briefings […]."[1108]

The US State Department's 2022 Report on Human Rights Practices states: "Citizens enjoyed broad freedom of expression but, in some instances, individuals were restricted from criticizing the government or from discussing matters of public interest. This included restrictions from laws that criminalize 'hate speech'." This report also records allegations from opposition politicians and activists that their social media accounts were blocked, and that anti-government postings or comments were removed, as well as anecdotal reports that police tapped cell phones and intercepted emails of journalists and opposition politicians. It was also alleged that the government disrupted internet speed during opposition party rallies.[1109]

[1106] *Seegum J v The State of Mauritius* 2021 SCJ 162, pages 17-18.
[1107] "2023 World Press Freedom Index: Mauritius", "Safety".
[1108] "Freedom in the World 2022: Mauritius", Freedom House, section D1.
[1109] "2022 Country Reports on Human Rights Practices: Mauritius", US State Department, section 2A.

A number of incidents appear to involve **trumped-up charges of drug trafficking as a means of intimidation of persons critical of government**:

- In August 2022, police arrested Akil Bissessur, a lawyer who regularly spoke out against government, and his partner Doomila Moheeputh on drug trafficking charges. Bissessur was released on bail after video footage emerged showing police officers entering his partner's house carrying the bag that allegedly contained the incriminating drugs.[1110]
- In November 2022, police arrested political activist Bruneau Laurette, a well-known government critic, and his son Ryan Luca Laurette on charges of trafficking synthetic drugs and hashish and illegal possession of firearms. Laboratory tests found that the package found in Laurette's house contained chia seeds and not narcotics. Nevertheless, Bruneau Laurette remained in police detention at the end of 2022 while his son was released on bail.[1111]
- In November 2022, three journalists - Nawaz Noorbux, Jean-Luc Emile, and al-Khizr Ramdin - and the Managing Director of *Top FM* radio station, Balkrishna Kaunhye filed complaints with police after experiencing online harassment by groups that were reportedly close to the ruling party. These groups posted materials suggesting that the journalists were involved in drug trafficking. Police did not identify or arrest the individuals behind the posts.[1112]

There were also reports that **relatives of journalists faced punitive job transfers** in retaliation for the journalists' criticism of the government.[1113]

There are several instances where **section 46 of the Information and Communication Technology Act which prohibits "false news"** was applied to information concerning the Covid-19 pandemic – even though that provision is not specific to Covid-19.

- In March 2020, activist Jahmeel Peerally was arrested for **spreading false news in violation of the Information and Communication Technology Act** (probably section 46). The issue was a Facebook post stating that there were riots in Mauritius following orders by the Prime Minister to close non-essential businesses during the Covid-19 pandemic. He believed the statement to be true at the time he posted it, and he removed it and apologised when he discovered that it was false. The post was shared over 10,000 times, but no harm or injury took place and there was no evidence that Peerally intended to cause violence or undermine the government's effort to address the pandemic.
- In April 2020, Rachna Seenauth was arrested on a charge of posting **false news** on Facebook, apparently under **section 46 of the Information and Communication Technology Act**. Her post was political satire concerning the government's response to the Covid-19 pandemic.
- In July 2020, Naushad Lauthan was arrested for **sharing false news** on Facebook about a second lockdown to deal with Covid-19, **in violation of section 46 of**

[1110] Id, section 1D.
[1111] Id.
[1112] Id, section 2A.
[1113] Id.

the Information and Communication Technologies Act. There appears to have been no intention to cause violence or undermine the government's effort to address the pandemic, and the government did in fact announce a second lockdown just a few days later. Lauthan reportedly paid a fine of Rs 25,000 and signed an IOU for an additional Rs 100,000.

- In November 2021, Raouf Khodabaccus was arrested on a charge of **knowingly transmitting a false message in violation of section 46 of the Information and Communication Technology Act**. The basis for the charge was a live video posted on his Facebook page, in which he claimed that "a hundred patients" were waiting at Jeetoo Hospital for Covid-19 testing and warned parents not to send their children to school the next day. Officials from the Ministry of Health complained that the video was a fake news broadcast designed to create panic among the population, while the Mauritius Broadcasting Corporation (MBC) asserted that the video was designed to discourage people from going to Jeetoo hospital for tests, to incite panic about Covid-19 and to dissuade parents from sending their children to school. Khodabaccus maintained that the content in the video was true and accused the MBC of suppressing facts about Covid-19 and its impact. Khodabaccus was convicted and fined Rs 100,000.[1114]

11.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

Mauritius has two key pieces of legislation on cybercrimes: the **Cybersecurity and Cybercrime Act 16 of 2021** and the **Information and Communication Technologies Authority Act 44 of 2001.**

A) CYBERSECURITY AND CYBERCRIME ACT 16 OF 2021

The Cybersecurity and Cybercrime Act 16 of 2021[1115] replaced the Computer Misuse and Cybercrime Act 22 of 2003.[1116] The new law adds additional offences to comply with the latest additions to Budapest Convention, making it an up-to-date piece of legislation.[1117] On the other hand, opposition politicians criticised the vague language in some of the offences, on the grounds that this gives authorities discretion to crack down on online content that they consider harmful. It has also been noted that the law increases the power of law enforcement officials to seize computer systems or devices.[1118]

[1114] "LEXOTA Country Analysis: Mauritius", last updated July 2022.
[1115] Cybersecurity and Cybercrime Act 16 of 2021.
[1116] The Computer Misuse and Cybercrime Act 22 of 2003 (now repealed) can be found here and here.
[1117] Mohammud Nabeel Khodabux, "Mauritius: Compliance Automation: A New Dawn In The Financial Services Sector", *mondaq* 29 March 2022.
[1118] "2022 Country Reports on Human Rights Practices: Mauritius", US State Department, section 2A.

The Act establishes a **National Cybersecurity Committee** that, amongst other things, advises the government on cybersecurity and cybercrime, implements government policy on these issues and receives and acts on reports relating to cybersecurity and cybercrime, coordinates protection for critical information infrastructure and promotes capacity building on the prevention, detection and mitigation of cyber threats, The Chairperson of the Committee is appointed by the Prime Minister. It also includes ten representatives of relevant government bodies, along with one representative of the private sector and one representative of civil society appointed by the relevant minister.[1119] It also sets up a **Computer Emergency Response Team of Mauritius (CERT-MU)** to deal with cybersecurity issues.[1120]

The Act contains some detailed technical offences, some of which list specific circumstances where no criminal liability is incurred.

CYBERSECURITY AND CYBERCRIME ACT 16 OF 2021 - TECHNICAL OFFENCES	
Section 7: Unauthorized access to computer data	It is an offence to gain unauthorized access to any program or data held in a computer system. The penalty is a fine of up to 1 million rupees and penal servitude for up to 10 years. Access to a computer system is unauthorized where the person who gained access – • is not entitled to control access of the kind in question; and • has not been authorized to have access of the kind in question by any person who is entitled to such access. It is irrelevant to the offence whether or not the access was aimed at a particular programme or data, or a particular type of programme or data. There are several grounds that allow a person to escape liability for unauthorized access: • the person had a right to control the operation or use of the computer system and exercised it in good faith; • the person had the express or implied consent someone empowered to authorise the access, or • reasonable grounds to believe that he had such consent. • the person was acting pursuant to the investigative measure set out in the Act. • the person was acting in reliance on a statutory power that allows obtaining information or taking possession of any document or other property. o Note that this offence requires access to a *programme or data* held in a computer system, as opposed to some other laws in the region that criminalize access to a computer system. o There is no general reference to the possibility of a lawful excuse or justification beyond those specifically listed, such as gathering information for the purposes of whistleblowing or investigate journalism.

[1119] Cybersecurity and Cybercrime Act 16 of 2021, sections 3-4.
[1120] Id, sections 38-39.

	○ While some assert that criminalization of "mere access" without more is justified given that it compromises data confidentiality, there is no universal consensus on whether criminalization of mere access to non-protected systems is warranted, or whether this crime should be narrowed by additional conditions.[1121] The *SADC Model Law on Computer Crime and Cybercrime* qualifies the offence of illegal access by requiring that it take place "intentionally, without lawful excuse *or justification* or in excess of a lawful excuse or justification".[1122] ○ The maximum penalties seem excessive for "mere access".
Section 8: Unauthorized interruption of computer service	It is an offence to use any technical means without authorization to wilfully intercept or cause the interception of – • computer data • electromagnetic emissions carrying computer data, or • non-public transmissions to, from or within, a computer system. The penalty is a fine of up to 1 million rupees and penal servitude for up to 10 years. There is an enhanced penalty where the commission of the offence impairs the operation of the computer system or suppresses or modifies transmitted computer data. It is irrelevant to the offence whether or not the access was aimed at a particular programme or data, or a particular type of programme or data. There are several grounds that allow a person to escape liability for unauthorized interruption: • the person has obtained the prior consent of both the person who sent the data and its intended recipient; • the person is acting in reliance on any statutory power; • the person is acting in the performance of lawful duties or contractual obligations or is discharging any legal obligation.
Section 9: Unauthorised interference	It is an offence, intentionally and without authorization, to hinder the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. The penalty is a fine of up to 1 million rupees and penal servitude for up to 10 years. An interference is unauthorized where the person who acted – • is not entitled to cause that interference; • does not have consent from a person who is so entitled. There is an enhanced penalty where the unauthorised interference - • results in financial loss to any person or organization; • threatens national security; • causes reputational damage to any person; • causes anyone's physical or mental injury or death; • causes, directly or indirectly, degradation, failure, interruption or obstruction of the operation of a computer system; or • threatens public health or public safety.

[1121] *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
[1122] SADC Model Law on Computer Crime and Cybercrime, section 4.

	It is irrelevant to the offence whether the unauthorized interference was aimed at a particular programme or data, or a particular type of programme or data, and whether it was temporary or permanent. o "Hinder" is not defined here. Some cybercrime laws in the SADC region include definitions of this term. o Regarding the enhanced penalties, "national security", "public health" and "public safety" are all undefined.
Section 10: Access with content to commit offences	It is an offence, intentionally and without authorization, to gain access to any computer program or computer data held in a computer system with intent to commit an offence. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. o Note that the maximum period of imprisonment for access with intent to commit an offence is double that for "mere access", although the maximum fine is the same for both.
Section 11: Unauthorised modification of computer data	It is an offence intentionally and without authorization, to modify computer data. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. A modification is unauthorized if the person who acted was not entitled to determine whether the modification should be made and did not have consent to make the modification from any person who is so entitled. There is an additional penalty where the commission of this offence suppresses, modifies or otherwise impairs the operation of the computer system, access to any computer program or computer data, the operation of any computer program or the reliability of any computer data. It is irrelevant to the offence whether the effect of the act was temporary or permanent.
Section 12: Unauthorised disclosure of password	It is an offence, intentionally and without authorization, to disclose any password, access code, biometric authentication, token, two-factor authentication, multi-factor authentication or any other means of gaining access to any computer program or computer data held in any computer system where this takes place for its production, sale, procurement for use, import or distribution. The penalty is a fine of up to 1 million rupees and penal servitude for up to 10 years.
Section 13: Unlawful possession of devices and computer data	It is an offence to intentionally manufacture, sell, procure for use, import, distribute or otherwise make available a computer system, computer data or any other device designed or adapted primarily for the purpose of committing any offence under this Act. It is also an offence, intentionally and without authorization, to receive or be in possession of such devices or computer data. "Possession of any computer data" includes - • having possession of a computer system or device that holds or contains the computer data or computer program • having possession of a document in which the computer data or computer program is recorded; or

	• having control of computer data or computer program that is in the possession of another person. The penalty for any of these offences is a fine of up to 1 million rupees and penal servitude for up to 10 years. o Section 2 includes a detailed definition of "device". o "Device" is well-described in the office, to capture only devices adapted primarily for illegal use.
Section 14: Electronic fraud	It is an offence, intentionally and without authorization, to cause loss of property to another person by - • any input, alteration, deletion or suppression of data; or • any interference with the functioning of a computer system, • in order to gain any form of advantage for oneself or another person. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years.
Section 15: Computer-related forgery	It is an offence, intentionally and without authorization, to input, alter, delete, or suppress computer data, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable or intelligible. The penalty is a fine of up to 1 million rupees and penal servitude for up to 10 years. There is an enhanced penalty if this offence is committed for wrongful gain, for wrongful loss to another, or for any benefit to oneself or another.

The law also creates six new content-based offences. Child pornography is not included here, being addressed by the Child Protection Act 30 of 1994 which makes it an offence to produce, distribute or possess an indecent photograph or pseudo-photograph (an image that appears to be a photograph) of a child, with the relevant terms being defined to include films and data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.[1123]

CYBERSECURITY AND CYBERCRIME ACT 16 OF 2021 – CONTENT-BASED OFFENCES	
Section 16: Misuse of fake profile	It is an offence, individually or with other persons, to make use of a fake profile to cause harm. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. o "Fake profile" is defined in section 2 as "an untrue online representation, existent or non-existent". o "Harm" is defined in section 2 as "physical, sexual, psychological, emotional or moral abuse, injury, neglect, ill-treatment, degradation, discrimination, exploitation or impairment of health or development". o The requirement that the use of a fake profile must cause harm usefully narrows the offence.

[1123] Child Protection Act 30 of 1994, sections 15 read with the definitions of "child", "film", "indecent photograph", "photograph" and "pseudo-photograph" in section 2. What constitutes indecency is not defined, however, nor is there any exception for artistic, educational or scientific materials.

Section 17: Cyberbullying	It is an offence, individually or with other persons, to commit cyberbullying. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. o "Cyberbullying" is defined in section 2 as any behaviour by means of information and communication technologies, which – • is repetitive, persistent and intentionally harmful; or • involves an imbalance of power between the perpetrator and the victim *and* causes feelings of distress, fear, loneliness or lack of confidence in the victim *and* results in serious physical or psychological harm, disability or death of the victim. o The definition seems to be reasonably well-narrowed. o This offence overlaps with section 46(ga) of the Information and Communication Technologies Authority Act 44 of 2001, which is more broadly formulated (discussed below).
Section 18: Cyber extortion	It is an offence to engage in cyber extortion. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. o "Cyber extortion" is defined in section 2 as a form of cybercrime which occurs when a person uses the internet to demand money or other goods or behaviour from another person, by threatening to inflict harm to that person, his reputation or his property.
Section 19: Revenge pornography	It is an offence, by means of a computer system, to disclose or publish a sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress. The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years. o "Sexual photograph or film" is defined in section 2 as an image or video that depicts nudity or a picture of someone who is engaged in sexual behaviour or posing in a sexually provocative way. o "Pornography" is defined in section 2 as a representation in a book, magazine, photograph, film, computer data or any such other media, or a scene of sexual behaviour in any form, that is erotic or lewd and is designed to arouse sexual interest. However, this term appears only in the tittle of the offence and not in the text that set out the elements of the offence. o Here the requirement of intent to cause distress may make the offence very difficult to prove. Some provisions on this topic in other countries require only distribution of the material without the consent of the person depicted. o This offence lacks a requirement that the person depicted be identifiable, which is included in some jurisdictions.
Section 20: Cyberterrorism	It is an offence to intentionally access, or cause access to, a computer system or network for the purpose of carrying out an act of terrorism, which has the same meaning as in the Prevention of Terrorism Act.[1124] The penalty is a fine of up to 1 million rupees and penal servitude for up to 20 years.

[1124] There is an extensive definition of "act of terrorism" in section 3(2) of the Prevention of Terrorism Act 2 of 2002.

Section 21: Infringement of copyright and related rights	It is an offence, without the express authorization of the author or owner of the copyright, to • attempt to use, publish or distribute another person's work for commercial purposes, through a computer system; • download movies, music files or pirated software applications for gain or against remuneration; or • post a copyrighted work online for gain or against remuneration. The penalty for a first offence is a fine of up to 300,000 rupees and imprisonment for a term of up to 2 years, and for a subsequent offence, a fine of up to 500,000 rupees and imprisonment for a term of up to 8 years.

All of the **penalties** authorise the imposition of a fine *and* a period of imprisonment. There are no minimum penalties and most of the maximum penalties are fines of 1 million rupees and penal servitude for a maximum or either 10 or 20 years.

There are increased penalties for the offences in sections 7, 8, 9, 10 and 11 if they were committed on a **critical information infrastructure**; in that case, the maximum fine is 2 million rupees and the maximum imprisonment is 25 years. Section 2 defines "critical information infrastructure" as an asset, facility, system, network or process, whose incapacity, destruction or modification would have a debilitating impact on essential services, or a significant impact on national security, national defence, or the functioning of the State. The National Cybersecurity Committee identifies "critical information infrastructures" that fit these criteria.[1125]

Investigatory powers: An investigatory authority (meaning the police or the police or any other body lawfully empowered to investigate any offence) can issue an **expedited preservation order** to retain and disclose **traffic data** relating to the communication under investigation. Such an order remains in force for 90 days and can be extended for an unspecified period by a judge.[1126] A **production order** for any specified data required for the investigation or prosecution of an offence can be issued by a judge.[1127] **Searches and seizures** require a warrant from a judge and can apply to stored content data.[1128] A judge can also authorise **real-time collection of traffic data**, or **real-time interception of content data**, in respect of specified communications by investigatory authorities.[1129] In addition, a judge can **order a service provider to delete or destroy unlawful material**.[1130]

[1125] Cybersecurity and Cybercrime Act 16 of 2021, section 33.
[1126] Id, section 26.
[1127] Id, section 27.
[1128] Id, section 28. A local newspaper provided a helpful description of the difference between "traffic data" and "stored data" for the layperson, describing "*traffic data*" as "the history of your everyday websites and online platforms that you visit, including your mobile internet traffic, phone calls, SMS, etc" and "*stored data*" as "your email content if your email is hosted by the service provider". Ish Sooken, "My thoughts on the Cybersecurity and Cybercrime Bill", *lexpress*, 2 November 2021.
[1129] Id, sections 29-30.
[1130] Id, section 31.

Take-down notifications: There is no take-down procedure based on complaints from members of the public. Instead, the administrator of an online account has a **duty "to moderate and control" undesirable content that has been brought to his attention by an "investigatory authority".** Failure to do so constitutes an offence punishable by a fine of up to one million rupees and penal servitude for up to 20 years. For this purpose, "undesirable content" includes any online content that –

- is deceptive or inaccurate, posted with intent to defame, threaten, abuse or mislead the public;
- threatens public health or public safety;
- threatens national security; or
- promotes racism.[1131]

CYBERSECURITY AND CYBERCRIME ACT 16 OF 2021

23. Failure to moderate undesirable content

1) It shall be the responsibility of the administrator of an online account to moderate and control undesirable content that has been brought to his attention by an investigatory authority.
2) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years.
3) For the purpose of this section -
4) "undesirable content" includes any online content that -

a) is deceptive or inaccurate, posted with intent to defame, threaten, abuse or mislead the public;
b) threatens public health or public safety;
c) threatens national security; or
d) promotes racism.

The Director of Public Prosecutions (DPP) has explained what this duty means in practice. An "investigatory authority" means the police, or any other body lawfully empowered to investigate any offence. The process that leads to criminal liability is a two-step one. First, the allegedly undesirable content on the online account is brought to the attention of the administrator. Second, after having received such a notification, the administrator of the account must moderate or censor the content to the satisfaction of the investigatory authority. The DPP expressed the opinion that this section will not apply to an administrator of a WhatsApp group since that administrator does not have the power to regulate, moderate or censor the content before it is posted on the group.[1132] However - looking at a point not touched on in the article by the DPP, it does seem that the administrator of a WhatsApp group could incur criminal liability for a failure to *delete* the post after being notified by an investigatory authority that it was "undesirable content".

This provision is rife with undefined terms, including a lack of clarity about what is meant by "moderate or control". Moreover, there is no provision for the involvement of a judicial authority nor is there any requirement of notice to the author of the material or a duty to allow that author to defend the material. This provision lacks safeguards against abuse by government authorities.

[1131] Id, section 23.
[1132] Satyajit Boolell, SC, "Director Of Public Prosecutions, Mr. Satyajit Boolell, Explains Role Of An Administrator Of A Whatsapp Group", *Le Matinal*, 21 March 2022.

B) INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 44 OF 2001

Section 46 of this Act contains a list of offences which can be classed as cybercrimes. This provision includes both technical and content-based offences. The technical offences apply to "information and communication networks", which refers to a network for the transmission of messages and includes a telecommunication network. It also includes offences relating to the messages sent on such networks with "message" being comprehensively defined as any form of electronic communication, or any other communication whether in the form of speech or other sound, data, text message, writings, images, photographs, signs, signals or code or in any other form or combination of forms. [1133] All of the offences in the list can be committed by "any person",[1134] even though some of them would most likely be performed by the licensee or its agents. Some of the offences in section 46 have been omitted from the table below, where they relate specifically to the licensing of services under the Act.

INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 44 OF 2001 – TECHNICAL OFFENCES	
Section 46(a)	harming the function of an information and communication service, including a telecommunication service, by means of any emission, radiation, induction or other electromagnetic effect
Section 46(b)	taking a message from the employee or agent of a licensee with intent to defraud, or with intent to prevent the sending or delivery of the message
Section 46(c)	taking a message from a place or vehicle used by a licensee in the performance of his functions, with intent to defraud
Section 46(d)	stealing, hiding or destroying a message o The wording of the provisions is overbroad; as the Centre for Law and Democracy Centre points out, destroying messages occurs every time someone deletes a message from their email inbox.[1135]
Section 46(e)	wilfully or negligently omitting or delaying the transmission or delivery of a message
Section 46(i)	dishonestly obtaining or making use of an information and communication service, including a telecommunication service, with intent to avoid payment for the service
Section 46(j)	using an apparatus or device to defraud a licensee of payment for the use of a service, to cause the licensee to provide a service to someone else without payment, or fraudulently installing or causing the installation of access to a telecommunication line
Section 46(k)	wilfully damaging, interfering with, removing or destroying an information and communication installation or service maintained or operated by a licensee

[1133] Information and Communication Technologies Authority Act 44 of 2001, section 2.
[1134] Id, section 46(1).
[1135] "Centre for Law and Democracy Note on the ICT Act", May 2021, page 12.

Section 46(ka)	wilfully tampering with the International Mobile Station Equipment (IMEI) of any mobile device (referring to a unique identifying number which is allocated to every such device and used to block stolen devices)
Section 46(m)	without the prior approval of the ICTA, importing any equipment capable of intercepting a message
Section 46(n)	disclosing a message or information relating to a message to any other person otherwise than in accordance with this Act, with the consent of the sender and each intended recipient, or for the purpose of the administration of justice or as authorized by a judge. o This offence is overbraad. It "would cover forwarding an email without obtaining the consent of the original sender, something virtually everyone who operates online has done repeatedly. It would also cover showing someone a mass text advertisement without obtaining the consent not only of the sender but also the potentially thousands of other recipients."[1136]
Section 46(p)	intercepts - or authorises, permits or enables interception – of a message passing over a network, except as expressly permitted by this Act or as authorized by a Judge

INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 44 OF 2001– CONTENT-BASED OFFENCES	
Section 46(f)	forging a message or transmitting or otherwise making use of a message knowing that it has been forged. o This offence raises the question of what constitutes 'making use' of a forged message; would it apply to a journalist who has quoted it in a report about corruption or some other wrongdoing? This does not seem to be the intent, but the wording could be made clearer.
Section 46(g)	knowingly sending, transmitting or causing to be transmitted a false or fraudulent message. o LEXOTA notes that this paragraph requires that the offence be committed "knowingly" but does not make it clear if this "means simply knowledge that the person is sending a message, or also knowledge that the message is false".[1137] o This offence could theoretically apply to the forwarding of a false of fraudulent message, even with an explanation, to publicise the falsehood. Again, this does not seem to be the intent, but the wording could be made clearer. o The Centre for Law and Democracy comments that "Inaccuracy alone is not sufficient to restrict freedom of expression", citing the 2017 Joint Declaration by the special rapporteurs on freedom of expression that: "General prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective

[1136] Id.
[1137] "LEXOTA Country Analysis: Mauritius", last updated July 2022.

	information'" are incompatible with international guarantees of freedom of expression."[1138]
Section 46(ga)	using telecommunication or ICT services, equipment or technologies to send, transmit, transfer, post, publish, deliver, show or otherwise communicate a message which is "obscene, indecent, offensive, abusive, threatening, menacing, false or misleading, which is likely to cause or causes harm to a person". o "Harm" is not defined, but section 46(3) states that it "includes serious emotional distress". However, there is a list of factors to be considered in determining whether harm was caused or was likely to be caused– • the extremity of the language used; • the age and characteristics of the alleged victim; • whether the message was anonymous; • whether the message was repeated; • the extent of circulation of the message; • the context in which the message appeared; • whether the message would cause harm or would be likely to cause harm to an ordinary reasonable person in the position of the alleged victim. o The key terms used here are not defined. with this being particularly problematic for the terms "obscene", "indecent", "offensive", and "abusive". o LEXOTA states: "It is not clear how to determine whether a message is 'false' or 'misleading', and the scope of what is considered 'obscene' or 'indecent'. Further guidance is needed to clarify the threshold of what might cause 'annoyance, humiliation, inconvenience, distress or anxiety' to any person. Section 46 does not, therefore, provide sufficient guidance for individuals and could provide an overly wide degree of discretion to those charged with its enforcement." It notes further that section 46(ga) does not require knowledge of the message's impact on the part of the sender.[1139]
Section 46(ha)	using telecommunication or ICT services, equipment or technologies to impersonate, or to impersonate by any other means, another person where this is "likely to cause or causes harm to that person". o It seems odd that this offence can be committed "by any means", which would seem to include acts that have nothing to do with ICT or telecommunications. o See the row above on the parameters of "harm".

The **penalty** for any of these offences is a fine of up to 1 million rupees and penal servitude for up to 10 years. [1140] The Centre for Law and Democracy suggests that it would be better practice to have more tailored graduated penalties, with more serious punishments reserved for more serious offences such as those involving intent

[1138] "Centre for Law and Democracy Note on the ICT Act", May 2021, page 11.
[1139] "LEXOTA Country Analysis: Mauritius", last updated July 2022.
[1140] Information and Communication Technologies Act 44 of 2001, section 47.

to defraud, and a lower penalty range of fines and warnings for less serious offences, such as obtaining telecommunication services without proper payment.[1141]

In the case of a conviction under this Act, the court may also order the **forfeiture of any equipment** used in connection with the offence, or the **suspension of a service** provided to the convicted person (such as their access to a telecommunications service, for instance). Where the culprit is a licensee, the court can order the **cancellation of the licence**. It can also order that the person in question is ineligible for a licence for any period that the court thinks fit.[1142]

This law also gives disturbing **powers of interception and censorship to service providers**. A public operator is permitted to intercept, withhold or otherwise deal with a message where it has reason to believe that the message violates the Act, is indecent or abusive or is "of a nature likely to endanger or compromise State's defence, or public safety or public order". Where a message is withheld on these grounds (but not where it is intercepted or otherwise dealt with), the operator must refer the matter to the Authority for directions.[1143] In essence, this allows public operators to intercept or block a communication, without any authorisation by an independent body and without any notice to the sender of the action taken or the reasons for it.

INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 44 OF 2001

32(5)(a) Nothing in this Act shall prevent a public operator or any of his employees or agents from intercepting, withholding or otherwise dealing with a message which he has reason to believe is -

i. indecent or abusive;
ii. in contravention of this Act;
iii. of a nature likely to endanger or compromise State's defence, or public safety or public order.

(b) Where a message is withheld pursuant to paragraph (a), the operator shall forthwith refer it to the Authority for such written directions as the latter may think fit.

The Centre for Law and Democracy comments that "while it is generally acceptable to allow for measures to address obscene content, subject to authoritative decision-makers such as courts elaborating on what that means over time, the definition of what might quality as 'indecent' or 'abusive' is simply too broad and flexible to serve as the basis for a restriction on freedom of expression, at least absent clear and appropriate definitions in the ICT Act of what these mean. Absent such a definition, this provision grants unduly broad discretion to intercept or withhold messages." The Centre suggests that this power should be removed entirely or at least limited to highly exceptional cases such as the dissemination of child pornography.[1144]

Investigatory powers: The Act provides that a Judge, on application by the police or the Independent Commission Against Corruption in relation to a criminal investigation or proceeding, may issue an order authorising a public operator to intercept or withhold a message, or disclose it to the police or the Commission.[1145]

[1141] "Centre for Law and Democracy Note on the ICT Act", May 2021, page 13.
[1142] Information and Communication Technologies Act 44 of 2001, section 47.
[1143] Id, section 32(5). This power is buried in a section entitled "Confidentiality".
[1144] "Centre for Law and Democracy Note on the ICT Act", May 2021 pages 10-11.
[1145] Information and Communication Technologies Act 44 of 2001, section 32(6)(a).

Moreover, section 32(6)(a) of the Act permits a Judge, where satisfied by application by the Police or the Independent Commission Against Corruption relating to a criminal proceeding, to issue an order authorising a public operator, or any of its employees or agents, to intercept or withhold a message, or disclose it to the police or the Commission. Such orders remain valid for a maximum of 60 days and should specify the exact location of the interception or withholding of the message.

C) CRIMINAL CODE

The **Criminal Code**[1146] contains several offences that could be applied to inhibit freedom of expression.

The key provisions are discussed here, although this is not a comprehensive list. Note that we found no recent examples where any of these provisions were applied in practice against journalists or persons engaging in political speech.

The main concern is **criminal defamation**, defined as "any imputation or allegation of a fact prejudicial to the honour, character or reputation of the person to whom such fact is imputed or alleged". It is possible to defame a deceased person where the statement is "calculated to throw discredit on or be hurtful to the feelings of the family or relatives of the deceased". The penalty is imprisonment for up to one year and a fine of up to 5 000 rupees. Truth and fair comment are defences. [1147]

The following are some other offences which could be applied to inhibit free expression:

- **Section 206: Outrage against public and religious morality** – It is an offence, through speech or publications, to commit an outrage against any legally established religion, "good morals" or "public and religious morality".
- **Section 282: Stirring up racial hatred** – It is an offence, through speech, publications or broadcasting, to communicate any matter that is "threatening, abusive or insulting" with the intent to stir up contempt or hatred against any section of the public distinguished by race, caste, place of origin, political opinions, colour or creed. "Broadcast is defined here as "using radio-communication whether by sound or vision, for reception by members of the public".
- **Section 283: Sedition** – It is an offence, through speech or publications, to bring into hatred or contempt, or excite disaffection towards, the Government or the administration of justice, or to raise discontent or disaffection among the citizens of Mauritius or promote feelings or ill-will and hostility between different classes of such citizens. This does not apply to statements that express

[1146] Criminal Code amended to 2006. Note that it has been further amended by the Criminal Code (Amendment) Act 11 of 2012 (section 285 and 285A on abortion), the COVID (Miscellaneous Provisions) Act 1 of 2020 (details of sections 4, 5, 6, 378, 382, and 385) and the Criminal Code (Amendment) Act 17 of 2021 (which adds a new section 76B: Misrepresenting the sovereignty of Mauritius over any part of its territory). See also the See also Criminal Code (Supplementary), which covers, amongst other things, dealing in obscene matter, exhibiting slides and video tapes in public, and bomb and fire hoaxes.
[1147] Criminal Code amended to 2006, section 288.

disapproval of government measures of the Government with a view to obtaining their alteration by lawful means, or to criticism of government actions that does not excite or attempt to excite hatred, contempt or disaffection. The compatibility of this offence with the right to freedom of expression was considered in the 1992 case of *DPP v Masson*, where the Supreme Court held that it must be read as including an element of incitement to violence or public disorder to be consistent with Article 12 of the Constitution. [1148]

- **Section 284: Inciting to disobedience or resistance to law** - It is an offence, through speech, or publications, to instigate disobedience or resistance to laws or the authorities entrusted with the execution of the laws.
- **Section 296: Insult** - It is an offence, through speech or written or printed matter, to use any "injurious expression or any term of contempt or invective, or other abusive language, not carrying with it the imputation of a fact".
- **Section 299: Publishing false news** - It is an offence to publish or disseminate false news or news which, although accurate in substance, has been altered in one or more parts or falsely attributed to some other person, if the statement is of a nature to disturb public order or public peace. It is a defence to show that the publication was made in good faith after making sufficient enquiries to ascertain its truth. LEXOTA criticises this provision's lack of clarity, which could give an overly wide degree of discretion to those charged with the enforcement of this law.[1149] The constitutionality of this provision was upheld in the 1990 case of *R v Boodhoo*.[1150] In the 2002 case of *Seneque v DPP*, the application of the offence was limited as follows:

> *Their Lordships accept that public indignation or outrage at some act of the Government or Government policy may be such that a false statement about such act or policy could be capable of creating a likelihood of disturbance occurring i.e. could be of such a nature as to disturb public order or public peace. The mere fact that such a statement is critical of Government and even that people, and particularly voters, will not like it, however, is not in itself enough.*[1151]

[1148] *DPP v Masson* (1972) M.R. 204, as discussed in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 10.
[1149] "LEXOTA Country Analysis: Mauritius", last updated July 2022.
[1150] *R v Boodhoo* [1990] MR 191, as discussed in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 11.
[1151] *Seneque & anor v DPP* [2002] UKPC 42 (PC), as quoted in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 12.

D) NATIONAL ASSEMBLY (PRIVILEGES, IMMUNITIES AND POWERS) ACT 22 OF 1953

The **National Assembly (Privileges, Immunities and Powers) Act 22 of 1953** lists several actions that constitute the offence of contempt of the National Assembly. These include:

- sending a member of the National Assembly an insulting or threatening letter;
- publishing any defamatory statement about the National Assembly or any committee, or the conduct or character of any member concerning that member's actions or statements in the National Assembly, where this would also be punishable as defamation under section 288 of the Criminal Code (discussed above)
- publishing any perverted or biased reports of proceedings of the National Assembly or any of its committees, or gross misrepresentations of the speeches of particular members
- publishing any statement reflecting on the conduct or character of the speaker, deputy speaker or chairperson of any National Assembly committee, or accusing any of these officials of partiality in the discharge of their duty.[1152]

E) SIM CARD REGISTRATION

Section 48 of the **Information and Communication Technologies Act** authorises the minster to make regulations on SIM card registration. These have been issued as the **Information and Communication Technologies (Registration of SIM) Regulations 2021**,[1153] which were amended by the **Information and Communication Technologies (Registration of SIM) (Amendment) Regulations 2023**.[1154] The amended regulations took effect on 30 June 2023, with a deadline of 31 December 2023 for registration of existing SIM cards to avoid deactivation.[1155]

F) STATE SURVEILLANCE

In addition to the investigatory powers described above under the two key laws on cybercrimes, CIPESA (Collaboration on International ICT Policy for East and Southern Africa) notes that the government implements the Safe City project "which is a **nationwide CCTV system** for the purpose of safeguarding national security as well as public security". Although this is not covered by any legislation, the Data Protection Office has issued a "code of practice" for the operation of the project.[1156]

[1152] National Assembly (Privileges, Immunities and Powers) Act 22 of 1953, section 6(1)(g), (n), (o) and (s), read with section 6(2).
[1153] Information and Communication Technologies (Registration of SIM) Regulations 2021 (not located online).
[1154] Information and Communication Technologies (Registration of SIM) (Amendment) Regulations 2023. The amendments concern the dates of coming into force.
[1155] ICTA Communique on Amendments to the Information and Communication Technologies (Registration of SIM) Regulations 2021, 18 January 2023.
[1156] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 38 (referring to a previous section number).

CIPESA also notes that the **Information and Communication Technologies Act 44 of 2001** empowers the ICTA to control the **importation of any equipment capable of being used to intercept a message**.[1157]

The laws examined do not discuss **encryption**, or restrict the use, development or importation of encryption software or products.

G) TAKE-DOWN NOTIFICATIONS

As discussed above, in terms of the **Cybersecurity and Cybercrime Act 16 of 2021**, take-down notifications in respect of **"undesirable content"** come, not from members of the public, but from investigatory agencies, with no notice or right of appeal for the author of the content concerned. Note that the concept of "undesirable content" is not necessarily "illegal content".[1158]

11.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Mauritius is expected to hold general elections in November 2024, after which the newly elected National Assembly will elect the President. The President appoints the Prime Minister.[1159]

By way of background, here is a brief description of the last election in 2019:

> *Mauritius is a multi-party, parliamentary democracy. Shifting coalitions are a feature of politics in the country. The President is the head of state, while the Prime Minister has full executive powers and heads the government. General elections were held in November 2019. The result was a victory for the Mauritian Alliance—a coalition of the Militant Socialist Movement (MSM), Muvman Liberater, Alan Ganoo Movement, and Plateforme Militante - which won 42 of the 70 seats".*[1160]

This outcome confirmed incumbent Prime Minister Pravind Jugnauth of the Militant Socialist Movement (MSM) for a second five-year term.[1161] Jugnauth first became prime minister in 2017 when his father stepped down from the post.[1162]

[1157] Section 18(u), as discussed in id, page 38 (referring to a previous paragraph number).
[1158] Cybersecurity and Cybercrime Act 16 of 2021, section 23.
[1159] Mauritius's 1968 Constitution, revised 2016, Articles 28(2) and 59(1).
[1160] "The World Bank in Mauritius: Overview", The World Bank, 23 March 2023, "Political Context".
[1161] "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
[1162] Jean Paul Arouff. "Mauritius elects incumbent PM for five-year term," *Reuters*, 8 November 2019.

> *Political opposition leaders challenged the validity of the results and claimed electoral irregularities, filing several legal petitions with the Supreme Court. This is the first-time election results in Mauritius have faced such grave contestation since the country's independence"*[1163]

Looking more generally at the country's political dynamics:

> *The democratically elected government can and does govern the country effectively. There are no individuals or groups with veto power. The aforementioned tendency to form alliances of political parties means that the government usually includes two or more political parties – a necessity for obtaining a majority in parliament. Such coalition governments are dependent on inter-party consensus. The opposition is an important pillar in Mauritius' political system, with the post of the opposition leader being explicitly provided for in the country's constitution. This confers some consultative powers to the leader of the opposition when it comes to certain institutional appointments, such as for the members of the Electoral Supervisory Commission, the body that bears general responsibility for the electoral process […].*[1164]

The Mauritian Constitution establishes an **Electoral Supervisory Commission** and an **Electoral Commissioner** to supervise elections. It provides a fair deal of detail about the structure and functions of these bodies.[1165]

MAURITIAN CONSTITUTION

38. ELECTORAL COMMISSIONS

1. […]
2. There shall be an Electoral Supervisory Commission which shall consist of a chairman and not less than 2 nor more than seven other members appointed by the President, acting after consultation with the Prime Minister, the Leader of the Opposition and such other persons as appear to the President, acting in his own deliberate judgement, to be leaders of parties in the Assembly.
3. No person shall be qualified for appointment as a member of […] the Electoral Supervisory Commission if he is a member of, or a candidate for election to, the Assembly or any local authority or a public officer or a local government officer.
4. Subject to this, section, a member of […] the Electoral Supervisory Commission shall vacate his office

[1163] "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
[1164] Id, "Executive Summary".
[1165] Mauritius's 1968 Constitution, revised 2016. Articles 38-41. The relevant sections are quoted in the box. The omitted portions relate to the Electoral Boundaries Commission, which makes recommendations on the borders of constituencies.

a. at the expiration of 5 years from the date of his appointment; or
b. when any circumstances arise that, if he were not a member of the Commission, would cause him to be disqualified for appointment as such.

5. The provisions of section 92(2) to (5) [grounds for removal of members of commissions] shall apply to a member of […] the Electoral Supervisory Commission as they apply to a Commissioner within the meaning of section 92.

39. CONSTITUENCIES

40. ELECTORAL COMMISSIONER

1. There shall be an Electoral Commissioner, whose office shall be a public office and who shall be appointed by the Judicial and Legal Service Commission.
2. No person shall be qualified to hold or act in the office of Electoral unless he is qualified to practise as a barrister in Mauritius.
3. Without prejudice to section 41, in the exercise of his functions under this Constitution, the Electoral Commissioner shall not be subject to the direction of any other person or authority.

41. FUNCTIONS OF ELECTORAL SUPERVISORY COMMISSION AND ELECTORAL COMMISSIONER

1. The Electoral Supervisory Commission shall have general responsibility for and shall supervise, the registration of electors [voters] for the election of members of the Assembly and the conduct of elections of such members and the Commission shall have such powers and other functions relating to such registration and such elections as may be prescribed.
2. The Electoral Commissioner shall have such powers and other functions relating to such registration and elections as may be prescribed, and he shall keep the Electoral Supervisory Commission fully informed concerning the exercise of his functions and shall have the right to attend meetings of the Commission and to refer to the Commission for their advice or decision any question relating to his functions.
3. Every proposed Bill and every proposed regulation or other instrument having the force of law relating to the registration of electors [voters] for the election of members of the Assembly or to the election of such members shall be referred to the Electoral Supervisory Commission and to the Electoral Commissioner at such time as shall give them sufficient opportunity to make comments thereon before the Bill is introduced in the Assembly or, as the case may be, the regulation or other instrument is made.
4. The Electoral Supervisory Commission may make such reports to the President concerning the matters under their supervision, or any draft Bill or instrument that is referred to them, as they may think fit and if the Commission so requests in any such report on a draft Bill or instrument, that report shall be laid before the Assembly.
5. The question whether the Electoral Commissioner has acted in accordance with the advice of or a decision of the Electoral Supervisory Commission shall not be enquired into any court of law.

The key laws pertaining to elections are the **Representation of the People Act 14 of 1958** and the **National Assembly Elections Regulations 2014** as amended by the **National Assembly Elections (Amendment) Regulations 2019**.[1166]

The **Representation of the People Act** contains one provision on speech. It is illegal to induce a person to vote, knowing that they are not eligible to do so, or to knowingly publish before or during an election a false statement that a candidate has withdrawn for the purpose of promoting or procuring the election of another candidate.[1167] These prohibitions are narrow and reasonable restrictions.

The National Assembly Elections Regulations 2014 prohibit campaign posters and other campaign material at polling stations[1168] – also a common and reasonable restriction.

The Electoral Supervisory Commission released a **Code of Conduct for the National Assembly Elections 2019**. Point 5 of this Code provided that all election participants (political parties or political party alliances, candidates, their agents, sub-agents, employees, supporters and backers) are entitled to fair and equitable access to the public, private and electronic media to present their electoral programme and promote their political views. It also required participants to undertake, in their campaigning on social media not to disseminate, publish and/or broadcast "fake or inaccurate news, distorted or unverified allegations, defamatory statements, and the denigration of their opponents and that of their family or other stakeholders".[1169] It is, of course, likely that a new code will be issued for the 2024 elections, but it may well include similar provisions.

The IBA regulates access to television and radio through the IBA Act. It issued guidelines for private and public broadcasters for the 2019 elections. However, MBC did not make provision for equal access for ruling and opposition parties in 2019, despite the protests of the opposition groups.[1170]

The **Mauritius Broadcasting Corporation Act 22 of 1982** does provide for a specific right of reply during election campaigns. 1) Any person who alleges that his honour, character, reputation or goodwill has been adversely affected by any political broadcast during any election campaign, may make a written application to the Chairman of the Board within 48 hours of the broadcast for a right of reply. *If the Board is satisfied* that the honour, character, reputation or goodwill of the applicant has indeed been adversely affected, it must grant a right of reply *on such terms and conditions as it thinks fit*.[1171] This approach clearly involves a great deal of discretion on the part of MBC.

[1166] All of these laws and regulations can be downloaded from the website of the Office of the Electoral Commissioner, "Legislation".
[1167] Representation of the People Act 14 of 1958, section 70.
[1168] National Assembly Elections Regulations 2014, section 28.
[1169] Code of Conduct for the National Assembly Elections 2019, point 3.
[1170] "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), "Political Participation".
[1171] Mauritius Broadcasting Corporation Act 22 of 1982, section 19.

CHAPTER 12

MOZAMBIQUE

CHAPTER 12: MOZAMBIQUE

MOZAMBIQUE KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **102nd globally; 26th out of 48 African countries** "Filipe Nyusi's re-election as president and a fragile peace deal with former army rebels have not slowed the worrisome decline in press freedom in Mozambique."
MALABO CONVENTION: Party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Mozambique's 2004 Constitution (revised 2007) (in English) The Constitution was extensively amended in 2018 with respect to the structure of government, but these amendments did not affect the provisions discussed here.[1172] **ARTICLE 48. FREEDOM OF EXPRESSION AND INFORMATION** 1. All citizens shall have the right to freedom of expression and to freedom of the press, as well as the right to information. 2. The exercise of freedom of expression, which consists of the ability to impart one's opinions by all lawful means, and the exercise of the right to information shall not be restricted by censorship. 3. Freedom of the press shall include, in particular, the freedom of journalistic expression and creativity, access to sources of information, protection of independence and professional secrecy, and the right to establish newspapers, publications and other means of dissemination. 4. In the public sector media, the expression and confrontation of ideas from all currents of opinion shall be guaranteed. 5. The State shall guarantee the impartiality of the public sector media, as well as the independence of journalists from the Government, the Administration and other political powers. 6. The exercise of the rights and freedoms provided for in this article shall be governed by law on the basis of the imperative respect for the Constitution and for the dignity of the human person. **ARTICLE 49. BROADCASTING RIGHTS, RIGHT OF REPLY AND OF POLITICAL RESPONSE** 1. Political parties shall, according to their degree of representation and to criteria prescribed by law, have the right to broadcasting time on public radio and television services.

[1172] Lei n.º 1/18 de 12 de Junho: Lei da Revisão Pontual da Constituição da República de Moçambique. The 2018 amendments are briefly summarised in English here ("Structure of the Constitution").

2. Political parties that have seats in the Assembly of the Republic but are not members of Government shall, in terms of the law and according to their degree of representation, have the right to broadcasting time on public radio and television services in order to exercise their right of reply and the right to respond to the political statements of the Government.
3. Trade unions, professional organizations and organizations representing social and economic activities shall also be guaranteed broadcasting rights, according to criteria prescribed by law.
4. During election periods, contestants shall have the right to regular and equitable broadcasting time on public radio and television stations of national or local range, within the terms of the law.

ARTICLE 50. SUPERIOR COUNCIL FOR THE MEDIA

1. The Superior Council for the Media shall guarantee the right to information, to freedom of the press and to independence of the media, as well as the exercise of broadcasting rights and the right of reply.
2. The Superior Council for the Media shall be an independent body composed of eleven members appointed as follows:
   * two members appointed by the President of the Republic, of whom one shall be the President;
   * five members elected by the Assembly of the Republic, according to the degree of parliamentary representation;
   * three representatives of journalists, elected by their respective professional organizations;
   * one representative of journalist businesses or institutions.
3. The Superior Council for the Media shall issue opinions prior to Government decisions on the licensing of private television and radio stations.
4. The Superior Council for the Media shall participate in the appointment and discharge of directors-general of public sector media organizations, in the terms of the law.
5. The law shall regulate the organization, functioning and other powers of the Superior Council for the Media.

ARTICLE 56. GENERAL PRINCIPLES

1. Individual rights and freedoms shall be directly applicable, shall bind both public and private entities, shall be guaranteed by the State, and shall be exercised within the Constitutional framework and the law.
2. The exercise of rights and freedoms may be restricted for the purposes of safeguarding other rights and interests that are protected by the Constitution.
3. The law may restrict rights, freedoms and guarantees only in cases expressly provided for in the Constitution.
4. Legal restrictions on rights and freedoms shall be of a general and abstract nature and shall not have retroactive effect.

KEY LAWS:
• Law no.º 24/19: Penal Code • Law no. 3/2017: Law on Electronic Transactions • Law no. 18/91: Press Law
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: Mozambique has no dedicated law on data protection, but there are some data protection and privacy provisions in Article 71 of the Constitution (Use of computerised data) and in several other laws.[1173]
ACCESS TO INFORMATION: Mozambique has a law on access to information.[1174]

*THIS CHAPTER WAS PREPARED WITH THE AID OF VARIOUS ONLINE TRANSLATION TOOLS.

12.1 CONTEXT

Article 50 of the Constitution (quoted on the first page of this chapter) establishes the **Superior Council of the Mass Media** ("Conselho Superior de Comunicação Social (CSCS)"). However, one commentator explains that it does not play a central role despite its constitutional status. It does not issue licences or determine the composition or structure of the media sector, but instead has more of a guidance and advisory function while the executive branch carries out the "real" media regulation.[1175]

The Council is governed by the 1991 Press Law (which pre-dates the current Constitution). The Press Law sets out its powers, which include:

- to obtain information from information agencies and government authorities to enable it to perform its functions
- to consider any violation of the Press Act and other relevant laws and to take appropriate measures to deal with such violations
- to hear and determine complaints received from the public about information agencies

[1173] See the following:
* The Civil Code (Decree-Law no. 47344, of 25 November 1966, in force in Mozambique through Edict no. 22869, dated 4 September 1967);
* The Penal Code (Law no. 24/19, of 24 December, as amended by Law no. 17/20 of 23 December);
* The Labour Law (Law no. 23/07, of 1 August); and
* The Electronic Transactions Law (Law no. 3/17, of 9 January).

Article 71 of the Constitution identifies the need to legislate on access, generation, protection and use of computerized personal data (either by public or private entities); however, implementing legislation has not yet been approved. "Data Protection Laws of the World: Mozambique", DLA Piper, 10 December 2022.

[1174] Law no. 34/14 of 31 December (in English).

[1175] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 10: Mozambique", Konrad Adenauer Stiftung, 2021, page 84 (hereinafter "Limpitlaw"). See also Leandro Gastão Paul, "CSCS: Conselho Superior de Comunicação Social - Um Órgão Inútil" (which translates as "A Useless Organ"), 2022; "Press Freedom: Mozambique", International Press Institute, December 2022, page 9.

- to be responsible for journalists' and advertisers' adherence to ethical norms and standards.

It lacks any direct regulatory powers.[1176]

A more significant body is the Government Press Office **GABINFO.** GABINFO operates as an arm of the executive branch of government operating from the Office of the Prime Minister, with a Director appointed by the Prime Minister. GABINFO took over the functions of the Minister of Information as from 1995. Thus, references in the Press Law to the Minister of Information are to be understood as references to GABINFO.[1177]

Article 3 of **Decree 4/95** sets out the functions of GABINFO, which include the following:

- to advise the Prime Minister in matters relating to the mass media
- to facilitate interaction between the government and the mass media
- to promote interactions between ministerial spokespeople and the mass media
- to promote the public dissemination of information regarding governmental activities
- to facilitate access to information by the mass media on government activities
- to make proposals to support the mass media
- to exercise state oversight over public or state organs of communication.

Additional functions were added by **Diploma 2/2005**, issued by the Prime Minister. so that GABINFO now accredits and registers foreign correspondents and publications and takes responsibility for the registration and licensing of the mass media. [1178]

The **1991 Press Act** governs the **mass media**, which covers **print, broadcasting and cinema**. This law requires the mass media to register with Gabinfo before commencing operations.[1179] Registration is not discretionary; it may be refused only if the applicant has not complied with the legal requirements and conditions.[1180] Gabinfo may exempt a print media entity from the registration requirements if its circulation is less than 500 copies.[1181]

With respect to print media, the Press Act requires periodical publications to display a significant amount of information in every publication that is printed, including details about the identity of the owner, editor, directors and printer as well as information about the publication's circulation. A publication that does not comply with this duty or an unregistered publication is considered to be "clandestine", which means that the police, military and administrative authorities can confiscate it. Writing, editing,

[1176] Lei nº 18/91 de 10 de Agosto: Lei de Imprensa, Article 37. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 10: Mozambique", Konrad Adenauer Stiftung, 2021, page 92.
[1177] Limpitlaw, pages 93, 95-96, 129.
[1178] Id, pages 120, 129-130.
[1179] Lei nº 18/91, Article 19(1); Limpitlaw, page 96. As noted above, references in the Press Law to the Minister of Information are to be understood as references to Gabinfo.
[1180] Id, Article 22; Limpitlaw page 97.
[1181] Id, Article 24. Limpitlaw, page 97.

printing, distributing or selling a clandestine publication is an offence.[1182] Unregistered broadcast media or cinema operators can also be "clandestine".[1183]

The Press Act requires all broadcasters to air official government news disseminated by GABINFO, at no cost.[1184]

The Press Act also governs journalists working in both print and broadcast media. The **rights of journalists** under this law include (amongst others):

- unfettered access to public places they deem necessary to exercise their profession
- the right not to be detained, excluded or otherwise impeded from being in any location necessary for them to exercise their profession
- the right to refuse to hand over their working materials in response to an illegal request to do so

Journalists also have a right of recourse to competent authorities for any infringements of their professional rights. Furthermore, in the case of violence, intimidation, aggression or attempts to corrupt faced by a journalist in the exercise of his or her profession, the employer must institute legal proceedings against the perpetrator. [1185]

The corresponding **duties of journalists** include:

- respecting the rights and liberties of citizens
- producing information that is complete and objective
- exercising their profession with rigour and objectivity
- rectifying false or inaccurate information that was published
- refraining from endorsing hatred, racism, intolerance, crime or violence
- refraining from engaging in plagiarism, slander, defamation, lies, accusations without any factual basis, injurious reporting, falsifying documentation, or using his or her professional prestige for personal or material gain.[1186]

The Press Law also provides for the **accreditation of journalists**. Local correspondents and part-time contributors must be accredited by the media house that employs them, while the government may regulate the activities of foreign correspondents.[1187]

In general, the Press Law provides detailed rules governing the **right to reply**, which must be afforded to any person (both individuals and legal entities) who considers themselves to have been injured by the publication of false or incorrect information affecting their moral integrity and good name.[1188] It also provides that a media outlet

[1182] Id, Articles 15(1) and 50. Limpitlaw, page 98.
[1183] Limpitlaw, pages 101-103.
[1184] Lei nº 18/91 de 10 de Agosto, Article 13; Limpitlaw, page 103.
[1185] Id, Article 27; Limpitlaw, page 94.
[1186] Id, Article 28; Limpitlaw, page 94-95.
[1187] Id, Article 32; Limpitlaw, page 95.
[1188] Id, Articles 33-34; Limpitlaw, page 100.

(print or broadcast) is civilly liable for publications or broadcasts which are injurious or contrary to legally-protected rights. It provides for joint responsibility between the person who produced the content and the media entity that published or broadcast it. An editor who had knowledge of the problematic material and did nothing to stop it also shares in civil liability. It requires that any court decision in a civil action for injurious material must be published or broadcast, together with the relevant facts, the identities of the complainant and the respondent in the matter and the sanction imposed by the court. Failure to do this constitutes the offence of disobedience, which is punishable by a fine. The Press Law also requires the offenders to be subject to internal disciplinary procedures in addition to any civil or criminal proceedings.[1189] The Press Law also covers criminal liability for defamatory material, as discussed below under content-based offences.[1190]

In addition to registration under the Press Act, radio and television broadcasters also have to be licensed by GABINFO in terms of **Decree no. 9/93 (The Broadcasting Decree)**.[1191] Radio Mozambique and Mozambique TV are state broadcasters that operate under separate decrees;[1192] neither operates independently.[1193]

Law no. 8/04 on Telecommunications, as amended by Law no. 4/2016, governs telecommunications networks and services generally, including the licencing of such services, and establishes the National Institute of Communications of Mozambique ("Instituto Nacional das Comunições de Moçambique (**INCM**)"). In 2019 INCM was renamed the Communications Regulatory Authority ("Autoridade Reguladora das Comunicações de Moçambique (**ARECOM**)"), but the name was changed back to **INCM** in 2020.[1194]

In 2017, **Law no. 3/17 on Electronic Transactions** established a legal framework for electronic transactions and addressed certain cybercrimes. This law is implemented by a regulatory entity called the National Institute of Information and Communication Technologies ("Instituto Nacional de Tecnologias de Informação e Comunicação (**INTIC**)".[1195]

The International Press Institute published the following assessment of the **media regulatory environment** in August 2022:

[1189] Id, Articles 41-42, 49, 53-54; Limpitlaw, page 110.
[1190] Id, Articles 43-ff.
[1191] Limpitlaw, pages 121-123.
[1192] Id, page 124. (Decree No 18/1994 governs Radio Mozambique, and Decree No 31/2000 governs Mozambique TV.)
[1193] Id, page 89, with details at pages 124-ff.
[1194] Lei n.º 8/04 de 21 de Julho: Aprova a lei das Telecomunições. This law was amended by Lei n.º 4/16. For a brief overview of this law in English, see Vanessa Manuela Chiponde, "Brief Remarks on the Licensing of Telecommunications Services under the New Telecommunications Legislation", *SAL & Caldeira Newsletter*, N.º 32, 2017, page 2; "Mozambique Regulatory Authority Name Changed to ARECOM", Approve-IT, 6 August 2019; "Mozambique Type Approval Authority Changes to INCM", Approve-IT, 29 May 2020.
[1195] Law n.º 3/17 de 9 de Janeiro establishes INTIC as the regulatory entity of the ICT sector. **Decree no. 60/2017** of November 6 redefines INTIC's authority to regulate and supervise the ICT sector. **Decree no. 82/2020** of September 10, establishes INTIC as a Regulatory Public Institute of ICT, coordinator of digital governance and Internet governance. **Decree No. 90/2020** of October 9 revokes Decree No. 60/2017 and establishes INTIC as a Public Institute regulating ICT and coordinating digital and Internet governance. Prof. Doutor Eng. Lourino Chemane, "Política para a Sociedade de Informação de Moçambique e Lei das Transacções Electrónicas: Grau de Implementação, Desafios e Perspectivas", INTIC. 29 Julho de 2021, Powerpoint: " 2. Contexto de Governação de TIC no País".

A key concern is the uncertain and unclear legal and regulatory environment under which the country's media operate. The country's constitution, 1991 Press Law, and 2014 freedom of information law set out strong formal press freedom and access to information guarantees. However, in practice implementation of these guarantees is weak and media are subject to a range of informal government controls that restrict access to information and limit independent reporting on a range of important issues of public interest, including the use of state resources and the conflict in Cabo Delgado.

The media are also subject to strong controls by the government's information office, known as GABINFO, which is under the auspices of the office of the prime minister. This is especially evident in the area of accreditation of journalists, which GABINFO uses as a tool to control the press, and particularly the work of foreign journalists.

Mozambique is currently considering two draft media laws that are intended to update the 1991 Press Law – a goal that is broadly shared in principle by numerous stakeholders. However, the draft media laws in their current form would be a major setback for press freedom and require urgent revision in a number of areas in order to bring these proposals into alignment with domestic, regional, and international democratic standards and obligations. Of paramount importance is to ensure that any media regulatory body be fully independent of the government – including regarding the procedures for nominating the body's members – and have a clearly defined mandate under the law.[1196]

The laws referred to in this assessment are the proposed **Law on Social Communications**[1197] that would replace the 1991 Press Law with new rules to regulate print media, and the proposed **Law on Broadcasting**[1198] that would set out new rules for radio and television. It is reported that the initial drafts were developed without sufficient consultation with stakeholders, and they have been criticised on the basis that they attempted to codify some of the most problematic informal government controls over the media.[1199]

Commenting on these two proposed laws for this study, Armando Nhantumbo, an investigative journalist and media and communication expert affiliated with MISA Mozambique, indicated that the proposals have not only complicated already tense relations between the media and government, but also ongoing discussion around media self-regulation.[1200] It seemed clear, according to Nhantumbo, that the government was "doing all they can do to control the media", through measures like increasingly onerous accreditation processes for journalists, before any effective self-regulatory mechanism emerged. He also indicated that the proposals came at a time, and complicated engagements, when MISA Mozambique and other stakeholders were in discussions with the government around "a specific law dealing with these issues related to cyber security and cyber crime".

[1196] "Mozambique: Urgent action needed to safeguard press freedom and democracy", International Press Institute, 21 August 2022
[1197] Lei da Comunicação Social (draft law in Portuguese).
[1198] Lei da Radiodifusão (draft law in Portuguese).
[1199] "Press Freedom: Mozambique", International Press Institute, December 2022, page 9; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.
[1200] Armando Nhantumbo was interviewed via Zoom on 20 July 2023.

According to the International Press Institute, the proposed **Law on Social Communications** would establish a formal licensing regime for all journalists, including those who work in online media. It would require anyone practising journalism in Mozambique to obtain a professional license - a certification that would ultimately be approved by the government, cementing the press accreditation system handled by GABINFO that many journalists and civil society stakeholders say is a powerful tool to censor and control the press. It would also introduce a new code of conduct for journalists and impose new rules for the registration of media companies. Other key concerns are the proposal to establish a new media regulator with insufficient safeguards for its independence, proposed new restrictions on the operation of foreign media in the country, and worrying overlaps between disciplinary and supervisory bodies. One newspaper editor said about the proposed laws would treat journalists as "the enemy". These two proposed laws are still under discussion as of mid-2023.[1201]

Another restrictive law proposed in 2022 is the **Draft Law on the Creation, Organization, and Operation of Nonprofit Organizations**. The stated aim of this law is to counter money laundering and terrorist financing, which is an understandable goal given the ongoing insurgency by an Islamic State-linked armed group, locally known as Al-Shabab or Mashababos, in the Cabo Delgado area. However, the bill has been criticised for imposing excessive requirements on the creation of organizations and giving government officials excessive discretion in deciding whether to authorize new organizations. For example, Article 7 of the bill invalidates the establishment of nonprofit organizations "whose purpose is legally impossible, indeterminable, contrary to the law, public order or social morality." The bill also imposes burdensome and unjustified reporting requirements, allows for the arbitrary dissolution of organizations, imposes excessive civil liability on the officers and members of organizations and provides for excessive government surveillance. There are concerns that the bill could restrict the freedom of expression of groups who want to advocate changes in law or policy by peaceful means as well as placing undue limitations on freedom of association.[1202] The bill was set to be considered by Parliament in 2023.[1203]

According to Armando Nhantumbo, of MISA Mozambique, this proposed law was an example of how the government was using the insurgency in Cabo Delgado as an excuse to "throttle the space of civil society" because in Mozambique civil society was widely regarded as the "main opposition for the government" and was seen by many as "doing the critical work in terms of defending the democracy".

Nhantumbo believed that the three problematic proposed laws discussed above have not been pushed for enactment because of the critical reporting by the media and the outcry of civil society with elections looming in both late 2023 and 2024, but that these proposed laws could well re-emerge after the elections.

[1201] "Press Freedom: Mozambique", International Press Institute, December 2022, page 9; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.
[1202] "Preliminary Analysis of Mozambique's 2022 Draft Law on Non-Profit Organizations", American Bar Association Center for Human Rights, November 2022 contains a detailed analysis.
[1203] "Mozambique: Lawmakers should reject restrictive NGO law", International Press Institute, 27 February 2023.

12.2 CONSTITUTION

Article 48 (quoted on the first page of this chapter) guarantees the right of freedom of expression only to *citizens*, not to all persons, which is unique amongst SADC states.

A more positive attribute of the provision is that it specifically discusses freedom of the press, with an unusual degree of detail about what freedom of the press entails, including "freedom of journalistic expression and creativity, access to sources of information, protection of independence and professional secrecy, and the right to establish newspapers, publications and other means of dissemination". The reference to "the right to establish newspapers, publications and other means of dissemination" appears sufficiently wide to capture broadcast and online media, while the reference to "professional secrecy" would presumably protect the confidentiality of sources. The right of the press to have access to sources of information is also very useful - especially now that it is reinforced by access to information legislation. It is also unusual and noteworthy that the Constitution requires the State to guarantee the "independence of journalists from the Government, the Administration and other political powers", and requires public sector media to include "the expression and confrontation of ideas from all currents of opinion". However, it has been noted that these promises of journalistic independence and diversity in public media are not observed in practice.[1204]

Another feature of Article 48 that is unusual in Southern Africa is the express statement that the exercise of freedom of expression and the right to information "shall not be restricted by censorship". However, the meaning of censorship is critical here; it is not clear if it means only that any laws restricting the rights in question must satisfy the constitutional requirements for limitations set out in section 56, or whether the prohibition on censorship adds another element that strengthens the rights.[1205]

According to **Article 43**, the constitutional principles in respect of fundamental rights – which includes the right to freedom of expression – "shall be interpreted and integrated in harmony with the Universal Declaration of Human Rights and with the African Charter of Human and Peoples Rights".[1206]

Article 48 was applied to protect journalists in a relatively recent case. In July 2018, the Mozambican government introduced a new licensing structure for media practitioners that set high accreditation fees, in **Decree No. 40/2018**. This decree required local freelance journalists to pay more than US$500 in annual accreditation fees, while foreign correspondents living in Mozambique had to pay over US$8,600 annually to report on the country. Other foreign correspondents were charged US$2,500 per trip to Mozambique for media accreditation. In August 2018, six rights

[1204] Limpitlaw, page 74.
[1205] This discussion draws in part on Limpitlaw, pages 72-74, 88. Limpitlaw says at page 74 that Article 48 includes an explicit reference to "training of journalists", but no reference to such training could be located.
[1206] Mozambique's 2004 Constitution (revised 2007) (in English), Article 43.

groups[1207] brought a petition against this law, and the Constitutional Council (the country's highest authority on constitutional law[1208]) found that these prohibitive fees deterred and inhibited the practice of journalism, thus violating constitutional standards of promoting a free press. The Council of Ministers accordingly revoked Decree No. 40/2018 in May 2020.[1209]

Article 41 of the Constitution provides: "All citizens shall have the right to their honour, good name and their reputation, as well as the right to defend their public image and to protect their privacy." This right is often raised in defamation cases. Since both this right and the right to freedom of the press are presented as part of the fundamental rights, duties and freedoms protected by the Constitution, cases where they clash require a balancing of constitutional rights.

One such instance is the 2015 case of ***Public Ministry v Castel-Branco and Mbanze***. In November 2013, Carlos Nuno Castel-Branco, a renowned economist, posted a public letter on Facebook criticizing the President of Mozambique. This post alleged that the President was out of control, had verbally attacked citizens who spoke out against the regime, had mocked the poor by claiming they were lazy and wanted to remain in poverty, and had appropriated Mozambique's wealth. The post also compared the President to fascists and dictators such as Hitler, Mussolini, Salazar, Franco and Mobutu, and declared that he was not fit to represent the people of Mozambique. Mbanzi, the editor of the newspaper *Mediafax* shared the post on his Facebook page, and published it in the newspaper's next print edition, clearly attributing it to Castel-Branco. Castel-Branco was charged with slander and libel of the President of the Republic, while Mbanze was charged with the crime of abuse of press freedom.

Castel-Branco argued in his defence that the post was a personal opinion about government affairs that was protected by the constitutional right to freedom of expression, as well as by international human rights conventions that Mozambique has joined. He asserted that he had no intention to offend the President, but rather to criticize the instability of the government. Mbanze raised the constitutional right to freedom of expression and freedom, as well as arguing that the post was already public before he re-published it and that political figures such as the President are not afforded the same protection as ordinary individuals in terms of their reputation and must be expected to tolerate criticism of their official functions.

The District Court of Kampfumo acquitted both men. It found that Castel-Branco's statement did not constitute slander or libel, but was a constitutionally protected form of expression, especially considering the President's role as a public figure. It held that Castel-Branco's right to freedom of expression trumped the President's right to privacy and the protection of his reputation. Since Castel-Branco's statement was

[1207] The six petitioners were the Media Institute of Southern Africa (MISA) Mozambique Chapter, the Association of Journalistic Companies, the National Forum of Community Radios, the Centre for Public Integrity, the Mozambican Bar Association and the Emergency Committee for the Protection of Fundamental Freedoms.

[1208] Mozambique's 2004 Constitution (revised 2007) (in English), Articles 240-248. Note that Article 244 was amended in 2018 by Lei n.º 1/18.

[1209] "Digital Rights in Mozambique", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraphs 6-7; "Mozambique: New Media Fees Assault Press Freedom", Human Rights Watch, 17 August 2018; "Mozambique: Government revokes decree on media fees", Club of Mozambique, 21 May 2020.

constitutionally protected, Mbanze's republication of it was similarly protected. The Court also found that it was normal in a democracy for the President to face criticism, which is part of healthy engagement in a democratic society. It also highlighted the need for open debate on issues of public interest, noting that the President has ample opportunity to refute criticism. in short, the case upheld the right to criticize the President, as long as criticism is not made with ill intent, and reaffirmed the concept that public figures must tolerate greater criticism than ordinary individuals.[1210]

Another fundamental constitutionally-protected right is contained in **Article 39**, entitled Acts against National Unity. It states: "All acts intended to undermine national unity, to disturb social harmony or to create divisions or situations of privilege or discrimination based on colour, race, sex, ethnic origin, place of birth, religion, level of education, social position, physical or mental ability, the marital status of one's parents, profession or political preference, shall be punished in terms of the law." This right is matched by a duty in **Article 44**: "All individuals shall have the duty to respect and consider their fellow beings without any form of discrimination whatsoever, and to maintain relations with them aimed at promoting, safeguarding and strengthening respect, mutual tolerance and solidarity." These provisions might have to be balanced against freedom of expression in some instances.[1211]

12.3 CASE STUDIES

In August 2022, the International Press Institute expressed concern about "reports of escalating physical attacks and threats against journalists, together with a pattern of impunity for these crimes".[1212]

According to the US State Department's 2022 Country Reports on Human Rights Practices, although the Constitution and the law provide for the right to freedom of expression, including for members of the press and other media, the government did not always effectively protect or respect this right. "Academics, journalists, opposition party officials, and civil society reported an atmosphere of intimidation and fear that restricted freedom of speech, the press, and other media. Journalists expressed concern regarding government intimidation by security forces." [1213]

[1210] *Public Ministry v Castel-Branco and Mbanze* (in Portuguese), 15 September 2015. The discussion of the case in the text relies entirely on the case summary by Global Freedom of Expression here.
[1211] Limpitlaw, page 78.
[1212] "Mozambique: Urgent action needed to safeguard press freedom and democracy", International Press Institute, 21 August 2022.
[1213] "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1A, 1C and 2A.

The International Press Institute raised concerns in 2022 about informal control over freedom of expression:

> In practice the country's media are subject to strong informal controls by the country's ruling party, Frelimo, which exerts power over the media through different bodies and mechanisms and in a number of areas not clearly established in law. Therefore, despite formal legal press freedom guarantees, journalists are in practice not free to cover certain topics without risk of retaliation, particularly related to reporting on the conflict in the Cabo Delgado province in the north. Other "red-line" topics include corruption, organized crime, security issues, and poaching in certain areas in Mozambique. There was also a clampdown on journalists leading up to the presidential and provincial elections in October 2019.[1214]

Reporting on Cabo Delgado, where some of the world's largest reserves of natural gas were discovered in 2010, has been a particular challenge since the outbreak of an Islamic insurgency in the region in 2017. Access to the area is tightly controlled, requiring permission from multiple authorities, including the region's governor and the local police - who reportedly tend to favour journalists working for state media. President Nyusi has made speeches accusing journalists and civil society organizations of spreading false information about Cabo Delgado, which has helped lead to self-censorship of reporting on Cabo Delgado that does not align with government positions. Journalists working in the region often risk police retaliation and harassment, including arbitrary detention and arrest, threats and intimidation.[1215]

- For example, in October 2022 police arrested journalist Arlindo Chissale in the Cabo Delgado Province and detained him for five days. He was initially accused of **terrorism and gathering information for terrorism purposes**, crimes that carry a penalty of up to 20 years in prison. He was provisionally released after a district court judge found that there wasn't a strong enough case to keep him in detention, pending the outcome of an investigation into a lesser charge of **working as a professional without a license or valid accreditation** under Article 344 (3) of the Penal Code which is punishable with a fine. These charges were not pursued after his press credentials were produced to the police.[1216]
- In 2021 GABINFO **revoked the press accreditation** of British journalist Tom Bowker, the editor of a newsletter that covers politics, economics, and the extractives industry in Mozambique. Having thus lost the basis for his visa, he was **expelled** from Mozambique by immigration authorities, who banned him from the country for 10 years. Bowker believes that these moves were politically motivated, sparked by this reporting on the extractive industry in Cabo Delgado. [1217]

[1214] "Press Freedom: Mozambique", International Press Institute, December 2022, page 8.
[1215] Id, page 14; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), pages 41-43.
[1216] "Mozambican journalist Arlindo Chissale faces lesser charge after terrorism accusation", Committee to Protect Journalists, 15 November 2022; "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, section 2A.
[1217] "Press Freedom: Mozambique", International Press Institute, December 2022, page 11; "Mozambique expels British journalist Tom Bowker, bans him for 10 years", Committee to Protect Journalists, 16 February 2021.

- One of the most serious cases in recent years took place in 2020, when journalist Ibraimo Mbaruco disappeared in the conflict area of Cabo Delgado. Mbaruco, a journalist for *Palma Community Radio*, was last heard from on April 7, when he sent a text message to a colleague saying he was "surrounded by soldiers". Mbaruco's brother says that Mbaruco was on his way home from work that evening when he met a group of soldiers. He sent a text message to a colleague, asking him to call because the soldiers were harassing him. When the colleague tried to call, Mbaruco's phone went unanswered. One report states, on the basis of information from a police officer, that he was taken by members of the Mozambican army from Palma to Mueda, where the army has an interrogation room. The circumstances led human rights groups to worry that Mbaruco was **forcibly 'disappeared'**. He is still missing.[1218]

Turning to some specific incidents in other areas, in June 2023, Leonardo Gimo, a reporter for the privately owned broadcaster *TV Sucesso*, was charged with **criminal defamation** in connection with a report on police corruption in 2022. A complaint was laid by a police official who claimed that the report tarnished the reputation of the police. Gimo had been briefly detained in 2022 on suspicion of terrorism after he spoke to other persons who were suspected of terrorist acts. On that occasion, he was questioned for more than an hour and then released with an apology after the police searched his bag, which contained his camera and laptop, and confirmed his identity. The police officer who made the complaint about the report on allegations police corruption believes that this report on corruption was motivated by spite for the journalist's previous detention.[1219] The International Press Institute commented that the case against Gimo "underscores the crucial role played by journalists in promoting transparency and accountability within society. Journalists serve as watchdogs, exposing wrongdoing and holding those in power accountable. By pursuing criminal charges against Gimo, the authorities risk stifling investigative reporting and hindering the flow of vital information to the public."[1220]

In March 2023, there were protests across the nation to remember the artist, Azagaia, who sang about poverty and injustice and urged people to hold authorities to account. Azagaia died suddenly on 9 March 2023, which inspired the wave of demonstrations. According to Amnesty International, at least seven protesters and organisers were **arrested** in connection with rallies in five different locations. Amnesty International condemned the heavy-handed response by police to these peaceful demonstrations, which included **beating up protesters with batons**, commenting: "There's no doubt that police were aiming to suppress the demonstrations, with the intention of belittling Azagaia legacy in Mozambique. Police's actions, seen beating

[1218] "Radio journalist Ibraimo Abú Mbaruco missing in Mozambique", Committee to Protect Journalists, 17 April 2020; "Mozambique: Journalist Feared 'Disappeared'", Human Rights Watch, 17 April 2020; "Media, Rights Watchdogs Worry Over Missing Mozambique Journalist", AFP - Agence France Presse. 17 April 2020; "Cabo Delgado: Two years on, Ibraimo Mbaruco's disappearance remains unanswered – DW", *Deutsche Welle*, 8 April 2022; Nompilo Simanje, "The right to truth: IPI demands justice for killed journalists in Africa", International Press Institute, 30 March 2023.

[1219] "Mozambique: IPI calls on authorities to drop criminal defamation and slander case against journalist Leonardo Gimo". International Press Institute, 30 June 2023; "Mozambican journalist Leonardo Gimo investigated for criminal defamation over report on alleged police corruption", Committee to Protect Journalists, 27 June 2023; Olalekan Adigun, "Calls to Drop Criminal Defamation Case against Journalist Leonardo Gimo in Mozambique", 30 June 2023.

[1220] Olalekan Adigun, "Calls to Drop Criminal Defamation Case against Journalist Leonardo Gimo in Mozambique", 30 June 2023.

up protesters in videos supplied to Amnesty International and shared on social media, are a disturbing pattern of reckless and unlawful tactics against people during the protests."[1221]

In January 2023, five Mozambique border police officers **detained and beat** journalist Rosário Cardoso, He was returning home in the evening from his shift at the community radio station *Thumbine* in the eastern province of Zambezi when the officers stopped him and demanded to know why he was out so late. Several other people were also detained, with the exercise apparently being aimed at soliciting bribes. When he protested about the bribes, two officers threw him on the ground, beating him on the buttocks repeatedly while telling him, "Mister journalist, here you don't speak." Cardoso was then released, and treated at a local clinic. He managed to lay a charge after some difficulty. The radio coordinator at the same station commented that "intimidation and threats against journalists in the province are frequent, and violence from authorities towards the media worsens in election years."[1222]

In 2022, a court acquitted Armando Nenane, a journalist and director of the *Crónica Jurídica e Juduciária* magazine in Maputo, of charges of **document forgery** and **defamation** brought by the former Minister of Defence. After this, two unidentified men handed a live bullet to Nenane, claiming to be acting on orders from their superiors. Undeterred, Nenane has filed a defamation suit against the former Minister,[1223]

The US State Department's 2022 Report on Human Rights Practices states that police and other government officials have been accused of violent or excessive responses to protests. It cites several such instances in 2021 and 2022:

- In January 2022, police reportedly locked a local human rights organization's press conference and briefly detained the organizer, then blocked a subsequent press conference.
- In March 2022, police in Zambezia Province reportedly killed two individuals and injured a third in response to a protest. According to local media, the provincial police commander stated that the killings were unintentional.
- In August 2022, police reportedly used live ammunition to disperse merchants in Manica Province who blocked traffic while protesting market conditions. Three protesters were injured three 21 protesters were arrested.
- In another incident in August 2022, Maputo city government authorities sent police with dogs to scatter young protesters demanding more job opportunities outside the Municipal Council.
- Also in August 2022, four National Criminal Investigation Service (SERNIC) officers attacked two television journalists covering the funeral of a police officer and destroyed the memory cards from their cameras. There were also reports that the

[1221] "Mozambique: Arbitrary arrests, teargassing and brutal assault of peaceful protesters a violation of the right freedom of assembly", Amnesty International, 18 March 2023.
[1222] "Mozambique border police detain, beat radio journalist Rosário Cardoso", Committee to Protect Journalists, 15 February 2023.
[1223] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.

officers threatened to shoot the journalists as they left. The reporters filed a complaint with police, which SERNIC said it would investigate.
- In September 2022, police reportedly used tear gas to disperse vendors blocking traffic at the Maputo fish market during a protest.
- Local civil society organizations filed a petition with the Attorney General's Office asking it to hold police accountable for suppressing a December 2021 demonstration against domestic violence by briefly arresting 19 women's rights activists. [1224]

Other similar incidents during the last few years could be cited.[1225]

12.4 CYBERCRIME

Currently, the main pieces of legislation on cybercrime are the **2019 Penal Code**[1226] and **Law no. 3/2017 on Electronic Transactions**.[1227] Content-based offences which are not limited to cybercrime can be found in the **1991 Press Law**[1228] and the **2019 Penal Code**.[1229] There are also some relevant provisions on international cooperation in **Law no. 14/2013 on Preventing and combating money laundering and financing of terrorism**.[1230]

A) TECHNICAL OFFENCES

In the 2019 **Penal Code**, Articles 336 to 339 are dedicated to *Computer fraud and related crimes*. This section contains offences on **computer fraud** (Article 336), **data interference** (Article 337), **systems interference** (Article 338) and **misuse of devices** (Article 339). Crimes committed under any of these articles can lead to a penalty of imprisonment from 1 to 2 years and a fine. Under Article 336, if there are aggravating circumstances, the penalty can go up to 8 years of imprisonment. **Illicit (illegitimate) access to computer systems** is covered by Article 256 and punishable with imprisonment from 1 to 2 years and a fine. The **creation of computer programs and other instruments to commit e-payments fraud** is addressed in Article 294 (Frauds related to e-payment channels and tools), with a penalty of imprisonment from 1 to 3 years and a fine.[1231]

[1224] "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1A, 1C, 2A and 2B. See also "Two journalists in Mozambique attacked by police while covering officer's funeral", Committee to Protect Journalists, 15 August 2022.
[1225] See "Mozambique Archive", Committee to Protect Journalists.
[1226] Lei n.º 24/19 de 24 de Dezembro: Lei da Rivisão do Código Penal, which replaces the 2014 Penal Code, as amended by Lei n.º17/20 de 23 de Dezembro (which adds a provision on trafficking in persons).
[1227] Lei n.º 3/17 de 9 de Janeiro: Lei das Transacções Electrónicas (Law on Electronic Transactions).
[1228] Lei nº 18/91.
[1229] Lei n.º 24/19 de 24 de Dezembro.
[1230] Lei n.º 14/13 de 12 de Agosto: Lei de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo (Law to Prevent and Combat Money Laundering and Terrorism Financing), as amended by Lei n.º 11/22 de 7 de Julho; "Mozambique: State of cybercrime legislation", Octopus Cybercrime Community, Council of Europe, undated.
[1231] Lei n.º 24/19 de 24 de Dezembro; summary based on "Mozambique: Substantive Law", Octopus Cybercrime Community, Council of Europe, undated.

The **Law no. 3/2017 on Electronic Transactions**, in Article 67, lists several actions that constitute offences:

a) **illegal access** to all or part of a computer system or computer network, through a breach of security measures, with the intention of obtaining data or another dishonest intent;
b) **illegal interception** of private data transmissions, carried out by technical means;
c) **intentional interference with data**, consisting of damage, deletion, deterioration, alteration or suppression;
d) **intentional interference with information systems**, which means affecting the functioning of a computer or computer network through the introduction, transmission, damage, elimination, deterioration, alteration or deletion of data;
e) **misuse of devices**, intentionally and without permission, which causes the loss of the property of another person through any introduction, alteration, deletion or deletion of data and any interference with the operation of a computer system or computer network;
f) **violation of a domain name**: violation of a domain name, misuse of a domain name, the name of an individual or a legal entity, or a name that is protected as an intellectual property right, or is so substantially similar to another that it is likely to create confusion, in order to benefit from it;
g) **breach of security of an electronic payment instrument**, or the production, acquisition, transfer, storage or offer to make available equipment, computer programs or any data designed or specially adapted to violate a security system related to an electronic payment instrument;
h) **supply to the public of an electronic payment instrument without authorization** from the Bank of Mozambique;
i) **unsolicited commercial electronic communications:** sending unsolicited commercial communications to a person who has informed the sender that such communications are undesirable;
j) **obstruction of, or refusal to cooperate with, an investigation** by competent authorities;
k) **breach of accreditation obligation**: provision of certification services, and delivery of qualifying certificates without accreditation by the competent services;
l) **breach of cryptography:** breach of the duty to declare the use and provision of encryption services as required under this Law;
m) **breach of data protection duty**: breach of the obligations of the data processor set out in this law.

The penalty for these crimes is a fine expressed in "minimum wages". The penalty for the listed crime ranges from a minimum of 30 or 40 minimum wages (depending on the crime) to a maximum of 90 minimum wages, with enhanced penalties where the perpetrator was a civil servant. Where the crimes listed overlap with other criminal laws (paragraphs (f), (i), (j), (k), (l) and (m)), the heavier criminal penalty applies. [1232]

[1232] Lei n.º 3/17, sections 67-68; see also "Mozambique: Substantive Law", Octopus Cybercrime Community, Council of Europe, undated.

On 22 November 2022, INTIC published a **draft Cybersecurity Bill**.[1233] This proposed bill would consolidate the national framework on internet regulation in Mozambique. The bill aims to ensure the protection of digital networks, information systems, and critical infrastructures in cyberspace. It would establish a National Cyber Security Council (CNSC) chaired by the Minister of Information and Communication Technology responsible for ensuring the alignment of policies and strategies on cybersecurity. The law is currently open for public comment, but no deadline for submissions has been announced.[1234]

The draft law, as its name indicates, focuses on cybersecurity rather than cybercrime, and does not appear to replace the existing cybercrime offences in the Penal Code and Law no. 3/2017 on Electronic Transactions. The draft would require data processors and controllers of electronic communications networks and information society systems to preserve data, including traffic data for 6 months, taking care to ensure its security and confidentiality. Certain specified service providers must retain traffic and location data and other data sufficient to identify the subscribers or users of publicly available digital services or main storage services for 12 months, for the purpose of investigation, detention and repression of crimes. There are also requirements concerning the linkage of IP addresses to physical locations. The draft bill also addresses responsibilities in connection with preservation orders ("*ordenada à conservação*") and orders for production ("*produção*") of traffic and location data under other laws. The data storage requirements would also apply to communications that are initiated or concluded outside Mozambique.[1235] The Bill would also provide for the creation of the National Cyber Security Council, a body that will work towards the alignment of policies on cybersecurity.[1236]

B) CONTENT-BASED OFFENCES

In some cases, there are overlapping and unharmonized offences in the **1991 Press Law**[1237] and the **2019 Penal Code.**[1238] However, the Penal Code takes precedence, repealing any other laws that are contrary to its provisions.[1239]

In general Article 51 of the Press Law **authorises a court to suspend a publication or broadcast service** if the court finds that it has made public content that disrupts public order, violates rights of citizens or incites the commission of crimes.[1240]

[1233] Proposed Law on Cybersecurity (in Portuguese). This is "Version 3.0" of the draft, dated 30 March 2023. Note that it is dated *after* the version marked "Version 4" on the INTIC website and identified by INTIC as being the most up-to-date version. See "Proposta de Lei de Segurança Cibernética", the page of the INTIC website which has links to download the different versions of the bill. The initial bill has already been revised from previous versions to take account of public and stakeholder input, but as of July 2023, the process of consultation on the proposed bill was still underway.

[1234] "Mozambique: New cybersecurity law proposed", alt.advisory, 29 November 2022 (note that the link in this article references the initial version of the bill which has since been revised); "Mozambique examines proposed cybersecurity law", *360 Mozambique*, 12 July 2023.

[1235] Proposed Law on Cybersecurity, Version 3.0 (in Portuguese), Articles 26-31.

[1236] Id, Article 7-ff.

[1237] Lei nº 18/91.

[1238] Lei n.º 24/19 de 24 de Dezembro.

[1239] Id, Article 2(2).

[1240] Lei nº 18/91, Article 51(1); Limpitlaw, pages 111-112.

The list here is not comprehensive, but it captures in particular criminal defamation (which is a frequently-used tool to silence speech) and the offences that are found in cybercrime laws in other SADC countries.

Criminal defamation: The 2019 **Penal Code** contains a chapter on Crimes Against the Dignity of Persons. Article 233 deals with criminal defamation. It is an offence to defame another person publicly by offending their honour or reputation through spoken word or words or images spread through any medium of dissemination. The penalty is up to one year's imprisonment and a corresponding fine. It is a defence if the publication was done to protect legitimate interests and the statements were true, or the person who made the statements believed in good faith that the facts were true. However, this defence does not apply if the defamatory statements concerned another's private or family life. Article 234 provides a similar offence of injuria, which concerns damage to another's dignity. There is an enhanced penalty for defamation or injuria against the President or other specified officials (Article 237).[1241]

Article 42 of the **Press Law** states that general criminal legislation applies to abuses of the press that violate protected interests, with some special provisions – although Article 47 discusses the crime of defamation in a manner that overlaps the Penal Code. As in the case of civil defamation, liability for criminal defamation under certain circumstances can potentially be shared by the author or producer of the material, the editor, the managing director of the publication or broadcaster, and the members of the editorial board. Article 46 of the Press Law makes it an aggravated offence to publish or broadcast material that constitutes injury, threats, defamation or calumny against the President, members of government and Parliament, magistrates, public authorities, foreign governments or accredited diplomats. A periodical publication that is found to have published defamatory material on three or more occasions within five years can be suspended for time periods set out in Article 48. State-employed journalists can also be penalised for having abused their authority in terms of Article 52 of the Press Law.[1242]

Public order and false news: Article 396(1) of the **Penal Code** makes it a crime to incite collective disobedience of the laws that maintain pubic order through publications or public speech. It is a crime under Article 396(2) to incite violent political struggle or to publish false or biased news which may cause alarm or unrest, or divisions within the Armed Forces, between different militarized or security forces, or between any armed forces and the government bodies.[1243] Article 48(4) of the **Press Law** makes it an offence to intentionally publish or broadcast false news or unfounded rumours where this implicates the public interest or "law and order".[1244]

Hate speech: Article 191(3)of the Penal Code makes it an offence, to disseminate by any media incitement of violence, defamation or threats against a person or group based on their race, colour, ethnic origin, nationality, religion, race or gender

[1241] Limpitlaw, pages 112-113.
[1242] Id, , pages 110-112.
[1243] Lei n.º 24/19, Article 386, Limpitlaw, page 113; "LEXOTA Country Analysis: Mozambique ", last updated December 2022.
[1244] Lei nº 18/91, Article 48; Limpitlaw, page 113; "LEXOTA Country Analysis: Mozambique ", last updated December 2022.

identity.[1245] Both incitement to genocide and agreement with genocide are crimes under Article 190 of the Penal Code.[1246]

Incitement: Article 345(1) of the **Penal Code** makes it an offence to use any manner of communication to incite the commission of a crime. Under Article 345(2) it is a separate crime to instigate acts of violence and disturbance of public order for religious reasons.[1247]

Child pornography: The **Penal Code** addresses various offences relating to child pornography, defined as "any material, whatever the support or platform, that visually represents a minor or person appearing to be a minor engaged in sexually explicit behaviour". It also prohibits the use of a child in pornographic performances, in a provision (Article 212) that is worded broadly enough to criminalise those who facilitate the live-streaming of child sexual abuse, even though this is not criminalised explicitly.[1248]

Privacy: Article 252 of the **Penal Code** outlaws the non-consensual interception, recording, transmission or disclosure of online communications, including email, messages, audio-visual and social media content. It also criminalises capturing, photographing, filming, manipulating, recording or dissemination of images of persons or intimate objects or spaces, as well as "secretly observing or listening to persons who are in a private place". Another offence is the disclosure of facts concerning the private life or serious illness of another person.[1249] No specific offence on "revenge porn" (the non-consensual sharing of intimate images) was located, although it would quite possibly be captured under these privacy provisions.

Terrorism: In 2022, Mozambique enacted **Law no. 13/22: Law on the Prevention, Suppression and Countering of Terrorism and Proliferation of Weapons of Mass Destruction**. [1250] This law introduces some controversial antiterrorism measures that could restrict critical journalism and limit reporting on the conflict in the north. Article 20(2) of the new law makes it a crime to intentionally disseminate information according to which a terrorist act was or is likely to be committed, knowing that the information is false or grossly distorted, with the intention of creating public panic, disturbance, insecurity and disorder. Commentators have expressed concern that this law's loosely defined provisions could have a chilling effect on reports about national security topics and give authorities discretion to restrict a wide range of speech. Article 9 of this new law states that telecommunications network operators and service providers "shall adopt measures to control users in the context of the prevention, repression and combating terrorism". It is not clear what is meant by

[1245] Lei n.º 24/19, Article 345; Lei nº 18/91, Article 51(1); Limpitlaw, page 114
[1246] Id, Article 190(2)-(3).
[1247] Id, Article 345; Limpitlaw, page 114.
[1248] Id, Article 211-ff; Limpitlaw, page 114; "Disrupting Harm in Mozambique – Evidence on online child sexual exploitation and abuse", ECPAT, INTERPOL, and UNICEF, 2022, page 20.
[1249] Id, Article 252; Digital Rights in Mozambique ", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraph 25.
[1250] Lei nº 13/22 de 8 de Julho: Lei que Estabelece o Regime Jurídico de Prevenção, Repressão e Combate ao Terrorismo e Proliferação de Armas de Destruição em Massa. This law repealed the previous terrorism law, Lei n.º 5/2018, de 2 de Agosto.
Law on the Prevention, Suppression and Countering of Terrorism and Proliferation of Weapons of Mass Destruction (8 July 2022).

"measures to control users".[1251] The case studies summarised in this chapter indicate that charges of terrorism have been applied, or threatened, in practice.

C) STATE SURVEILLANCE AND CRIMINAL INVESTIGATIONS

Mozambique's Constitution provides strong protections for privacy. Article 41 affords all citizens the right to protect their privacy. Article 68 says that a person's home, correspondence and other forms of private communication are inviolable, except as specifically provided by law, and that entry into the home of a citizen without consent may be ordered only by competent judicial authorities, in such instances and according to such procedures as are specifically established by law. Article 65(3) says that evidence obtained through abusive intrusion into a person's private and family life or into their home, correspondence or telecommunications, shall be invalid.[1252] V**arious laws in the communication sector contain provisions that protect privacy and prohibit unauthorised interception of private communications.** [1253]

Nonetheless, there are reports the government does not always respect the privacy of personal communications, particularly in respect of civil society activists and journalists. Some civil society activists have reported that government intelligence services and ruling party operatives have monitored telephone calls and emails without warrants, conducted surveillance of their offices, and followed members of opposition parties. It has also been reported that government and party operatives have monitored social media for criticism of the government without legal authority. For example, members of civil society reported that government intelligence agents have used false names to infiltrate social network discussion groups.[1254]

Law no. 8/04 on Telecommunications, as amended by Law no. 4/16, requires all telecommunications operators to have an operational and efficient system of interception of communications, for the purpose of criminal investigations – while noting that such interceptions can be carried out only with the authorisation of a criminal investigation judge. Article 14 of **Law no. 3/17 on Electronic Transactions** similarly requires intermediate data transmission service providers to maintain the secrecy and confidentiality of all communications, with disclosure of information being allowed only upon judicial or administrative decision.[1255] This provision is

[1251] "Proposed amendment to Mozambique's anti-terror law threatens press freedom", Committee to Protect Journalists, 7 June 2022; "Press Freedom: Mozambique", International Press Institute, December 2022, page 13; 2022 Country Reports on Human Rights Practices: Mozambique", US State Department, section 2A; Dércio Tsandzana, "Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023; "LEXOTA Country Analysis: Mozambique ", last updated December 2022. Note that some secondary sources refer to the 2022 law as constituting amendments to the 2018 law on terrorism. The law as finally enacted *repealed* the 2018 law ("revoga a Lei n.º 5/2018, de 2 de Agost").

[1252] Mozambique's 2004 Constitution (revised 2007) (in English), Articles 41, 65(3) and 68.

[1253] For example, Article 10 of Decree no. 44/2019 on "Telecommunications Service Consumer Protection" provides for the consumer's right to privacy and protects against the unauthorised use personal information from their communications. Article 7 of Decree no. 66/2019 on "regulation of the security of telecommunications networks" also highlights privacy. Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.

[1254] "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1F and 2A.

[1255] Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.

weakened by the reference to "administrative" orders – which dovetails with a provision on the power of the Communications Regulatory Authority (ARECOM), which is obliged to ensure that its administrative instructions to service providers and other users of radio frequency and telecommunications numbering resources do interfere with the rights and freedoms defined by law *except* where there is justifiable fear of crime or danger to state security.[1256]

Article 222 of **Law no. 25/19, the new Criminal Procedure Code** covers the situations where wire-tapping may be permitted. It can be authorised by a judge to gather evidence on a list of crimes – some of which are serious (such as corruption, trafficking in persons and child pornography) while others are less so (disturbance of peace and quiet through electronic methods, and attacking public probity - "*probidade pública*").[1257] The use of electronic communications for criminal investigations falls under the National Service of Criminal Investigation (SERNIC), established by **Law no. 02/17**. With regard to crimes that SERNIC is responsible for investigating, interception and recording, of conversations, images or any other type of communication requires judicial authorisation.[1258]

The real problem here is not the law, but the fact that wiretaps are carried out outside the scope of SERNIC, by the State Intelligence and Security Service (SISE), "and are based merely on distrust and speculative measures and, in many situations, without any authorisation from a judicial authority".[1259]

Another problem is that the concept of "state security" which can be used to justify surveillance is broad and diffuse. **Law no. 19/91 on Crimes against State Security** states in Article 22 that defamation of the President, ministers, Supreme Court judges and even general secretaries of political parties is considered a crime against state security, punishable by one to two years of imprisonment. This means that concerns about "state security" open a wide door to monitoring the communications of citizens who are critical of the government.[1260]
In addition, the latest law on combating terrorism states that, in public places and private places of public access, measures must be adopted to prevent terrorist acts by installing means of security and electronic surveillance.[1261]

[1256] Id, page 6.
[1257] Law nº 25/19 de 26 de Dezembro: Lei de revisão do Código de Processo Penal. Article 222; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
[1258] Lei n.º 2/17 de 9 de Janeiro: Cria o Serviço Nacional de Investigação Criminal, abreviadamente designado por SERNIC (Creating the National Criminal Investigation Service, abbreviated as SERNIC), Article 21; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
[1259] Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
[1260] "Assessment of Media Development in Mozambique" MISA Mozambique for the UNESCO Communication and Information Sector, UNESCO 2011; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 6. Law no. 19/91 could not be located online.
[1261] Lei nº 13/22 de 8 de Julho, Article 8; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.

D) SIM CARD REGISTRATION

Law No. 3/17 on Electronic Transactions obligates intermediate providers to **register and identify their users** in terms of regulations issued under the law.[1262]

Mozambique has also instituted a **biometric SIM card registration** scheme, building on an existing registration scheme that did not collect biometrics. In terms of a Decree issued by INCM, anyone registering a SIM card will now be required to provide their fingerprint and face biometrics, along with an approved form of identification such as a national ID card, passport or driver's licence. The new registration process will register all mobile devices, as well as all sellers and agents of telecoms services. Two databases will be created: one to store information on subscribers' identities and devices, and one to document fraud or attempted fraud by users. It will establish a risk centre to identify fraudulent activity and implement mechanisms for blocking users suspected of fraud.[1263] The Mozambican government believes SIM card registration will be a useful tool for combating crime and fraud.[1264]

In the same vein, in terms of Law No. 3/17, while intermediate service providers have no general obligation to monitor the information they transmit or store, they do have a duty to inform the competent public authorities of illegal activities that are detected and to identify users who transmit or store data with offensive content, using the communication service with an unidentified sender.[1265]

E) TAKE-DOWN NOTIFICATIONS

No information on this topic was located.

[1262] Law n.º 3/17 de 9 de Janeiro, Article 19: User identification record.
[1263] Decree no. 13/23 of 11 April, which approves the Regulation on the Registration of Telecommunications Services (not located online); James Barton, "Mozambique implements biometric SIM registration in major overhaul", 25 April 2023; "Biometric registration of SIM cards and other changes on their way: Mozambique", Carta de Moçambique, 21 April 2023.
[1264] "Digital Rights in Mozambique ", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraph 24.
[1265] Law n.º 3/17, Article 18(1) and (2)(d) ("identificar os utilizadores que transmitem ou armazenem dados com conteúdo ofensivo, usando o serviço de comunicação com remetente não identificado").

12.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Mozambique is expected to hold elections for local government, the National Assembly and the President (who is directly elected) in October 2024.

Freedom House gives the following account of the last election in Mozambique:

The president, who appoints the prime minister, is elected by popular vote for up to two five-year terms. President Nyusi of the Front for the Liberation of Mozambique (FRELIMO) won the presidential contest in 2019 with 73 percent of the vote. Additionally, because FRELIMO won the most votes in all provinces, it received the right to select all 10 of the country's provincial governors. Turnout was reported at just over 50 percent.

The campaign was marred by violence, much of which targeted opposition members or their supporters, and several politicians and activists were killed. Anastácio Matavel, a respected independent election observer, was killed that October, with members of an elite police unit accused of carrying out the murder. Further violence was reported at dozens of polling stations on election day, as were instances of harassment of poll workers, notably those appointed by the opposition, with police taking part in the intimidation. Additionally, there were credible reports of ballot-box stuffing; interference with the registration of election observers; serious voting-register inaccuracies, particularly in Gaza Province; and tabulation irregularities. As in past elections, FRELIMO enjoyed a strong advantage due to its use of state resources to fund campaign activities and secure media coverage.

Opposition parties denounced the election as fraudulent. Civil society organizations characterized the polls as not free, unfair, nontransparent, and the worst since the introduction of multiparty democracy in 1994. They also argued that the ruling party had captured the electoral machinery through the National Elections Commission's (CNE) appointment process. International observers from the Community of Portuguese Language Countries, the European Union, and the US embassy expressed concern about the reports of irregularities and election-related violence, but ultimately recognized the outcome.

Members of the 250-seat unicameral Assembly of the Republic are elected to five-year terms. The 2019 legislative elections were held concurrently with the presidential election. FRELIMO took 184 seats, up from 144 previously. The Mozambique National Resistance (RENAMO) won 60 seats, down from 89 previously, and the Democratic Movement of Mozambique (MDM) took 6 seats, down from 17 previously.
The legislative polls were marred by the same violence, irregularities, and fraud allegations as the presidential election. International observers objected to their conduct but accepted the results; opposition parties rejected the elections; and a coalition of civil society groups called them patently flawed.

In May 2022, President Nyusi suggested postponing the election of district assemblies, which are scheduled to take place in 2024. The proposed postponement of the elections has been met with sharp criticism by the opposition; RENAMO leaders have repeatedly insisted that the elections must be held as planned. In December, Nyusi announced that a team would be established to determine the feasibility of holding

the elections as originally scheduled.[1266]

The Bertelsmann Transformation Index provides more detail about the election irregularities that took place in 2019:

The 2004 constitution of Mozambique guarantees fundamental rights and civil liberties for all its citizens. It protects the right to choose leaders through universal, direct, secret and periodic suffrage, through referenda on major national issues and through permanent democratic participation in government affairs. The right to vote is also extended to the diaspora. The constitution safeguards a two-term presidential limit. In the last elections in 2019, 26 parties and two alliances registered. Three candidates ran in the presidential elections.

Since the 1992 peace accord, Mozambique has regularly organized presidential, parliamentary and provincial elections as well as elections in the independent municipalities (autarquias). However, over the years the quality has deteriorated. Violent clashes, infringements on the right of assembly for all parties and a continuously imbalanced playing field have become characteristic of the country's electoral processes. Observers called the 2019 presidential, parliamentary and provincial elections the worst and the most blatantly rigged. Evidently, the ruling party FRELIMO did not want to take chances after years of mediocre governance and corruption scandals of unprecedented dimensions. First and foremost, the incumbent regime intended to secure an absolute majority for its presidential candidate Filipe Nyusi in order to avoid a second round where opposition parties could unite against the sitting president.

Large-scale electoral fraud began with the registration process and implicated the National Election Commission (CNE) as well as the administrative body, the Technical Secretariat for Elections (STAE). In opposition strongholds like Sofala province, registrations were limited. Many citizens had lost their identity cards in the floods following the tropical cyclone Idai that hit particularly hard Beira and Sofala province. Authorities made it difficult for citizens to receive new cards and often did not accept alternatives, thus excluding these voters from the process. In Zambezia province about 10% of registration posts were destroyed by the cyclone and many more in provinces such as Tete and Sofala.

In the FRELIMO stronghold Gaza province, the voter rolls grew by 300,000 citizens (80% of the population/national average 47%) – an amount that did not correspond with the 2017 census and which led to the resignation of the director of the National Institute for Statistics, who declared that "he remains committed to professional ethics and international standards."

For security reasons, voters could not go to the polls in three districts in Cabo Delgado (Mocímboa da Praia, Muidumbe and Macomia).

Within the ranks of local election observers a climate of intimidation was planted with the murder of the much-revered civil society activist Anastácio Matavel in Gaza

[1266] "Freedom in the World 2023: Mozambique", Freedom House, sections A1-A2.

province some days before election day. In addition, two party members, one each from FRELIMO and RENAMO became victims of politically motivated murder. CNE and STAE, their capacities and independence were largely doubted and mistrust was not only shown to CNE members with a political party background but also to those coming from civil society.

Election campaigns by the two major opposition parties, RENAMO and MDM, were continuously obstructed by roadblocks or by the occupation of spaces identified for their rallies. As in previous elections, FRELIMO made extensive use of state resources for its campaign, distorting the level playing field. An uneven playing field also existed in the media coverage of parties and elections campaigns, with more time allocated to the ruling party.[1267]

Elections are administered by the **National Electoral Commission** (*Comissão Nacional de Eleições*) (**CNE**), and a support body, the **Technical Secretariat for Electoral Administration** (*Secretariado Técnico da Administração Eleitoral*) (**STAE**).[1268] Article 135 of the Constitution as amended in 2018 establishes the CNE as "an independent and impartial body", but states that its "composition, organization, operation and competences are fixed by law".[1269] According to Freedom House: "While the CNE's members hail from FRELIMO, RENAMO, the MDM, and civil society, FRELIMO effectively controls the selection process. Domestic and international observers have long argued that this structure has led to the politicization of the body and deeply undermines stakeholder confidence in its operations."[1270]

Lei n.º 1/2018: Lei da Revisão Pontual da Constituição da República de Moçambique

Artigo 135

(Princípios gerais do sistema eleitoral)

1. O sufrágio universal, directo, igual, secreto, pessoal e periódico constitui a regra geral de designação do Presidente da República, dos deputados da Assembleia da República, dos membros das assembleias provinciais, dos governadores de Província, das assembleias distritais, dos administradores de Distrito, dos membros das assembleias autárquicas e dos presidentes dos conselhos autárquicos.
2. O apuramento dos resultados das eleições obedece ao sistema de representação proporcional.
3. A supervisão do ecenseamento e dos actos eleitorais cabe à **Comissão Nacional de Eleições**, órgão independente e imparcial, cuja composição, organização, funcionamento e competências são fixados por lei.
4. O processo eleitoral é regulado por lei.

[1267] "Mozambique Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
[1268] The website for these two bodies can be found here.
[1269] Lei n.º 1/18 de 12 de Junho: Lei da Revisão Pontual da Constituição da República de Moçambique. The current composition of the CNE is summarised here.
[1270] "Freedom in the World 2023: Mozambique", Freedom House, section A3.

The election process is regulated by the **Elections Law (Law no. 8/13).** [1271] This law protects the rights of freedom of expression of the media during election periods, and entitles political parties and presidential candidates to make use of the state broadcaster to publicise their election campaigns pursuant to regulations issued by the **National Electoral Commission**.[1272] All political parties, coalitions of political parties, and their support groups are entitled to equal treatment by public and private entities in respect of their electoral campaigns.[1273]

Political parties, coalitions and political support groups and their members may not use any media, or their entitlements to media coverage during electoral campaigns to appeal to disorder or insurrection, incitement to hatred, violence, war, insult or defamation. The sanction is a suspension of the right for a minimum period of one day up to a maximum of the rest of the campaign period, depending on the severity of the fault and the degree of repetition. [1274]

The Elections Law also provides that processions and parades can take place on any day and time, in accordance with limits imposed by the maintenance of public order, and transportation and rest periods for citizens. The usual notice periods for demonstrations are reduced during election periods.[1275]

No campaigning may take place during the 48 hours preceding the elections, or during the election itself.[1276]

It is prohibited to disclose the results of polls or surveys concerning the opinion of the voters regarding the candidates for the election and the direction of the vote, from the beginning of the electoral campaign until the announcement of the election results by the National Election Commission.[1277]

The **Press Law** states that political parties have the right to regular and equitable air time on the national radio and television broadcasters, and interestingly provides that opposition political parties have the right to reply to political declarations made by the government on the national radio and television broadcasters where these that put their respective political positions directly into question.[1278]

Through the leadership of MISA-Mozambique and the National Union of Journalists ("SNJ – Sindicato Nacional de Jornalistas"), a voluntary **Code of Conduct for Election Coverage** was established in 2008. This Code includes a set of standards to guide journalists and national media during the election. It calls for "fair and balanced"

[1271] Lei n.º 8/13 de 22 de Fevereiro, Article 22.
[1272] Id, Article 31.
[1273] Id, Article 12.
[1274] Id, Articles 207 and 209.
[1275] Id, Article 23.
[1276] Id, article 36.
[1277] Id, Article 24.
[1278] Lei n.º 18/91, Article 12.

coverage in the electoral process and expects journalists to refuse bribes and to refrain from acting as spokespersons for candidates or political parties.[1279]

[1279] Cláudia Aranda, "Handbook on Journalistic Ethics in Media Coverage of Electoral Processes", UNDP, June 2011, pages 85-86; "African Media Barometer; Mozambique 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert Stiftung (FES), page 8.

CHAPTER 13

NAMIBIA

CHAPTER 13: NAMIBIA

NAMIBIA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **22nd globally; 1st out of 48 African countries** "Freedom of the press is firmly anchored in Namibia… The political and legislative environment is conducive to the free exercise of journalism."
MALABO CONVENTION: Party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Namibia's 1990 Constitution with amendments through 2014 **ARTICLE 21 FUNDAMENTAL FREEDOMS** (1) All persons shall have the right to: (a) freedom of speech and expression, which shall include freedom of the press and other media; […] (2) The fundamental freedoms referred to in Sub-Article (1) hereof shall be exercised subject to the law of Namibia, in so far as such law imposes reasonable restrictions on the exercise of the rights and freedoms conferred by the said Sub-Article, which are necessary in a democratic society and are required in the interests of the sovereignty and integrity of Namibia, national security, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.
KEY LAWS: • Draft Computer Security and Cybercrime Bill, 2019 • Communications Act 8 of 2009
CRIMINAL DEFAMATION: Technically in force under common law, but not used in practice
DATA PROTECTION: Namibia has a draft data protection law that is still under discussion.[1280]
ACCESS TO INFORMATION: Namibia has passed an access to information law which had not been brought into force as of mid-2023.[1281]

[1280] Namibia Draft Data Protection Bill, accessed 21 June 2023.
[1281] Access to Information Act 8 of 2022.

13.1 CONTEXT

The **Newspaper and Imprint Registration Act 63 of 1971**, a South African law which is still in force in Namibia, prohibits the printing and publishing of any newspaper that is not registered under the Act[1282] – with "newspaper" being defined as "a periodical publication published at intervals not exceeding one month and consisting wholly or for the greater part of political or other news or of articles relating thereto or to other current topics, with or without advertisements, and with or without illustrations, but does not include any publication not intended for public sale or public dissemination".[1283] The law is still applicable, but there have not been any new print newspapers in Namibia since about 2009; all new newspapers in recent years are digital ones which are not required to register.[1284]

The **Namibia Film Commission Act 6 of 2000** has never been brought into force, although the Commission operates as though the law is active. This Act requires anyone who is not a Namibian citizen or permanent resident, or a company registered in Namibia, to obtain the written authorization of the Commission in order to carry out any film production in Namibia unless the Commission has granted an exemption to this requirement.[1285]

The communications sector in Namibia (including telecommunications) is generally regulated by the **Communications Act 8 of 2009**. The Act establishes the Communications Regulatory Authority of Namibia (CRAN) as the regulatory body for the communications industry, which includes electronic communications and the postal service.[1286] The Board of CRAN is appointed by the relevant minister,[1287] and the minister has explicit authority to issue policy guidelines to CRAN which it must follow in the exercise of its powers.[1288] CRAN is responsible for issuing broadcasting licences, telecommunications licences and postal service licences. The Act envisages the establishment of an ".na Domain Name Association" to administer internet domains using this space, but this portion of the Act has not yet been brought into force.[1289] Although the Act refers to CRAN as an "independent regulatory authority",[1290] the

[1282] Newspaper and Imprint Registration Act 63 of 1971, section 2. Prior to Namibian independence, in 1985, *The Namibian* newspaper was asked to provide a hefty deposit as a decision of registration pursuant to a Cabinet decision. This requirement was invalidated by the High Court of South West Africa (Namibia) in the case *The Free Press of Namibia (Pty) Ltd. v. Cabinet of the Interim Government of South West Africa* 1987 (1) SA 614 (SWA).
[1283] Newspaper and Imprint Registration Act 63 of 1971, section 1.
[1284] Information from MISA Namibia, 23 June 2023.
[1285] Namibia Film Commission Act 6 of 2000, sections 20-21.
[1286] Communications Act 8 of 2009, sections 4-5 read with definition of "communications" in section 1.
[1287] Id, sections 8-9. "The process of appointing CRAN board members is ostensibly transparent, with the Ministry of Public Enterprises advertising calls for applications for all appointments on various boards. These applicants are interviewed by a panel drawn from the government and civil society. A recommended shortlist is drawn up from which the Ministry of ICT makes the final decision.[…] However, members of the CRAN board of directors are generally seen as political appointees. While none of them hold positions in the ruling party, SWAPO, they are known to be aligned with the party's governing faction." *African Media Barometer Namibia 2022*, Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), pages 46-47.
[1288] Communications Act 8 of 2009, section 7.
[1289] Id, Chapter IX.
[1290] Id, section 2(b).

provisions under which it operates do not satisfy the requirements for independence.[1291]

There are several state media outlets that are established and governed by legislation:

- The government newspaper, *New Era*, is established by the **New Era Publication Corporation Act 1 of 1992**. The object of this corporation is to produce a newspaper that places special emphasis on community-related issues, particularly those relating to the rural areas of Namibia, "issues of national interest" and "government related matters which may concern the community".[1292] It has been observed that the New Era newspaper was never intended to be independent: "It was established overtly as a government newspaper, with a mandate which includes reporting on the government. Its board is entirely appointed by the minister and, while its main aim is to provide an objective and factual information service, there is no reference in the legislation to operating in the public interest."[1293]

- The Namibian Press Agency (NAMPA) is also established by a statute, the **Namibian Press Agency Act 3 of 1992.** Its stated object is to operate "a news agency service and Information Technology (IT) service".[1294] The agency is governed by a board appointed by a minister.[1295] and funded primarily by budget allocations from Parliament.[1296] It is thus not an independent news agency.

- The **Namibian Broadcasting Act 9 of 1991** establishes the Namibian Broadcasting Corporation (NBC), which is tasked carry out a broadcasting service with these objects –

    - to inform and entertain the public of Namibia;
    - to contribute to the education and unity of the nation, and to peace in Namibia;
    - to provide and disseminate information relevant to the socio-economic development of Namibia;
    - to promote the use and understanding of the English language.[1297]

[1291] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, pages 162-163.
[1292] New Era Publication Corporation Act 1 of 1992, section 3.
[1293] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, page 152.
[1294] Namibia Press Agency Act 3 of 1992, section 3.
[1295] Id, section 6.
[1296] Id, section 12; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, page 164.
[1297] Namibian Broadcasting Act 9 of 1991, section 3.

The NBC is controlled by a board appointed by the minister.[1298] The NBC is a state broadcaster, given that it lacks a sufficient degree of independence from government to be considered a public broadcaster.[1299]

Namibia has a **Media Ombudsman** and an **Editor's Forum of Namibia**, both of which are non-governmental bodies set up by the media for purposes of self-regulation in terms of a **Code of Ethics and Conduct for Namibian Print, Broadcast and Online Media** issued by the Editor's Forum.[1300]

13.2 CONSTITUTION

It is noteworthy that the constitutional right to freedom of speech and expression in Article 21(a) explicitly states that this includes "freedom of the press and other media" – which is sufficiently broad to include online expression.

There are several grounds for restrictions mentioned in the Constitution for restricting freedom of expression:

- the sovereignty and integrity of Namibia
- national security
- public order
- decency or morality,
- contempt of court
- defamation
- incitement to an offence.[1301]

However, a restriction imposed on of these grounds must be "reasonable", imposed by law and "necessary in a democratic society".[1302]

The 2019 *Haufiku* case considered the question of a limitation of freedom of expression on national security grounds.[1303] The case involved an Government attempt to prevent publication of a newspaper article on alleged misuse of public funds by the Namibia Central Intelligence Service for the purchase of farms and houses for private use. The intended publication came to the attention of the Government when the journalist in question approached the Namibia Central Intelligence Service for comment. The Government then sought a court order banning publication of the

[1298] Id, sections5-6.
[1299] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, pages 165-166.
[1300] The Code of Ethics and Conduct for Namibian Print, Broadcast and Online Media defines "online media" as "media which is published over the Internet, and includes, without limitation, web-sites, blogs, and social media". Section 1(f).
[1301] Article 21(1)(a) of the Namibian Constitution, quoted above on the first page of this chapter.
[1302] Article 21(2) of the Namibian Constitution, quoted above on the first page of this chapter.
[1303] *Director General of the Namibian Central Intelligence Service v Haufiku & Others* 2019 (2) NR 556 (SC), summarised and analysed by Global Freedom of Expression here.

article on national security grounds.[1304] The journalist in question, relying on the constitutional right to freedom of expression, asserted that information was lawfully obtained from public databases, posted no security risk and was a matter of public interest because it concerned potential corruption by government officials.

The High Court dismissed the Government's application on the grounds that it had not presented sufficient evidence to show that the proposed publication would undermine national security. On appeal, the Supreme Court considered the government's argument that the Court must accept the assertion of the executive that national security issues were at stake, without the requirement of demonstrating this by means of evidence. The Court disagreed, holding that the Government could substantiate its case by presenting any sensitive evidence to the Court *in camera* if necessary – thus affirming that the judiciary does exercise oversight of government attempts to suppress information on national security grounds; the Court stated that the "notion that the court must simply interdict because the State assigns something the label of national security is not consonant with the values of an open and democratic society".[1305] The Supreme Court found that the government had not made out a case that information had been obtained illegally, or that there was a valid reason for suppressing its publication.[1306]

13.3 CASE STUDIES

According to Reports Without Borders in its 2023 World Press Freedom assessment:

> *Verbal attacks against journalists are not uncommon, especially from members of the government, but they are rarely exposed to threats or dangers. Relations between the authorities and reporters are generally good. No cases of intimidation have been reported when journalists were covering strikes or protests.*[1307]

Freedom House provides a similar overview:

> In practice, journalists face few legal restrictions and generally work without risking their personal safety. While self-censorship is common in state media, private media remain critical of the government.[1308]

[1304] The Government relied on the Protection of Information Act 84 of 1982 read with the Namibian Central Intelligence Service Act 10 of 1997. Section 4(1)(b) of the Protection of Information Act 84 of 1982 makes it a criminal offence to disclose any information obtained by means of a violation of the Act, or information relating to "a prohibited place, anything in a prohibited place, armaments, the defence of the Republic, a military matter, a security matter or the prevention or combating of terrorism", amongst other things. The Government argued that the information in question fell into the category of "security matter" because it related to the national security functions of the Namibia Central Intelligence Service as set out in section 5(1)(a) the Namibian Central Intelligence Service Act 10 of 1997.
[1305] *Director General of the Namibian Central Intelligence Service v Haufiku & Others*, paragraph 74.
[1306] Id, paragraphs 106-108.
[1307] "2023 World Press Freedom Index: Namibia", section on "Safety".
[1308] "Freedom in the World 2022:Namibia", Freedom House, section D1.

The US State Department's 2022 Report on Human Rights Practices in Namibia states that the constitutional right to freedom of expression is generally respected by the government.[1309]

Few specific examples of State action against journalists were located.

In 2023, an anti-LGBT protest was organised by a church group in Windhoek. Upon receiving the required advance notification of the protest, police had warned the anti-LGBT protesters not to use hate speech. A single counter-protester who was waving a pride flag at the same venue was **detained by police** along with some of his colleagues. They were released without charge a few hours later, and informed that they had been removed from the scene for their own protection.[1310]

In 2022, two Namibian journalists John Grobler and Nrupesh Soni, were arrested for alleged **trespassing** on a private farm when they used a drone to film elephants on the farm. The journalists were investigating the possible illegal sale of pregnant wild elephants to buyers based in Dubai. The arrest took place after the farm owner made complaints to police and wildlife authorities. According to the journalists, they were detained at a police roadblock and taken to a police station, where they were held for about four hours. Grobler reported that police disabled his vehicle's car security system and searched the vehicle without his consent, as well as seizing Soni's drone and its memory card for further investigation. They were also reportedly investigated for using a drone to **wilfully disturb specially protected game without a permit or written authority** from the Ministry of Environment, Forestry and Tourism.[1311] As of late August 2023, the drone had not been returned.[1312]

Some journalists were reportedly **detained by police** during a 2020 "*#Shutitalldown*" protest against gender-based violence. They were not charged with any crime. Police said that they had not recognised them as journalists rather than protesters, as they had no visible media attire, but the journalists maintained that they had presented accreditation cards to police officers.[1313]

There were a few reports of rough and intimidating treatment of journalists during 2020-2022:

- Two female journalists from private newspapers who attempted to cover an official opening of a new isolation centre at Windhoek State Hospital in 2020 were forcibly removed from the venue by security officials, despite having been invited. They were told that only state media was permitted entry. and later threateningly told by police, "You are lucky you weren't shot". They reported the incident to the

[1309] "2022 Country Reports on Human Rights Practices: Namibia", US State Department, section 2A.
[1310] Personal communication with the counter-protester, June 2023.
[1311] "Namibian journalists investigated for trespassing for drone journalism", Committee to Protect Journalists, 28 March 2022
[1312] Personal communication with John Grobler, 24 August 2023.
[1313] June Shimuoshili, "A Beacon of Hope for Press Freedom" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), pages 44-46.

police and the Office of the Ombudsman but were informed that the Prosecutor-General decided that the case would not be prosecuted. [1314]

- During a press briefing on the ruling party's involvement in the Fishrot corruption scandal, a government minister reportedly "manhandled" a female journalist from the *Namibian Sun*.[1315]
- A female journalist from Eagle FM, who was wearing a press jacket, was reportedly harassed by police during the course of her work.[1316]
- In June 2022, journalists covering a disgruntled group of pensioners who had not received their social welfare grants were forcibly pushed away by members of the Special Field Force, a military unit, who told them not to take photographs and to leave the area.[1317]

In 2009, two British journalists who were filming Namibia's annual seal cull were arrested after some of the persons who were culling the seals reportedly attacked them with the clubs that are used to kill the seals and seized their equipment. The journalists were convicted on charges of **entering a protected marine area without a permit**, fined, and given six-month suspended sentences. None of the hunters who accosted them were arrested.[1318]

In 2011, a decade-long **State advertising boycott** of *The Namibian*, the country's largest daily newspaper, finally came to an end. This boycott was initiated by Namibia's first President, Sam Nujoma, in December 2000 in an attempt to punish the newspaper for what was perceived as an anti-government stance. The State stopped advertising in the newspaper and forbid government purchases of its issues. According to the newspaper's founding editor, this move caused a loss of only 6% of the newspaper's advertising revenue and 650 single-copy sales to government officials. Thus, this attempt to use financial pressure to muzzle the newspaper was entirely unsuccessful and was quietly cancelled by the State.[1319]

Several public officials have filed **civil defamation suits** against media outlets or individuals in Namibia.

- For example, in 2022 the High Court ruled on a lawsuit for civil defamation brought by the First Lady of Namibia after a video clip on social media accused her of encouraging the liquidation of Air Namibia to further her own commercial interests in a private aviation company, and alleged that she had been romantically involved and conceived a child with a prominent Namibian businessman who is currently in jail on charges of corruption in the Fishrot matter (discussed below). It further alleged that this businessman procured her as a bride for the current President Hage Geingob. The defence of the person who made and circulated the video was that he was just repeating widely-circulating rumours. He conceded that he could

[1314] "African Media Barometer Namibia 2022", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), pages 66-67; "CIPESA and Small Media UPR Submission, Session 38", [2020]. paragraph 12.
[1315] "African Media Barometer Namibia 2022", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 67.
[1316] Id, page 67. No further details about this incident were provided.
[1317] Id, page 68.
[1318] Tom Rhodes, "In Namibia seal hunt, journalists said to become prey", Committee to Protect Journalists, 17 July 2009.
[1319] Tom Rhodes, "A quiet victory for The Namibian", Committee to Protect Journalists, 9 September 2011.

provide no factual basis for the allegations but maintained that the circulation of the allegations was in the public interest. The Court found that allegations to be defamatory and false. Furthermore, it found no evidence that the allegation had been published to further public interest. It awarded the First Lady N$ 250 000 in damages, as well as requiring the defendant to pay punitive costs.[1320]

- In 2021, Namibia's labour minister, Utoni Nujoma, filed a defamation suit against the owners and editor of a weekly newspaper, the *Windhoek Observer,* in response to a 2019 article alleging he had extorted money from a farmer in exchange for providing a government certificate of waiver that would enable the farmer to sell part of his property.[1321]
- Other civil defamation cases have been brought successfully by the previous director of Air Namibia,[1322] the Permanent Secretary in the Ministry of Foreign Affairs,[1323] and the former mayor of Namibia's capital city, Windhoek.[1324]

Namibia is currently in the throes of a massive corruption scandal popularly known as "Fishrot", which led to the arrest of the former Minister of Justice and the Minister of Fishing on allegations of corrupt allocation of fishing quotas. This case was exposed by the combined efforts of a whistleblower and investigative journalists in Namibia and Iceland and was the subject of an *Al Jazeera* documentary. The whistleblower, a former employee of the Icelandic company Samherji which allegedly also benefitted from the scheme, shared some 30 000 documents supporting his allegations with Wikileaks, which made them accessible to the various journalists working on the story.[1325] Those who are criminally charged in this case have not yet come to trial, but the Fishrot saga already illustrates the power and importance of unfettered independent journalism in Namibia. It also shows how documents which may have been obtained and shared without authorisation were crucial to uncovering what appears to be a far-reaching instance of corruption.

13.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

Namibia is the only SADC country without a dedicated cybercrime law or a set of cybercrime offences in a broader law - with Lesotho close behind, having a cybercrime bill that has made it through Parliament but has not yet been finalised as law.[1326]

[1320] *Geingos (born Kalondo) v Hishoono* 2022 (2) NR 512 (HC).
[1321] "Freedom in the World 2022: Namibia", section D1; Maria Amakali, "Nujoma sues over N$1.5m extortion claims", *New Era*, 30 September 2021.
[1322] *Free Press of Namibia (Pty) Ltd and Others v Nyandoro* 2018 (2) NR 305 (SC).
[1323] *Nghiwete v Nekundi* 2009 (2) NR 759 (HC).
[1324] *Shikongo v Trustco Group International Ltd and Others* 2009 (1) NR 363 (HC).
[1325] Roman Grynberg, Shinovene Immanuel and Tangeni Amupadhi, *Fishrot: Fisherties and Corrupton in Namibia*, 2023.
[1326] Lesotho's cybercrime law had been passed by Parliament as of mid-2023, but had not yet received Royal Assent and was still a under debate.

A) DRAFT COMPUTER SECURITY AND CYBERCRIME BILL, 2019

Discussions around a new cybercrime law in 2005, with consultations taking place in 2010. This process produced the draft Electronic Transactions and Cybercrime Bill 2013 which was crafted with technical assistance from the International Telecommunications Union. This bill was placed on the Parliamentary agenda in early 2017, but almost immediately withdrawn for further consideration. After the initial bill was prepared, the adoption of the *African Union Convention on Cyber Security and Personal Data Protection* in June 2014 provided an updated source of guidelines which had not been incorporated into the 2013 Bill. A revised draft Electronic Transactions and Cybercrime Bill was produced in 2017.[1327] The 2017 Bill was considered by Cabinet in early 2019, and a decision was taken to split it into two separate bills, one on electronic transactions and one on cybercrimes.[1328] The Electronic Transactions Act 4 of 2019 was enacted in late 2019 and brought partly into force on 16 March 2020,[1329] but the draft Computer Security and Cybercrime Bill is still a work in progress.[1330]

The most recent draft made available to the public proposes three categories of technical offences and three categories of content-based offences. The technical offences are listed in the table below.

DRAFT COMPUTER SECURITY AND CYBERCRIME BILL, 2019 - TECHNICAL OFFENCES	
Clause 10: Unauthorised access	It is an offence for a person to access a computer system or an information system while he or she knows or should reasonably have known that he or she is not authorised to do so, or to access a system in a manner which he or she knows or should reasonably have known that he or she is not authorised to do. Higher penalties may be imposed if the unauthorised access was for the purpose of committing fraud or theft, if the access had the effect of, or was calculated to cause, major disruption or serious damage, or if the access was for the purpose of obtaining information that is detrimental to the national security of Namibia. o "Access" in relation to a computer system or an information system, means to - (a) transfer data to; (b) obtain data from; (c) run a program on that system (whether that program is stored on that system or is transferred to that system) or causes any program

[1327] The government invited written submissions from the public, but these do not appear to have had much influence on the revised 2017 Bill. See Frederico Links, "Tackling Cyber Security/Crime In Namibia – Calling For A Human Rights Respecting Framework", Institute for Public Policy Research, January 2018 at 1-2, 11.
[1328] The splitting of the two bills was recommended by civil society; see id at 12.
[1329] Electronic Transactions Act 4 of 2019.
[1330] The government circulated a draft Computer Security and Cybercrimes Bill for comment in 2021, but this version of the bill was the same as the one circulated in 2019.The Ministry of Information and Communication Technology (MICT) has indicated that the bill has been revised since it was last circulate, but the revised version has not yet been made available to the public. MICT input to Child Online Protection Task Force quarterly meeting, 28 June 2023. For more information about the background to the bill, see "Familiar Flaws – Unpacking Namibia's draft Cybercrime Bill", Institute for Public Policy Research (IPPR), February 2022, sections 1 and 2.

	to perform any action or function or to render any data, function or action accessible to any program or person; or (d) do anything that might reasonably have the effect that the system in question performs any action referred to in paragraph (a) to (c)" (definition in clause 1). This definition narrows the meaning of access beyond merely entering a computer and "looking around", but it requires no intent to cause harm of to commit another crime. o This offence is broad and vague, exacerbated by the fact that "national security" is not defined for the purpose of heavier penalties.
Clause 11: Unauthorised interference	It is an offence for any person "intentionally, without authorisation" to perform any action that has the result (or is calculated to have the result) that - • computer data is altered, damaged or deteriorates • computer data is deleted; • computer data is recorded wrongly; • computer data is rendered inaccessible to any person or program; or • the performance or effectiveness of any information system, computer system or any program running on such system deteriorates, Higher penalties may be imposed if the unauthorised interference had the effect of, or was calculated to cause, major disruption or serious damage, or if "the action was for the purpose of obtaining information that is detrimental to the national security of Namibia". o As in the case of unauthorised access, this offence is broad and vague, exacerbated by the fact that "national security" is not defined for the purpose of heavier penalties.
Clause 12: Unlawful devices, systems or programs	It is an offence to intentionally create, distribute or possess any system, program, device or data whose purpose is to commit any offence under this Act or any other law. There are exceptions where a person in good faith - • does research relating to the security of information systems or computer systems; • is learning or teaching skills relating to the security of information systems or computer systems; • is testing the security of information systems or computer systems in whose security he or she has a legitimate interest; or • communicates security vulnerabilities or laws to the public in order to promote the security of a specific information system or information systems in general. o The exceptions are commendable, particularly the last one, which could apply to journalists.[1331]

[1331] See also "Situation Report Namibia: Legislation on cybercrime and electronic evidence", GLACY+ (Global Action on Cybercrime Extended), Version 20 March 2020, page 8 on this clause: "The carveouts are well-drafted and a positive addition to the draft legislation […]."

In addition, the draft bill proposes content-based offences relating to **child pornography**, **electronic harassment** and **grooming**. The way forward is not yet settled, as it has been proposed that these content-based offences in the cybercrime bill should be replaced by more detailed and comprehensive bills that cover both online and offline manifestations of these issues. A bill on the online and offline sexual exploitation of children, persons with severe mental disabilities, and in some instances adults, is on the table for discussion.[1332] A more comprehensive draft bill that would provide quick and accessible remedies for both online and offline harassment has also been put forward.[1333] In addition, the Office of the Ombudsman has also proposed a bill covering online and offline hate speech which is currently with the Law Reform and Development Commission for study, as a replacement for the seldom-used Racial Discrimination Prohibition Act 26 of 1991.[1334] It was envisaged that these three laws would move forward together as companions to the Cybercrime Bill, to prevent gaps in coverage if only online wrongs were addressed in the law.[1335] Part of the advantage of these three more dedicated bills is that their greater attention to detail would help to prevent situations where good faith journalism or other speech in the public interest is caught up in the net of prohibitions on harmful speech.

In the meantime, the Cybercrime Bill still contains proposals on child pornography, grooming and harassment. The proposed provision on **child pornography** is not limited to online manifestations of "child pornography", which is defined as:

> the depiction by means of images, sounds, text or in any other manner of a real or imaginary person who is under the age of eighteen years, who appears to be under the age of eighteen years or who is represented or held out to be below that age (referred to in this definition as "the child") –
>
> (a) while performing a sexual act;
> (b) in such a manner that it strongly suggests that the child is performing such an act or is inviting such an act;
> (c) while engaging in other sexually explicit conduct where the material is calculated or appears to be calculated to stimulate erotic, sadistic or masochistic feelings or emotions:
>
> Provided that material whose primary purpose is scientific, educational or artistic is not child pornography.[1336]

It seems inappropriate and possibly misleading to cover offline instances of child pornography in a law on cybercrime. As the *Luxembourg Guidelines on Child Sexual*

[1332] *Draft Combating of Sexual Exploitation Bill*, October 2020, which would create offences aimed at child pornography, voyeurism, non-consensual distribution of intimate images, grooming and other forms of sexual exploitation, with particular attention to the protection of children and persons with severe mental disabilities. The development of this bill was commissioned by Sisters for Change (an international NGO which is a member of the Equality & Justice Alliance), acting in consultation with the Minister of Justice, from the Legal Assistance Centre (a Namibian NGO)

[1333] *Draft Combating of Harassment Bill*, October 2020. which was part of the same project. The two bills were initially combined, but split at the suggestions of a consultation with key stakeholders in February 2020.

[1334] This is the *Prohibition of Discrimination, Discriminatory Harassment and Hate Speech Bill*, which was discussed at a public consultation in May 2021.

[1335] Discussions at consultations around these bills attended by the authors during 2021-2023.

[1336] The offence is contained in clause 13 of the *Draft Computer Security And Cybercrime Bill, 2019,* and the definition appears in clause 1.

Exploitation point out, the line between online and offline child sexual exploitation "is often blurred" and "the Internet is a means, albeit very potent, to exploit children sexually; it is not, in and by itself, a distinct type of sexual exploitation".[1337] Moreover, the proposed definition does not seem to cover all of the possible forms of child pornography. The formulation of the offence has other weaknesses, but none that seem particularly problematic for freedom of expression or journalism.

The proposed offence of **grooming**, in contrast, covers only online activities. It applies to using "a computer system or another communications device" to –

- procure or attempt to procure a child under the age of 16 for the performance of a sexual act or for the performance of any action complying with the definition of child pornography, irrespective of where that child is in the world;
- engages a child in conversations or exchanges data messages with that child for the purposes of determining the child's willingness to perform a sexual act or to participate in child pornography, or suggests the performance of these acts;
- arranges a meeting or attempts to arrange a meeting with a child referred to at which a sexual act or to participation in child pornography is "performed, discussed or suggested".[1338]

This definition does not seem sufficiently exhaustive, but its weaknesses do not appear to raise significant freedom of expression concerns.

[1337] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse Adopted by the Interagency Working Group in Luxembourg* ("Luxembourg Guidelines)", adopted by the Interagency Working Group in Luxembourg, 28 January 2016 at 27-28 (footnotes omitted).
[1338] *Draft Computer Security and Cybercrime Bill, 2019*, clause 15.

The most problematic content-based provision is the proposed crime of **electronic harassment**, which does not seem to be clearly conceptualised. For instance, it leaves victims of physical stalking and some other forms of offline harassment without any remedy – even though offline and online forms of harassment often occur in tandem. It also places the non-consensual sharing of intimate images under the concept of harassment, which seems unhelpful since this is a crime even if the person who is depicted in the images is unaware that the images have been created or shared. At the same time, part of the provision reiterates to a large extent the existing common-law offence of criminal defamation, while many international standards and guidelines recommend the complete abolition of this crime.[1339]

14, ELECTRONIC HARASSMENT *(PROPOSED OFFENCE)*

A person who intentionally posts or sends a data message, or who intentionally causes a data message to be displayed -

(a) with the intention that it causes serious emotional distress to another person;
(b) which makes credible threats of violence or other harm;
(c) which contains a statement that the accused knows to be false or with reckless disregard whether it is true or false, and with the intention to do serious harm to the reputation of another person;
(d) which makes explicit sexual suggestions knowing it to be offensive or annoying to the person to whom it is directed;
(e) contains any pictorial representation of sexual activity or nudity of a specific person -
  (i) if that person has provided that information to the perpetrator privately and the person who provided that information has a reasonable expectation that the information should not be shared with other persons or the public;
  (ii) if the photographic material has been created without the permission of the person depicted therein or the material has been obtained without the permission of the person depicted therein; or
  (iii) if that pictorial representation has been created by the manipulation of an image or photograph that does not depict sexual activity or nudity,commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

The **Combating of Harassment Bill** and **Combating of Sexual Exploitation Bill** which have been proposed as alternatives include the following remedies which are absent from the draft cybercrime bill:

- a simple expedited procedure for protection orders modelled on the protection orders already in place for domestic violence;
- mechanisms for assistance from police and electronic service providers in the case of anonymous harassment or exploitation;
- quick and accessible procedures for getting unlawful materials removed from various forums with safeguards for free speech rights;
- provisions designed to facilitate investigation by law enforcement officers – such as where such officers take over an email or cell phone account and

[1339] See the section on criminal defamation in Chapter 2 of this report.

pretend to be a child or a victim of harassment in order to collect evidence of wrongdoing.

The **proposed Combating of Harassment Bill** would also create a new civil action for damages resulting from harassment and provide for more severe criminal penalties and punitive civil damages in respect of harassment based on protected personal characteristics such as sex, race, ethnicity, religious belief or disability. It has been asserted that addressing harassment and sexual exploitation in separate laws "with greater specificity allows for a more carefully drawn balance between the need to protect against these harms and the constitutional necessity of minimising infringement on the right of free speech".[1340]

The draft cybercrime bill also includes a number of procedural and evidentiary provisions. It **applies the existing search, seizure and forfeiture provisions in Namibia's criminal procedure law to the digital realm**,[1341] with some details about how this would work in practice. The import is that cybercrime-related searches will normally require warrants issued by a judicial authority, except where the search is conducted with the consent of the relevant persons or where police reasonably believe that a warrant would be issued but the delay involved would probably defeat its purpose because it would give the suspects time to hide or destroy the evidence. Police also have the authority to search a person without a warrant where an arrest has been made on a reasonable suspicion of committing a crime.[1342]

The draft cybercrime bill allows police to issue a **preservation order** for a period of seven days, which can be extended for periods of up to three months at a time by a judicial officer.[1343] It also provides for **production orders**, but only on the authority of a judicial officer.[1344]

Under the proposed cybercrime bill, police may, with judicial authorisation, **intercept communications** or make use of a "**forensic tool**", defined as "an investigative tool (including software or hardware) installed on or in relation to a computer system or part of a computer system which logs, stores or transmits any activity, data or any other matter relating to such a system".[1345] The three-fold criteria for a warrant for either of these purposes is that (1) a less intrusive method of investigation will not provide the information required; (2) the investigation is sufficiently important and the offence is sufficiently serious to justify the method specified in the warrant; and (3) the information sought is relevant for the investigation of an offence under this Act or any other law.[1346] A warrant for either of these purposes is valid for a maximum of three months, but may be renewed.[1347] A warrant for the interception of communications

[1340] "Input on the Cybercrime Bill as discussed during the workshop held on 17-28 February 2020", Legal Assistance Centre, 30 April 2020.
[1341] *Draft Computer Security and Cybercrime Bill, 2019*, clause 18(1): "The provisions of Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) are construed to relate to computer systems, computer equipment, storage media or data."
[1342] Criminal Procedure Act 51 of 1977, sections 21-23.
[1343] Id, clause 20.
[1344] *Draft Computer Security and Cybercrime Bill, 2019*, clause 19.
[1345] Id, clause 21(1) and definition of "forensic tool" in clause 1.
[1346] Id, clause 21(1).
[1347] Id, clause 21(4).

must specify what communications it covers, but it is permissible for it to apply to all of the communications of a specified person.[1348]

Warrants are understandably issued without notice to the person who is being investigated,[1349] but the draft lacks a provision for notifying the person in question of the communications monitoring after the investigation is completed – meaning that the affected persons may never know that their data has been accessed, in contrast to traditional searches and seizures which generally become known by their nature. It also lacks an independent oversight mechanism for assessing the use of such warrants. Without such mechanisms, Namibia's surveillance actions cannot easily be analysed or challenged.

B) COMMUNICATIONS ACT 8 OF 2009

Namibia's Communications Act 8 of 2009 also creates certain criminal offences relating to communications of all kinds. The following are particularly relevant to freedom of expression.

It is an offence to use a telecommunications device knowingly to make, create, solicit or initiate transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person".[1350] This provision with its multitude of undefined terms is very vague, and it sets the bar very low by including an intent to "annoy".

The same is true of the offence of making a telephone call or utilising a telecommunications device "without disclosing his or her identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications".[1351] However, the inclusion of the failure to disclose identity helps to narrow this offence.

CONTENT RESTRICTIONS IN OTHER LAWS

The Defence Act 1 of 2002 prohibits the publication by any means of "any information calculated or likely to endanger national security or the safety of members of the Defence Force", except where the information has been furnished or the publication has been authorized on the Minister's authority. The penalty is a fine of up to N$20 000 or imprisonment for up to five years, or both (section 54(1)-(2) read with section 63) .

The Protection of Information Act 84 of 1982 makes it an offence to publish any secret official code or password, or any document, model, article or information relating to "the defence of the Republic, a military matter, a security matter or the prevention or combating of terrorism", in any manner or "for any purpose which is prejudicial to the security or interests of the Republic". The penalty is a fine of up to R10 000 or to imprisonment for up to 10 years, or both (section 54).

[1348] Id, clause 21(8).
[1349] Id, clause 21(2).
[1350] Communications Act 8 of 2009, section 117(1)(d). The Act does not define a "telecommunications device", but "telecommunications services" means "services whose provision consists wholly or partly in the transmission or routing of information on telecommunications networks by means of telecommunications processes but does not include broadcast services" (section 1)
[1351] Communications Act 8 of 2009, section 117(1)(e).

Other offences which require repeated communications actions in order to constitute harassment are more justifiable.[1352] It is also useful to journalists seeking comment that making repeated telephone calls or communications to someone is an offence only if this is done *solely* to harass the recipient of the communication.[1353]

In any event, the communications offences in this law do not seem to be utilised in practice.

C) DATA RETENTION AND STATE SURVEILLANCE

***Communications Act 8 of 2009*:** The provisions of the Communications Act on data retention and surveillance are more problematic.

The Act charges the President to establish "such **interception centres** as are necessary for the combating of crime and national security" to be staffed by the Namibia Central Intelligence Service. Where any law authorises the interception or monitoring of electronic communications, the person or institution in question can forward a request "together with any warrant that may be required under the law in question" to the head of an interception centre to carry out the interception or monitoring, as well as any decoding or decryption that is necessary. The Director-General of the Namibia Central Intelligence Service is empowered to issue directives on how information obtained by interception must be handled and on any other technical or procedural matters that are "necessary or expedient" to ensure that intercepted information is used only for its intended purpose.[1354]

Telecommunications service providers have a legal duty to provide their services in a manner that allows for interception; in instances of interception, to store information relating to the originator, destination and contents of the telecommunications concerned in the manner prescribed by regulations; and to provide assistance for the purposes of interception.[1355] Regulations on storage of the *content* of telecommunications have not yet been issued.

However, **section 73 of the Communications Act requires telecommunications service providers to collect and retain certain information about *all* of their customers**, as set out in regulations issued under the Act.[1356] For customers who are natural persons, this information currently includes the customer's name, address and Namibian identity number (or other identification information). The service provider must also retain a copy of an identity document for that person which contains a photograph. Similar information is required for juristic persons. The service provider must store the identification data in question while the person is a customer and for at least five years

[1352] Id, section 117(1)(f) and (g).
[1353] Id, section 117(1)(g).
[1354] Id, section 70.
[1355] Id, sections 71-72.
[1356] Regulations in terms of Part 6 of Chapter V of the Communications Act, issued on 15 March 2021. This discussion draws on "Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?", Legal Assistance Centre [written by one of the authors of this paper], June 2021.

after that. In addition, the service provider must collect and store each customer's telephone number or IP address, in addition to "any information that might be necessary to link a specific packet to a specific customer", as well as data about individual communications including the nature of the telecommunications; their source and destination; their date, time and duration; and specified location data in respect of the use of cellular phones or similar devices whether it is voice, fax, a message service or any other form of data.
Although there is no authorisation for the storage of content data, the other data that must be stored constitutes a serious intrusion into individual privacy which essentially removes the possibility of anonymous communications and reveals a great deal of personal information. As the Office of the United Nations High Commissioner for Human Rights has stated:

> The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[1357]

Stored information about a specific person can be accessed by police or by the Namibia Central Intelligence Service after getting authority from a judge or a magistrate, who must be satisfied that the requested information is "necessary or relevant" for the investigation concerned, that there is "no other expedient manner of obtaining the information concerned"; and that "the obtaining of the information is authorised by the law of Namibia".[1358]

Following the approach of Namibia's general criminal procedure law, **the regulations make provision for the police (but not the intelligence services) to access customer information from a telecommunications service provider *without court authorisation* in urgent situations**. However, in contrast to the approach in Namibia's Criminal Procedure Act 51 of 1977, [1359] the communication regulations place responsibility for this assessment on the *telecommunications service provider* instead of on the police officer. The regulations require the police officer making the request to convince the *authorised officer at the telecommunications service provider* "on reasonable grounds" of three things: (1) that the requested information is required urgently; (2) that the delay in getting court authorisation would defeat the purpose of the request; and (3) that a request to the court for authority for requesting the information would have been granted if it had been made.[1360] The following problems have been identified with this approach:

[1357] "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014.
[1358] Regulations in terms of Part 6 of Chapter V of the Communications Act,, regulation 5.
[1359] Section 22 of the Criminal Procedure Act 51 of 1977 allows a police official to search any person or container or premises without a search warrant if *that police official* believes on reasonable grounds that a search warrant would be issued but that the delay in obtaining the warrant would defeat the object of the search.
[1360] Regulations in terms of Part 6 of Chapter V of the Communications Act,, regulation 5(7).

> Firstly, service providers designate the staff members who will function as "authorised staff members", and they can be selected individually or identified on the basis of the positions that they hold. The names/positions must be provided to the Communications Regulatory Authority of Namibia, but there are no requirements concerning qualifications, training or even orientation to the relevant law. The selection of these persons/positions is solely at the discretion of the service provider. This means that the "authorised staff members" of telecommunications service providers are unlikely to have training or experience in legal matters. Secondly, a police officer is subject to statutory authority and could be disciplined if he or she abused the power to bypass judicial authorisation to access information – but there would be no similar recourse against staff members of a private telecommunications service provider.[1361]

This mass data retention scheme raises several potential concerns about its constitutionality in light of Namibia's constitutional protection for privacy:

> No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.[1362]

One concern is overbreadth. The current law requires telecommunications service providers to retain a massive amount of data of which only a tiny proportion is likely to ever be requested by the police or intelligence services. This would likely mean that the law probably violates the principle that justifiable interference with a constitutional right must be as minimal as possible, and only what is reasonably necessary to serve the objective. It is more likely that a *targeted* data retention scheme will pass constitutional muster - with data being retained and stored in the first place *only in respect of persons who are reasonably suspected of having some connection to serious crime*. The types of data that must be collected and retained may also be found to go beyond what is strictly necessary for the law's purposes, which could mean that the approach is disproportionate to the objective.

It can also be questioned whether the data retention requirements are well-suited to their crime-fighting objectives. It is likely that terrorists and persons involved in organised crime will have or develop techniques to evade this type of surveillance, meaning that the intrusion into the privacy of innocent citizens may be for nought.

[1361] "Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?", Legal Assistance Centre [written by one of the authors of this paper], June 2021, page 4 (reference omitted).
[1362] Namibian Constitution, Article 13(1).

As in the case of the communications interception provisions in the draft cybercrime bill, the legal regime for accessing telecommunications data under the Communications Act lacks any *ex post facto* notice to affected individuals and no other safeguards in respect of the *ex parte* proceedings involve in obtaining a warrant to access the data.
Another concern is the absence of any attention to data protection principles such as measures pertaining to the security of the data, protections for confidentiality and the prevention of unauthorised access, or provision for the erasure or destruction of data after the requisite time period for its retention has expired.

It has been noted that these measures could undermine the ability of journalists to protect confidential sources, which is an integral aspect of media freedom, as well as endangering whistleblowers, interfering with attorney-client privilege and undermining the work of civil society researchers that involves confidential sources of information.[1363]

The provisions in the Communications Act on the interception of telecommunications tie in with the authority to monitor communications in other laws, discussed below.

Namibian Central Intelligence Service Act 10 of 1997: The Namibian Central Intelligence Service Act provides for the issue of judicial directives authorising the Namibian Central Intelligence Service (NCIS) –

- to intercept a particular postal article or a particular communication transmitted by telephone or over a telecommunications system;
- to intercept *all* postal articles or communications to or from a specific person, body or organization;
- to monitor conversations by or with a person, body or organization by means of a monitoring device, whether or not a telecommunications system is being utilised.[1364]

A judge can issue such a directive only if the judge is convinced that the gathering of information concerning a threat or potential threat to the security of Namibia is necessary to enable the NCIS to properly investigate such a threat or potential threat, or to effectively perform its functions in terms of the Act or any other law, *and* that the NCIS cannot accomplish these objectives in any other manner.[1365] Such a directive is valid for three months but can be extended by a judge for three months at a time.[1366]

Combating and Prevention of Terrorist and Proliferation Activities Act 4 of 2014: This Act contains a provision on the interception of communications that follows a similar procedure as that in the Namibian Central Intelligence Service Act. A judge can issue a warrant for the interception of communications that authorises the Inspector-General of Police –

[1363] Frederico Links "Quality of Democracy Under Threat", *IPPR blog*, 20 June 2023, quoting
[1364] Namibian Central Intelligence Service Act 10 of 1997, section 24(2).
[1365] Id, section 25(1)(b).
[1366] Id, section 25(3)-(4).

- to require a communications service provider to intercept and retain a specified communication or communications of a specified description
- to authorise a member of the Police or the Namibia Central Intelligence Agency to make use of devices for the interception and retention of communication installed on any premises
- to intercept all postal articles to or from a particular person, body or organization.[1367]

A judge can issue such a warrant only if convinced that the gathering of such information concerning a terrorist activity is necessary to enable the police force to investigate properly, and that the terrorist or proliferation activity in question cannot be properly investigated in any other manner.[1368] Such a warrant is valid for three months but can be extended by a judge for three months at a time.[1369]

It should be noted that the test for interception of communication in the case of threats to national security or suspected terrorist-related activities seem to be *more stringent* than those for accessing data about telecommunications from telecommunications service providers – which can be authorised by a judge *or a magistrate*, and in urgent cases *even by an authorised officer at a telecommunications service provider*, only upon a showing that the information is necessary or relevant to a criminal investigation, that there is no other expedient manner of obtaining the information, and that there is some legal authority for obtaining the information.

None of the provisions on secret interception of communications or communications data provide for any notice to the affected person after the investigation is concluded, or for any overarching monitoring mechanism to guard against abuse.

D) TAKE-DOWN NOTIFICATIONS IN THE ELECTRONIC TRANSACTIONS ACT 4 OF 2019

Namibia's Cybercrime Bill and the other laws making certain communications illegal must be read in conjunction with the take-down provision in the **Electronic Transactions Act 4 of 2019**. Chapter 6 of this Act concerns the liability of service providers for unlawful material. A service provider can avoid civil or criminal liability in respect of material that originates with third parties provided that certain conditions are met – one of which is removing or disabling access to the material upon receiving a notification that the material is unlawful. This refers to a written notice alleging that identified material infringes some right of the complainant. It is an offence to make a false or misleading statement in such a notice.[1370]

[1367] Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014, section 40.
[1368] Id, section 41(1)(b).
[1369] Id, section 41(3)-(4).
[1370] Electronic Transactions Act 4 of 2019, sections 51-52 and 54(1) and (8).

In a provision that is unique in the SADC region, a service provider that removes the material must notify the person who made the material available within three days of the take-down. That person may then give notice to the service provider of any objection to the removal of the material. The service provider must forward the objection to the person who requested the take-down, who then has three days to provide further information to the service provider. The service provider must restore the information if he or she has a *bona fide* belief that the information may reasonably be lawful after considering the relevant submissions It is an offence to make a false or misleading statement in any of the notices that form part of this procedure.[1371]

The law explicitly states that a service provider is not liable for wrongful take down when acting in good faith in response to a complaint about unlawful materials – which clearly skews the balance in favour of removal of material that is alleged to be unlawful.[1372]

This approach to urgent removal of online material is problematic. It makes service providers, who are not necessarily expected to have legal training or to be accountable to the public, to make decisions on the legality of online materials. The scheme in the law could lead to censorship, where online media outlets are subjected to removal of their publications without the involvement of any judicial officer, which appears to constitute a serious inroad into the right to freedom of expression as well as undermining the right of the public to access information. The removal of harmful materials such as child pornography or intimate mages published without consent could be dealt with by means of urgent access to a court, rather than placing the decision in the hands of telecommunications service providers.[1373]

13.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Elections in Namibia for President, National Assembly and regional councils are scheduled to take place in **late 2024**. The newly-elected Regional Councils will elect members from amongst their number to the second house of Parliament, the National Council.[1374]

Elections in Namibia are supervised by the **Electoral Commission of Namibia (ECN)** which is set up by the Constitution as an independent body. Its commissioners are appointed by the President with the approval of the National Assembly, and no commissioner may serve more than two five-year terms of office. [1375]

[1371] Id, section 54(3)-(7).
[1372] Id, section 54(2)
[1373] See, for example, "Submission: Draft Provisions of the Electronic Transactions and Cybercrime Bill", Access to Information Namibia (ACTION) Coalition, 13 September 2017.
[1374] Namibian Constitution, Articles 28(2), 46, 49 and 69(1).
[1375] Article 94B was inserted into the Namibian Constitution by the Namibian Constitution Third Amendment Act 8 of 2014.

Namibian Constitution

Article 94B Electoral Commission of Namibia

(1) There shall be an Electoral Commission of Namibia which shall be the exclusive body to direct, supervise, manage and control the conduct of elections and referenda, subject to this Constitution, and an Act of Parliament shall further define its powers, functions and duties.
(2) The Electoral Commission of Namibia shall be an independent, transparent and impartial body.
(3) The Electoral Commission of Namibia shall consist of five Commissioners, including the Chairperson, appointed by the President with the approval of the National Assembly, and such Commissioners shall be entitled to serve for a five (5) year term: Provided that no Commissioner shall serve more than two (2) terms.
(4) Subject to Sub-Article (3), the Chairperson shall serve in a full-time capacity for a term of five (5) years and shall be eligible for reappointment.
(5) The depository of the records, minutes, documents of the Electoral Commission of Namibia, as well as the electoral and referenda materials shall be the Chief Electoral and Referenda Officer.
(6) The qualifications for appointment, conditions and termination of service for the Chairperson, Commissioners and the Chief Electoral and Referenda Officer shall be determined in accordance with an Act of Parliament.

Elections are governed by the **Electoral Act 5 of 2014**,[1376] which also provides more details about the organization and functions of the ECN.

Under UN -upervised elections in November 1989, Swapo (Namibia's liberation movement turned political party) obtained a majority of 58%. Independence was proclaimed on 21 March 1990, with a Constitution that was unanimously adopted by the Constituent Assembly which served as Namibia's first Parliament. By 2014, Swapo had consolidated its political dominance into an impressive 80% of votes for the National Assembly, and 86% of votes in the direct election that put the current president, Hage Geingob, into office. However, the next election in 2019 proved to be a turning point, coming shortly after allegations of corruption in the Namibian fishing industry led to the resignation and arrest of two government ministers. It also comes during a time of increasing frustration with Namibia's widespread unemployment. SWAPO lost its two-thirds majority in the National Assembly by a hair, with a majority of 65.5%, while President Geingob was re-elected with only 56% of the vote. The runner-up was Panduleni Itula, who ran as an independent candidate and received 29% of the vote, while the leader of the official opposition party, McHenry Venaani, came in third with 5.3%.[1377]

[1376] Electoral Act 5 of 2014.
[1377] See, for example, "Namibia and South Africa's ruling parties share a heroic history - but their 2024 electoral prospects look weak", *The Conversation*, 10 May 2023; "Namibia election: president wins second term despite scandal and recession", *The Guardian*, 1 December 2019.

The **2019 election results were challenged in court** by Itula, who asserted that it was unconstitutional to use electronic voting machines without a paper trail that could be used to verify the results. Section 97(1) and (2) of the Electoral Act provided for the use of electronic voting machines, while sections 97(3) and (4) required that they must be accompanied by paper trails. The relevant minister brought subsections (1) and (2) into force, but not subsections (3) and (4). Namibia's Supreme Court found that this selective implementation of section 97 breached the separation of powers by undermining the intended legislative scheme. However, the Court declined to nullify the 2019 Presidential elections on this basis, holding that it had not been proved that the lack of paper trails had materially affected the election result.[1378]

The impact of the ensuing 2020 local authority elections, and in some regional by-elections, has been assessed as follows:

> *The regional and local authority elections in late November 2020 reinforced the centrifugal tendencies with a substantial shift from SWAPO to opposition parties, as LPM, IPC and PDM won power in several regions and many local authorities (including in all the large municipalities). For the first time, SWAPO was degraded to an opposition party in several regions, and many cities and towns. This has changed the political atmosphere and tested SWAPO's respect for democracy, as the party is no longer in firm control. It now faces the challenge of regaining credibility and trust.*
>
> *The loss was to some extent a result of a lack of delivery due in part to the negative effects of an ongoing recession since 2016. It was also a response to the growing number of large-scale corruption cases and misappropriation of funds. Namibia has entered a stage of political competition in which SWAPO for the first time must earn support from voters. It remains to be seen if the support the party wins is based on fair competition and a result of improved governance, or on coercion through the monopoly over state power that is vested in the military and police loyal to SWAPO.*[1379]

In 2024, President Geingob is not eligible to run again due to Namibia's two-term limit,[1380] and it is likely that Swapo will field Namibia's first female Presidential candidate, Netumbo Nandi-Ndaitwah, who is currrently the Deputy Prime Minister, with Itula and Venaani also expected to join the field once again along with Job Amupanda, former Mayor of the capital city of Windhoek and others. [1381]

In terms of rules on expression during election periods, this law makes it an offence to use a loudspeaker to interrupt voter registration and the nomination of candidates, or to urge voters to register or not to register in a manner that disturbs, hinders or interferes with voter registration.[1382] It is also an offence to engage in certain acts within 500 meters of a polling station on polling day: to canvass for votes, to put up posters for

[1378] *Itula & Others v Minister of Urban & Rural Development & Others* 2020 (1) NR 86 (SC); Ndjodi Ndeunyema,"Vote, But You Cannot Verify: The Namibian Supreme Court's Presidential Election Decision", Oxford Human Rights Hub, 17 February 2020.
[1379] "Namibia Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
[1380] Namibian Constitution, Article 29(3).
[1381] Edward Mumbuu, "Road to State House gets crowded", *New Era*, 5 May 2023.
[1382] Electoral Act 5 of 2014, sections 174(1)(d) and 175(1)(d)(i).

this purposes, to use a loudspeaker (other than for official purposes), or to organise or participate in any procession or demonstration.[1383] In addition, it is an offence to attempt to influence or interfere with voters by means of threats of violence or by the application or threat of any physical or psychological injury, damage, hazard, loss, or disadvantage.[1384] The "Bill of Fundamental Voters' Rights and Duties" appended to the Electoral Act requires voters to refrain from dressing in any political party colours and regalia within five hundred meters of polling stations or other electoral centres, and "to refrain from instigating, participating and involving in any conduct which may result in causing any infringement upon any other voter's right to participate in elections without fear".[1385] These rules technically infringe freedom of expression, but they appear to be reasonably and narrowly crafted to safeguard crucial electoral processes.

There are also criminal offences regarding campaign materials. Every bill, placard, poster, pamphlet, circular or other printed matter which references an election or referendum, published electronically or otherwise, must include the name of the political party, organization or candidate who has approved it and the name and address of the printer and publisher. Printing, publishing or posting such material without this information is an offence that attracts stiff penalties (a fine of N$25 000 or imprisonment for up to five years, or both. on a first offence, doubling in the case of a second or subsequent conviction). The proprietor or publisher of a printed or electronic publication must cause the words "advertisement" and "endorsed by (the name of the political party, organization or candidate endorsing the advertisement)" to appear as a headline for any paid publicity, with failure to do so punishable by a fine of up to N$10 000 or imprisonment for up to two years, or both.[1386] Note that this requirement applies only to materials officially endorsed by a political party, organization or candidate, and thus does not interfere with the rights of others to engage in anonymous speech.

The **Guidelines for the Conduct of Political Activities by Political Parties in Respect of Elections** state that speakers at political rallies may not use language which incites violence, and that parties must not issue "pamphlets, newsletters or posters" that incite people to violence.[1387] Because this Code dates from 1992, it fails to make any mention of electronic communications.

The **Broadcasting Code for broadcasting licensees issued in terms of the Communications Act 8 of 2009**[1388] contains a section which requires fair and balanced coverage on "current affairs programmes that deal with elections or referendums", but leaves "news coverage of elections and referendums" at the discretion of the news editor of the broadcasting licensee. However, broadcasting licensees are required to be balanced and impartial in their election or referendum reporting and

[1383] Id, section 178(1)(b).
[1384] Id, section 180.
[1385] Id, Schedule ,: Bill of Fundamental Voters' Rights and Duties, items 3.3 and 3.5, read with section 95(b) of the Act.
[1386] Id, section 187.
[1387] General Notice 143/1992 (Government Gazette 503).
[1388] The Broadcasting Code for Broadcasting Licensees is issued under the Communications Act 8 of 2009, section 89. It is contained in General Notice 602/2018 (Government Gazette 6750), Part C, and definitions in section 1. The Code is amended by General Notice 134/2019 (Government Gazette 6915) and by General Notice 24/2021 (Government Gazette 7445), but these amendments do not affect the provisions discussed here.

to ensure that no political party, candidate or proponent is discriminated against in editorial coverage or the granting of access to coverage. A broadcasting licensee that allows any party election broadcast must make available at least four time slots not exceeding two minutes each to all political parties every day throughout the election broadcast period (which extends from the day declared as nomination day under the Electoral Act up to 48 hours before the polling commences). If the State broadcaster, NBC, affords free airtime to any political party, it appears that the Code requires it to afford the minimum free slots to other political parties – although this part of the Code is confusingly drafted.[1389]

[1389] See Part C, in particular sections 19, 20(2), 21 and 22. The references in section 21 to the "formulae" in section 22 are unclear.

CHAPTER 14

SEYCHELLES

CHAPTER 14: SEYCHELLES

SEYCHELLES KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **63rd globally; 10th out of 48 African countries** "Attacks on press freedom are quite rare in Seychelles. The environment tends to favour the practice of journalism."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Seychelles 1993 Constitution, revised 2017 Subsequent amendments to the Constitution did not affect Article 22. **ARTICLE 22** 1. Every person has a right to freedom of expression and for the purpose of this article this right includes the freedom to hold opinions and to seek, receive and impart ideas and information without interference. 2. The right under clause (1) may be subject to such restrictions as may be prescribed by a law and necessary in a democratic society - a. in the interest of defence, public safety, public order, public morality or public health; b. for protecting the reputation, rights and freedoms or private lives of persons; c. for preventing the disclosure of information received in confidence; d. for maintaining the authority and independence of the courts or the National Assembly; e. for regulating the technical administration, technical operation, or general efficiency of telephones, telegraphy, posts, wireless broadcasting, television, or other means of communication or regulating public exhibitions or public entertainment; or f. for the imposition of restrictions upon public officers. **ARTICLE 47** Where a right or freedom contained in this Charter is subject to any limitation, restriction or qualification, that limitation, restriction or qualification- a. shall have no wider effect than is strictly necessary in the circumstances; and b. shall not be applied for any purpose other than that for which it has been prescribed.
KEY LAWS: • Cybercrimes and Other Related Crimes Act 59 of 2021 • Penal Code (updated to 1 June 2021), as amended by the Penal Code (Amendment) Act 42 of 2021

• Seychelles Media Commission Act 36 of 2010, as amended
CRIMINAL DEFAMATION: No, the Penal Code was amended in 2021 to remove Chapter 18, meaning that defamation is no longer a crime[1390]
DATA PROTECTION: Seychelles has a law on data protection, but it is not operational.[1391]
ACCESS TO INFORMATION: Seychelles has a law on access to information.[1392]

14.1 CONTEXT

Print newspapers are covered by the **Newspaper Act [*Cap 147*]**. They are required to register with the relevant minister before they commence publication, and the minister has the discretion to require a bond of up to 2000 rupees as a condition of registration. Printing, publishing or knowingly distributing an unregistered newspaper can be punished with a fine.[1393]

Films in Seychelles are governed by the **Film Classification Board Act 2 of 1994**. It establishes a Film Classification Board (FCB) appointed by the relevant minister to review films and determine if they are suitable for veining, either generally or subject to restrictive classifications. No film may be commercially exhibited without first being submitted to the FCB.[1394]

Broadcasting and telecommunications are currently governed by the **Broadcasting and Telecommunication Act 2 of 2000**,[1395] but this law is set to be replaced by the **Communications Act 3 of 2023,**[1396] which was passed by Parliament but not yet in force as of mid-2023.

The Communications Act is intended as a comprehensive law for the regulation of the ICT and broadcasting services, under a new independent regulator, the **Seychelles Communications Regulatory Authority (SCRA)**.[1397] The new SCRA take over responsibility for granting different categories of licenses, from the current Seychelles Licensing Authority (SLA).[1398]

[1390] Penal Code (Amendment) Act 42 of 2021. See "President Ramkalawan Assents to the Penal Code (Amendment) Act 2021", Office of the President of the Republic of Seychelles, 20 October 2021.
[1391] Data Protection Act 9 of 2003. Section 28 of the Constitution contains a few basic data protection provisions.
[1392] Access to Information Act 4 of 2018.The Constitution protects the right to information in section 28.
[1393] Newspaper Act [*Cap 147*] (revised 1991), sections 3 and 8 in particular.
[1394] Film Classification Board Act 2 of 1994; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, pages 217-218.
[1395] Broadcasting and Telecommunication Act 2 of 2000.
[1396] Communications Act 3 of 2023.
[1397] "Communications Bill 16 of 2022", "Objects and Reasons".
[1398] "New regulatory authority to be established under approved Communications Bill", National Assembly, 23 March 2023. The Seychelles Licensing Authority (SLA) is established by section 3 of the Licences Act 23 of 2010. The Broadcasting and Telecommunications Act 2 of 2000 requires all broadcasting services to have a licence issued by the SLA, but this requirement will fall

Note that the Act contains a broad definition of "broadcasting services": "any service rendered by a person who composes or packages or distributes or who delivers or enables the delivery of broadcasting programmes on a free or subscription, or other basis, for reception by the general public or sections of the general public or the subscribers to such a service irrespective of technology used". It also applies to a broad spectrum of "electronic communications services", including cell-phone services, and "private electronic communications networks", which are electronic communications networks used primarily for providing electronic communications and broadcasting for the owner's own use or for the use of a closed user group - which would appear to capture forums such as WhatsApp groups.[1399]

The SCRA will be governed by a Board and a Chief Executive Officer appointed by the President.[1400] The law also establishes a Communications Tribunal, made up of members appointed by the President, to handle appeals from decisions of the SCRA.

The law states that the Tribunal must "be independent and shall not be subject to the direction or control of any person or authority",[1401] but there is no similar statement about the Board – although Board members may be removed only an inquiry made by an independent panel.[1402] Policies and regulations will be set by the relevant minister.[1403]

The Communications Act itself has few content directives. However, it requires that every broadcasting service operator must comply with the Code of Conduct prescribed by the Seychelles Media Commission and establish its own code on the standards of broadcast programmes, which must be approved by the Seychelles Media Commission (which is described below).[1404] Broadcasting service operators are not bound to broadcast political advertisements, but if they elect to do so, they must afford equal opportunities to all registered political parties – whether or not this takes place during an election period.[1405] The Communications Act requires that every broadcaster must set up its own procedure for handling complaints from consumers of its services, which must be approved by the Seychelles Media Commission. Complaints can also be submitted directly to the SCRA or the Seychelles Media Commission.[1406] Violations of the Act by licensees can result in financial penalties or suspension or revocation of the licence.[1407]

away under the Communications Act 3 of 2023 (see section 173(2)(b)). The SLA is responsible for many types of licences issued in Seychelles in areas unrelated to the media, so it will continue to exist. See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, at page 202 (published before the Communications Act 3 of 2023 was enacted).

[1399] Communications Act 3 of 2023, section 4.
[1400] Id, sections 148 and 158.
[1401] Id, section 163(2).
[1402] Id, section 149(4).
[1403] Id, sections 6 and 172.
[1404] Id, sections 132-133.
[1405] Id, section 136.
[1406] Id, sections 134-135.
[1407] Id, sections 143-144.

Interestingly, Article 168(1) of the Seychellois Constitution requires the state to ensure that all **broadcasting media that are owned or controlled by the state or that receive contributions from public funds**, must operate independently of the state, any political party or any other body or person. Article 168(2) requires that all such owned broadcasting media must also present divergent views.[1408]

State broadcasting in Seychelles is governed by the **Seychelles Broadcasting Corporation Act 2 of 2011,**[1409] which establishes the **Seychelles Broadcasting Corporation (SBC).** The SBC Board consists of a Chairperson and six other members, all of whom are appointed by the President. The Chairperson and two of the members must be selected from candidates proposed by the Constitutional Appointments Authority.[1410] The Act states that the SBC "shall be independent and shall operate independently of the State and of the political or other influence of other bodies, persons or political parties".[1411]

There is also a state-run press agency, the **National Information Services Agency (NISA)** which publishes the *Seychelles NATION* newspaper and aims to contribute generally to the development of the mass media in Seychelles. This body is governed by the **National Information Services Agency Act, 2010,** which was revised in 2017. Its Board is appointed by the President. The Chairperson and Vice-Chairperson are nominated by the Constitutional Appointments Authority, while the other five board members are drawn from civil society, academia, the Association of Media Professionals and government.[1412]

In 2014, representatives from different media houses established the **Association of Media Practitioners Seychelles (AMPS)** to serve as an advocacy group for journalists.[1413]

One of the key bodies in respect of media and journalism is the **Seychelles Media Commission (SMC),** a statutory body established by the **Seychelles Media Commission Act of 2010**[1414] "to preserve the freedom of the media, improve and maintain high standards of journalism in Seychelles, require publishers of newspapers, radio and television broadcasters, news agencies and journalists to respect human dignity, freedom from discrimination on any grounds except as are necessary in a democratic society, and to maintain high standards of integrity and good taste".[1415]

It is governed by a Board composed of a Chairperson and eight other members, all of whom are appointed by the President. However, five of the members must represent specific interests and be nominated by the groups concerned: the

[1408] Seychelles 1993 Constitution, revised 2017, section 168.
[1409] Seychelles Broadcasting Corporation Act, 2011 (as amended to 2012).
[1410] Id, section 4.
[1411] Id, section 3(3).
[1412] "The National Information Services Agency", *Seychelles NATION*, 28 June 2021. The original National Information Services Agency Act, 2010 can be found here. The revised version could not be located online.
[1413] "Freedom of the Press 2015: Seychelles", Freedom House, "Legal Environment".
[1414] Seychelles Media Commission Act 36 of 2010, as amended by the Seychelles Media Commission (Amendment) Act 7 of 2017 (affecting sections 4, 6, 7, 10A and 12) and by the Seychelles Media Commission (Amendment) (No. 2) Act 18 of 2017 (affecting section 4).
[1415] Id, section 13(1).

Association of Media Practitioners Seychelles (the advocacy group for journalists), the National Assembly, the Judiciary, the government body responsible for information, the Citizens' Engagement Platform Seychelles (the national umbrella for civil society). The Chairperson must be selected from candidates proposed by the Constitutional Appointments Committee and must have either a wide background as a media practitioner or strong legal and administrative experience.[1416] The Chief Executive Office is appointed by the President in consultation with the speaker of the National Assembly and the Chief Justice from amongst persons who have applied for the post after it is advertised.[1417]

The SMC has been described as "a media content regulator".[1418] Its key duties are –

- to provide independent arbitration between different types of media organizations and between members of the public and media organizations;
- to promote the independence of the print and electronic media;
- to formulate a Code of Conduct for publishers and journalists in print, broadcast and online media, and monitor compliance with the Code and all other legal obligations in force;
- to monitor any developments likely to restrict the dissemination of information, including expressions of opinion on matters of public interest and importance, and to assist in resolving them;
- to defend the constitutional right of the citizens to accurate, truthful and timely information;
- to receive complaints from members of the public relating to any infringement of the individual's right to privacy by journalists or agents of media organizations, and sanction journalists or media organizations according to law;
- to review existing legislation governing the media sectors and to make recommendations to the government to bring them in line with the constitution and current trends;
- to maintain a national database of media practitioners and institutions.[1419]

The SMC must prepare an annual report that includes a general review of the functioning of mass media for submission to the relevant minister, who must present it to the National Assembly.[1420]

In 2013, the Commission produced a **Code of Conduct for the Media in Seychelles**.[1421] The SMC initiated a review process in 2018 and was still collecting local input in 2020, but no more recent version of it has been located.[1422] There is a complaints procedure

[1416] Id, section 4 (as amended by the Seychelles Media Commission (Amendment) Act 7 of 2017 and by the Seychelles Media Commission (Amendment) (No. 2) Act 18 of 2017).
[1417] Id, section 10A (as inserted by by the Seychelles Media Commission (Amendment) Act 7 of 2017).
[1418] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, page 209.
[1419] Id, selected duties from section 13(2)/
[1420] Id, section 19.
[1421] Code of Conduct for the Media in Seychelles, 2013.
[1422] Facebook post, Seychelles Media Commission, 25 May 2020; Facebook post, Seychelles Media Commission 15 Oct 2019. Note that the SMC website was inaccessible during the preparation of this chapter.

for the consideration of complaints that a publisher or a journalist "has offended against the standards of journalistic ethics or decency as embodied in the Code of Conduct" or that an editor or working journalist has "committed any professional misconduct". After holding an inquiry, the SMC may warn or admonish the publisher, editor, journalist or media outlet concerned, publicly express disapproval of the conduct in question or require any publisher or broadcaster to publicise specified particulars relating to the inquiry or the full adjudication.[1423] This appears to encompass orders to publish an apology or to allow a right of reply.[1424]

Where the Code of Conduct allows for exceptions to the rules in the "public interest", it applies the following definition: "detecting or exposing crime or a serious misdemeanour, protecting public health and safety or preventing the public from being misled by some statement or action of an individual or organization". It also states that where public interest is invoked, "the editor will be required to explain and demonstrate how the public interest was served". Furthermore, in cases involving children, editors "must demonstrate an exceptional public interest to override the normally paramount interests of the child".[1425] Some of the key provisions of the code are reproduced in the box below.

CODE OF CONDUCT FOR THE MEDIA IN SEYCHELLES, 2013

In interpreting any of the Articles of this Code of Conduct, the provisions of The Constitution of the Third Republic and all existing laws consistent with it shall always prevail.
All references to the Press shall mean both the print, electronic and broadcast media.
There may be exceptions to the clauses marked with an asterisk* where they can be demonstrated to be in the public interest.
[,,,]

1. ACCURACY

1.1 The Press should not publish inaccurate, misleading or distorted information, including pictures.
1.2 A significant inaccuracy, misleading statement or distortion once recognized must be corrected promptly and with due prominence, and - where appropriate - an apology published.
1.3 The Press shall clearly distinguish between news, infomercials and advertisements.
1.4 The Press, whilst free to take a partisan stance, should distinguish clearly between opinion, comment, conjecture and fact.

[1423] Seychelles Media Commission Act 36 of 2010, section 14; Code of Conduct for the Media in Seychelles, 2013, Preamble.
[1424] Code of Conduct for the Media in Seychelles, 2013, sections 1.2 and 2.
See, for example, "Seychelles Media Commission: Complaint by the Chief Press Secretary against Le Seychellois Hebdo", reproduced in Facebook post by State House Seychelles, 30 November 2013.
[1425] Code of Conduct for the Media in Seychelles, 2013, Annexe.

1.5 A publication must report fairly and accurately the outcome of an action for defamation to which it has been a party, unless an agreed settlement states otherwise, or an agreed statement is published.

2. OPPORTUNITY TO REPLY

A fair opportunity for reply to inaccuracies must be given when reasonably called for.

3. PRIVACY*

3.1 Everyone is entitled to respect for his or her private and family life, home, health and correspondence, including digital communications.

3.2 It is unacceptable to photograph individuals in private places without their consent.

Note - Private places are public or private property where there is a reasonable expectation of privacy.

4. DEFAMATIONS

The Press shall not engage in character assassination or defamation which could result in action for slander or libel.

5. HARASSMENT*

5.1 Journalists should not engage in intimidation, harassment or persistent pursuit of private individuals in their daily life.

5.2 They should not persist in questioning, telephoning, pursuing or photographing private individuals once asked to desist; nor remain on their property when asked to leave and must not follow them.

5.3 Editors should ensure these principles are observed by those working for them and take care not to use non-compliant material from other sources.

6. INTRUSION INTO GRIEF OR SHOCK

6.1 In cases involving personal grief or shock, enquiries and approaches must be made with sympathy and discretion and publication handled sensitively. This should not restrict the right to report legal proceedings.

6.2 Photographs and video from conflicts, accidents and crime or disaster scenes shall be used with sensitivity and not to add further to the sufferings of victims and relatives and with due regard to the public interest and good taste.

7. CHILDREN*

7.1 Young people should be free to complete their time at school without unnecessary intrusion.

7.2 A child under 18 must not be interviewed or photographed on issues involving their own or another child's welfare unless a custodial parent or similarly responsible adult consents or is present.

7.3 Pupils must not be approached or photographed at school without the permission of the school authorities.

7.4 Minors must not be paid for material involving children's welfare, nor parents or guardians for material about their children or wards, unless it is clearly established that this would not harm the child's interest.

7.5 Editors must not use the fame, notoriety or position of a parent or guardian as sole justification for publishing details of a child's private life.

8. CHILDREN IN SEX CASES*

8.1 The Press must not identify children under 18 who are victims or witnesses in cases involving sex offences.

9. HOSPITALS*

10. REPORTING OF CRIME, VIOLENCE OR HATRED*

10.1 Relatives or friends of persons convicted or accused of crime should not generally be identified unless they are genuinely relevant to the story.

10.2 Particular regard should be paid to the potentially vulnerable position of children who witness, or are victims of, crime. This should not restrict the right to report legal proceedings.

10.3 The Press should not publish material that may encourage or glorify violence, terrorist activities, ethnic, racial or religious hostilities and xenophobia.

11. HARM AND OFFENCE

11.1 The Press should avoid prejudicial or pejorative reference to an individual's race, colour, religion, gender, sexual orientation or to any physical or mental illness or disability unless genuinely relevant to the story.

11.2 The Press should avoid use of offensive language, violence, sex, humiliation and expressions that violate human dignity.

11.3 The Press shall not encourage, glamorise or condone the use of illegal drugs, the abuse of drugs, smoking, solvent abuse and the misuse of alcohol.

12. VICTIMS OF SEXUAL ASSAULT

The Press should not identify victims of sexual assault or publish material likely to contribute to such identification unless there is adequate justification, and they are legally free to do so.

13. FINANCIAL JOURNALISM

Journalists must not use for their own profit financial information they receive in advance of its general publication, nor should they pass such information to others for their profit.

14. NEWS AND INFORMATION SOURCES

14.1 Journalists have a moral obligation to protect confidential sources of information.

14.2 Save for confidential sources, publishers and broadcasters must acknowledge sources wherever and whenever possible and refrain from plagiarism.

14.3 Journalists and broadcasters should identify themselves when gathering news and opinions as a matter of courtesy unless doing so will place them in danger or it is impractical.

14.4 Clandestine devices and subterfuge should not be used. The Press should not seek to obtain or publish material acquired by using hidden cameras or clandestine listening devices; or by intercepting private or mobile telephone calls, messages or e-mails; or by the unauthorized or illegal removal of documents or photographs. Engaging in misrepresentation or subterfuge, can generally be justified only in the public interest and then only when the material cannot be obtained by other means.

15. REPORTING ON JUDICIAL PROCEEDINGS

16. PAYMENT TO CRIMINALS*

17. GENDER SENSITIVITY

The Press should be gender sensitive and avoid stereotyping when reporting.

18. OFFICIAL NATIONAL LANGUAGES

19. ELECTIONS

Once Elections have been officially announced, the Electoral Commission, by law, is mandated with special powers in respect of publications and broadcasts.

19.1 The Press shall abide by the provisions laid down by the Electoral Commission in its pursuit of free and fair elections and a responsible media landscape.

19.2 The Electoral Commission shall publish any special provisions and requirements so that the Press is fully aware of them.

14.2 CONSTITUTION

Article 22 of the Seychellois Constitution, quoted on the first page of this chapter, is admirable for its explicit inclusion with this right of "the freedom to hold opinions and to seek, receive and impart ideas and information without interference". It includes a rather extensive list of grounds for limitation of the right to freedom of expression – including the broad concepts of "defence, public safety, public order, public morality or public health", but all of the grounds for limitation must be "prescribed by a law and necessary in a democratic society".[1426]

In 2010, in the case of ***Seychelles National Party v Michel***,[1427] the Court of Appeal

[1426] Seychelles 1993 Constitution, revised 2017, section 22.
[1427] *Seychelles National Party v Michel* [2010] SCCA 9.

applied Article 22 of the Constitution to a media question. In 2006, the **Broadcasting and Telecommunication Act 2000** was amended to exclude political parties and persons affiliated to such parties from being licenced to run a broadcasting service under the Act. The Court held that this ban was an interference which is necessary in a democratic society and therefore permissible:

> *None disputes the rights of political parties, either during election time or before or after, to air their views, to lobby, to take positions in national issues and disseminate them from public or private platforms. But their right to air and disseminate their party-political ideas, opinions and views through their own privately-run broadcast station amounts to a negation of the democratic values enshrined in our Constitution. To the same extent, it amounts to a distortion of the free and fair electoral process by creating class divisions in the political rights of citizens. Such a system favours the advantaged against the less advantaged and the rich at the expense of the less rich in a system whose value is based on one person one vote.*[1428]

The Court also held that this ban must be balanced by the establishment of an independent regulatory body that can ensure the airing of competing views, opinions and policies, flowing from Article 168 of the Constitution which requires state-owned, state-controlled and state-funded broadcast media to operate independently and to present diverse viewpoints. The State must establish an independent regulatory body to ensure the accountability of all broadcasting media, public and private. The Court stated: "Political neutrality in broadcasting cannot be attained where the government is itself judge and party to whether it is fulfilling the expectations of the public in discharging its right to information subject to the rights of others and the public interest." It ordered the State to report back to it on its progress in implementing this duty.[1429]

In the **2014 *Sullivan* case**,[1430] the Court of Appeal upheld the offence of **criminal defamation in the Penal Code** against a Constitutional change. It held that the approach to determining whether a limitation on freedom of expression is permissible is a three-part test: (1) Is the legislative objective sufficiently important to justify limiting a fundamental right? (2) Are the measures taken rationally related to the legislative objective? (3) Are the means that impair the right or freedom no more than is necessary to accomplish the objective? In other words, are they proportionate to the legislative aim in light of the impact on the right?[1431] Applying this test the Court held that this offence was a proportional limitation on the right to freedom of expression:

> *[…] [I]t is our considered opinion that the offence of criminal defamation in Seychelles is so narrowly framed considering the elements that have to be proved and the defences that exist, that it accomplishes the legislative objective of the obligation*

[1428] Id, Part II (unpaginated online version).
[1429] Id, Part III (unpaginated online version).
[1430] *Sullivan v Attorney General and another* (SCA 25 of 2012) [2014] SCCA 29 (14 August 2014).
[1431] Id, paragraph 29

> *without encroaching unnecessarily on the fundamental right to freedom of expression. We have already outlined above the extremely strict and narrow confines of the offence and the ingredients that must be proved beyond reasonable doubt by the prosecution, including the proof of an opinion not honestly held in good faith by an accused person. It is clear that one can only be prosecuted for the offence in very limited circumstances. The third test is therefore passed.*[1432]

Another example of the application of Article 22 is the **2015 Constitutional Court case** that considered the constitutionality of various provisions of the **Public Order Act 22 of 2013**.[1433] This Act generally gives police powers to control public gatherings, public meetings and public processions to maintain law and order. The case addressed numerous provisions of this law, but this discussion considers only the Court's assessment of provisions that implicated freedom of expression.

The Court began its assessment by examining the concept of "public order":

> *The notion of 'public order' is a relatively nebulous idea, which includes the maintenance and preservation of the normal functioning of society. In modern constitutional democracies, this also involves control of the exercise of competing rights and freedoms in order to ensure that all citizens are able to exercise the fullest range of rights and freedoms within that society without disruption from [the] state and without disrupting others. The phrase 'public order' appears throughout the constitution as part of the justifiable limitations on certain rights, and there is a clear understanding in the Constitution that [the] notion of public order is important to be protected.*
>
> *In many countries, draconian laws have sought to control the behaviour of the population under the guise of protecting the 'public order'. These laws have granted very wide, unchecked powers to state authorities and historically, these authorities have been able to suppress fundamental rights and freedoms of the population or portions of the population under the guise of protecting the public order. This is particularly concerning when it is used to control free association and freedom of expression which are fundamental tenets of a democratic society. We were required, in this case, to determine the extent to which the present Public Order Act is justifiable under the Constitution. The Seychellois Constitution specifies that such laws are only permissible to the extent that they are necessary in a democratic society and this is the standard against which the provisions of the Public Order Act must stand.*[1434]

In considering how to apply the test of whether a restriction on a right is "necessary in a democratic society", the Court held that this must include a consideration of proportionality, meaning that the limitation must be "only as wide as is strictly necessary in a democratic society".[1435] Three of the challenged provisions were found to constitute violations of the right to freedom of expression because they lacked proportionality:

[1432] Id, paragraph 32.
[1433] *The Seychelles National Party and Others v The Government of Seychelles*, CC No 02/2014 / *Dhanjee v Alix and Others*, CC No 03/2014 [2015] SCCC 2. This was a consolidation of two cases raising similar issues.
[1434] Id, paragraphs 15-16.
[1435] Id, paragraph 54.

- The Court considered **section 5(1) of the Public Order Act** which gave the Commissioner of Police power "to 'control and direct' the extent to which speech may be amplified and disseminated in a public place (which includes the playing of music, broadcasting of ideas and amplification of the human voice)" and power to "'control and direct' the conduct of all public gatherings, which are defined as the 'gathering or concourse of ten or more persons in any public place'." For these purposes, the Commissioner was given authority to issue orders whenever "appears" to the Commissioner to be "necessary or expedient".[1436] The Court found that this wording meant that discretion could be exercised on the basis of subjective criteria that required a very low threshold to be invoked. So, while the power to control such situations was rationally connected to the legitimate goal of maintaining public order, the powers given to the Commissioner is not proportional to the legislative objective, rendering the provision an unconstitutional violation of the right to freedom of expression as well as the right of assembly and association.[1437]

- The Court considered section 7 **of the Public Order Act**, which required notice to the Commissioner of Police in order to hold a public meeting or procession. The Court noted that the definitions of "public meeting" and "public procession" were so broad that they would capture all manner of activities, including any discussion about matters of public interest at a private residence, any group of persons walking one after the other even if they had no common intention or purpose and even a demonstration by a single individual. The section thus imposed an unnecessary restriction on the freedom of expression and the right to peaceful assembly.[1438]

- The Court considered **section 29(2)(a) of the Public Order Act**, which authorised a police officer to order a person to cease filming any law enforcement operation or investigation, and to immediately delete, erase, or otherwise destroy the film or picture or document. It found that this provision impacted freedom of expression:

> *An individual who is forced to stop making, exhibiting or communicating a film or picture is prevented from capturing information which may be relevant to … the public interest, or in their own defence or in the defence of others. We are aware of the need to hold public officers to account and the increasingly important role of video footage in shedding light on situations as they arise. This footage may equally be used to vindicate the police in instances where individuals allege police brutality. This right is important for the purposes of public accountability. In this modern era anyone can become a journalist, in the moment, and they should not be silenced in order to protect the police in their investigations and operations. If it turns out that they were responsible for transmitting information which caused frustration to the investigation, there are other offences under which the individual involved will be able to be*

[1436] Id, paragraphs 62 and 65.
[1437] Id, paragraphs 65-68.
[1438] Id, paragraphs 95-102.

prosecuted.[1439]

The Court found that, while the section in question may have served the legitimate purpose or protecting police officers in their duties, it failed the proportionality test because less restrictive measures could have sufficed. It violated the constitutional right to freedom of expression as well as the right to property.[1440]

14.3 CASE STUDIES

The following overview comes from Reporters Without Borders:

Since the introduction of a multiparty system in 1993, the practice of self-censorship, which was prevalent during decades of communist rule, has slowly dissipated. State-owned media outlets no longer shy away from criticising the government or from reporting on corruption and nepotism. Nevertheless, several publications continue to be aligned with political parties.

The constitution guarantees press freedom. Defamation was decriminalised in 2021 – a major advance that followed the adoption, three years earlier, of a law on access to state-held information. The confidentiality of sources is protected, and each outlet has its own ethical code. Since 2014, the Association of Seychelles Media Professionals has been responsible for defending journalists and press freedom.

A major reduction in the cost of launching a broadcast media outlet (the price of a radio licence has been reduced eight-fold since 2012) has allowed the entry of new private-sector actors and has ended the state's monopoly of radio and television. The print sector, which is unprofitable, suffers from high printing and circulation costs in an archipelago of 115 islands. Some publications have therefore abandoned print editions in favour of publishing online. The state-owned Nation is the last daily newspaper with a print edition.

Seychelles is one of the very few African countries in which most journalists are women. Attacks on journalists are quite rare. These mostly take place on social media, with political party activists generally responsible. Sanctions against media are also infrequent but can be extremely heavy. In 2020, a newspaper was fined more than 23,000 euros for an allegedly defamatory article published in 2016. Two journalists were banned from covering the president's press conference at the end of 2022, for no official reason.[1441]

[1439] Id, paragraph 225.
[1440] Id, paragraphs 227-229.
[1441] "World Press Freedom Index 2023: Seychelles", Reporters Without Borders (subheadings omitted).

Few specific incidents involving freedom of expression have been reported. Journalists were generally free to do their work and were not subjected to arrests or violence, but there were complaints of harassment, intimidation and harsh criticisms from authorities in respect of critical reporting.[1442]

For example, in November 2022, the President summoned SBC officials to discuss critical reporting of a government minister's role in a traffic accident. The journalists protested this government interference, which they viewed as intimidation.[1443] In December 2021 the editor of the Seychelles News Agency, Rassin Vannier, had his mobile phone confiscated by police while reporting in court. When he went to police headquarters to retrieve his phone, a police officer reportedly verbally abused and threatened him.[1444]

In the past, the media exercised a degree of self-censorship to protect advertising revenues and to avoid the possibility of being charged with criminal defamation – even though that offence was seldom applied in practice. However, self-censorship has declined in recent years, particularly since the repeal of the criminal defamation law in October 2021.[1445]

14.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) CYBERCRIMES AND OTHER RELATED CRIMES ACT 59 OF 2021

In 2016, Seychelles added provisions to its **Penal Code** to criminalise fraud and forgery committed using digital technology.[1446] Then, in 2021, the country enacted the **Cybercrimes and Other Related Crimes Act 59 of 2021**,[1447] which repealed the **Computer Misuse Act 1998** but left the computer-related provisions in the Penal Code in place. The new cybercrimes law came into force on 1 February 2022.[1448] In introducing the new law, the Vice-President stated: "This new piece of legislation is more modern and up to date on crimes that are being committed in the digital space and it is on par with best international practices in this sector."[1449] In 2023 Seychelles was in the process of setting up a Cybercrime Unit within its police force.[1450]

[1442] "2022 Country Reports on Human Rights Practices: Seychelles ", US State Department, section 2A.
[1443] Id.
[1444] Id.
[1445] "Freedom in the World 2023: Seychelles", Freedom House, section D.
[1446] "Southern African Development Community Cybersecurity Maturity Report 2021", Cybersecurity Capacity Centre for Southern Africa (C3SA), 2022. The amendments were made by the Penal Code (Amendment) (No. 2) Act 12 of 2016. The new offences are oddly placed in Chapter XXXVI of the Penal Code, which is entitled "Offences relating to coin and to bank and currency notes".
[1447] Cybercrimes and Other Related Crimes Act 59 of 2021.
[1448] "Technology, Media and Telecommunications Africa Quarterly e-Bulletin", Werkman's Attorneys, 26 May 2022, citing the Cybercrimes and Other Related Crimes Act, 2021 (Commencement) Notice gazetted on 31 January 2022.
[1449] "New law to better fight cyber, other crimes committed on social media, digital platforms", *Seychelles NATION*, 25 November 2021.
[1450] Vidya Gappy, "Cybercrime Unit in the offing", *Seychelles Nation*, 28 January 2023.

CYBERCRIMES AND OTHER RELATED CRIMES ACT - TECHNICAL OFFENCES	
Section 4: Unauthorised access to computer system	It is an offence to cause a computer system to perform a function with the intent to secure unauthorised access to any computer data held in a computer system. The penalty is a fine or imprisonment for up to 5 years, or both. Access is unauthorised where the person in question is not entitled to control access of the kind in question and does not have consent such access from any person who is so entitled. It is irrelevant to the offence whether or not the access was aimed at a particular programme or data, or a particular type of programme or data. o "Access" in relation to a computer system means "to instruct, communicate with, store data in, retrieve data from or otherwise make use of any of the resources of a computer system (section 2). o This offence has a stiff maximum penalty for "mere access" which is performed without any criminal intent. o This offence contains no explicit defence for unauthorised access that is carried out in the public interest, such as for testing security vulnerabilities or investigative journalism.
Section 5: Access with criminal intent	It is an offence to cause a computer system to perform any function for the purpose of securing access to any computer data held in any computer system, with criminal intent. The penalty is a fine or imprisonment for up to 20 years, or both. It is irrelevant to the offence whether the access was authorise or unauthorised. It is also irrelevant where the criminal offence being facilitated by the access take place at the same time or another time.
Section 6: Unauthorised interception	It is an offence to intentionally use technical means to intercept, or cause the interception of, any function or non-public transmission to, from or within, a computer system without authority for the interception. It is also an offence to intentionally use or cause the use of, a computer system for the purpose of committing an offence, whether directly or indirectly. The penalty for both offences is a fine or imprisonment for up to 5 years, or both. For the purpose of these offences "intercepting" includes "listening to or viewing, by use of technical means, or recording, a function of a computer system or acquiring the substance, meaning or purport of any such function". o The grouping of these two offences seems odd because the second offence – "intentionally uses or causes to be used, directly or indirectly, a computer system for the purpose of committing an offence" – does not mention interception at all.
Section 7: Unauthorised interference with computer data	It is an offence to do any of the following acts intentionally and without authority: • destroy or alter computer data; • render computer data meaningless, useless, inaccessible, ineffective, unreliable or impaired; • obstruct, interrupt or interfere with the lawful use of computer data;

	• obstruct, interrupt or interfere with any person in the lawful use of computer data; • deny access to computer data to any person authorized to access it; or • access or intercept any computer data without authority. The penalty is a fine or imprisonment for up to 20 years, or both. o "Accessing" computer data without authority could be applied to accessing information procured by a whistleblower or stored in a Wikileaks-type cache, which could affect investigative journalism – although this would not fit the title of the section since it would not constitute "interference" with the data.
Section 8: Unauthorised interference of computer system operation	It is an offence to do the following acts any of the following acts intentionally and without authority: • interfere with, interrupt or obstruct the use of a computer system; or • impede, prevent access to or impair the usefulness or effectiveness of, any computer data in a computer system. The penalty is a fine or imprisonment for up to 20 years, or both. (For the purposes of this offence, interference, interruption, obstruction or impeding of a computer system, includes - • cutting the electricity supply to a computer system; • corrupting a computer system by any means; and • inputting, deleting or altering computer data. o The parts of this offence relating to computer data appear to overlap with section 7.
Section 9: Unlawful possession of illegal devices	It is an offence intentionally and without justification, to produce, sell, procure for use, import, export, distribute or otherwise make available • a device, including computer data, that is designed or adapted for the purpose of committing an offence in terms of sections 6, 7, or 8 of the Act; or • a computer system password, access code or similar computer data by which the whole or any part of a computer system is capable of being accessed; It is also an offence to possess any of these items with the intent that it be used by any person for the purpose of committing an offence in terms of section 6, 7, or 8 of the Act. The penalty is a fine or imprisonment for up to 5 years, or both. o There is no definition of "device" other than the description provided in this section. o Although it is not specified that the targeted device must be *primarily* designed or adapted to commit an offence (to exclude dual-use devices that are capable of being used for both lawful and unlawful purposes), the reference to "justification" would probably protect innocent possession or trade of dual-use devices.
Section 10: Electronic fraud	It is an offence "intentionally and without right" to cause loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system, with intent to procure an advantage or economic benefit for

	oneself or another person. The penalty is a fine or imprisonment for up to 10 years, or both. o The required intent helps to ensure that this offence is properly targeted.
Section 11: Computer system related forgery	It is an offence to cause loss of property to another person by any input, alteration, deletion or suppression of computer data resulting in inauthentic computer data, with the intent that such data to be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the computer data is directly readable and intelligible. The penalty is a fine or imprisonment for up to 20 years, or both.
Section 12: Unauthorised disclosure of access credentials	It is an offence, "without lawful excuse or justification", to disclose, sell, procure for use, distribute or otherwise makes available, any password, access code or other means of gaining access to a computer system or computer data - • for wrongful gain; • for any unlawful purpose; • to overcome security measures for the protection of computer data; or • with the knowledge that it is likely to cause prejudice to any person,. The penalty is a fine or imprisonment for up to 5 years, or both.

There are several similar technical offences in the **Electronic Transactions Act 8 of 2001:**

- It is an offence under **section 42** to knowingly or intentionally conceal, destroy or alter a computer source code used for a computer, computer program, computer system or computer network, where this computer source code is required to be kept or maintained by law. "Computer source code" for this purpose means the listing of programmes, computer commands, design and layout and programme analysis of computer resources in any form.
- It is an offence under **section 46** to secure access or attempt to secure access to a "protected system" without authority. A protected system is one that has been identified as such under this law, by notification in the *Official Gazette*.
- In the absence of legal authority, it is an offence under **section 48** to secure access to any electronic record, book, register, correspondence, information, document or other material and then disclose any of these items to another without the consent of the person concerned.[1451]

These offences appear to have no implications for freedom of expression.

In addition, sections 363A-363G of the **Penal Code** contain several offences aimed at **unlawful acts involving "identity information"**, several of which involve the use of computer systems. These offences involve, for example, fraudulent acts involving automated teller machines and electronic devices used to process payments, forging or falsifying credit cards and debit cards, and using devices to copy identity information from a computer.

For this purpose, "identity information" means "any information including biological or physiological information of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, card number, card personal identification number, financial institution account number, passport number, National Identification Number or computer password".[1452]

[1451] Electronic Transactions Act 8 of 2001.
[1452] Penal Code (updated to 1 June 2021), as amended by the Penal Code (Amendment) Act 42 of 2021.

These offences appear to have no implications for freedom of expression.

In addition to the technical offences, the cybercrimes law creates six categories of content-based offences.

CYBERCRIMES AND OTHER RELATED CRIMES ACT – CONTENT-BASED OFFENCES	
Section 13: Cyber extortion	It is an offence to perform or threaten to perform any of the cybercrimes in the law (technical or content-based) for the purposes of obtaining any unlawful advantage, by undertaking to cease or desist from such actions or undertaking to restore any damage caused as a result of those actions. The penalty is a fine or imprisonment for up to 5 years, or both. o This would cover, for example, the use of ransomware, where persons are asked to pay for restoring their own data, or threatening to post a private sexual photograph online unless payment is made.
Section 14: Cyber harassment	"A person who uses a computer system or who knowingly permits a device to be used for any of the following purposes - (a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or (b) threatening to inflict injury or physical harm to the person or property of any person; or (c) sending, delivering or showing a message, visual or otherwise, which is abusive, obscene, indecent, threatening, false or misleading, causing annoyance, inconvenience or is likely to cause distress or needless anxiety to any person, commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both." o This offence seems overbroad in several respects. o Key terms which could be subjectively interpreted are not defined – including "indecent", "abusive", "annoyance", "inconvenience", "distress" and "needless anxiety". o The offence does not require repeated messages, which is often what turns an initial innocent communication into harassment. o This provision would cover a sexual proposal made to an adult on a single occasion – which would probably capture many uses of dating apps and private messages. It could be applied for example, to annoying emails from a creditor seeking payment, even where they were within general ethical boundaries. It could also be applied in theory to a journalist who caused annoyance or distress by repeatedly contacting someone for comment if the messages were perceived as being abusive or threatening. o The reference to "false or misleading" communications is particularly worrying, since this could be hard to determine and apply. It could, for example, arguably be applied to the online sharing of news articles or political cartoons, satires or spoofs that were considered annoying or distressing by their targets.

Section 15: Cyber stalking	It is an offence to willfully, maliciously or repeatedly use electronic communication to harass another person, or make a threat with the intent to place that person in reasonable fear for his or her safety or for the safety of his or her immediate family. The penalty is a fine or imprisonment for up to 5 years, or both. o The requirement that the communication must cause reasonable fear for safety narrows it appropriately.
Section 16: Offensive electronic communications	A person who wilfully, maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues. The penalty is a fine or imprisonment for up to 5 years, or both. o It might be difficult to know what would "disturb the peace, quiet or privacy" or another, but the requirement that there must be "no purpose to legitimate communication" helps to keep the offence from being overbroad.
Section 17: Pornographic or obscene material [and grooming]	For the purposes of this section: • "child" means a person under age 18. • "child pornography" includes material that visually or otherwise depicts a child, a person who appears to be a child or a realistic image representing a child engaging in sexually explicit conduct. • "sexually explicit conduct" means any conduct, real or simulated, which involves - * sexual intercourse (genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex) * bestiality, * masturbation, * sadistic or masochistic sexual abuse, or * the exhibition of the genitals or pubic area of a child. It is an offence, through a computer system, to produce, publish or access child pornography or "obscene material relating to children". It is also an offence to possess child pornography or obscene material relating to children in a computer system or on a computer data storage medium. A further offence is to publish an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children. o "Obscene material relating to children" is not defined. o There are no exceptions for *bona fide* artistic, scientific or educational materials, which might apply in particular to a depiction of the genitals or pubic area of a child. It is an offence by means of a computer system, to communicate with a person who is, or who the accused believes is - • under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code;

	• under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or • under the age of 16 years, for the purpose of facilitating the commission of any sexual offence with that person under the Penal Code. This applies whenever the person in question was represented to the accused as being under the requisite age. It is no defence if the accused believed that he or she was communicating with a person over the requisite age unless the accused took reasonable steps to ascertain that person's age. It does not matter if the person in question was a fictitious person presented to the accused as a real person. o With regard to the qualifications, law enforcement agents may pose as children to gather evidence. The penalty for both offences is a fine or imprisonment for up to 5 years, or both. o In this case, the maximum penalty of 5 years imprisonment seems low, keeping in mind that child pornography is a serious and growing problem internationally.
Section 18: Pornographic publication	It is an offence, by means of a computer system, to disclose or publish a private sexual photograph or film without the consent of the person who appears in it. o Neither "private" nor "sexual" is defined, which could complicate prosecution for this offence.
In addition, sections 157A-363G of the **Penal Code** make it an offence to observe or visually record a private act of another person, in circumstances where a person would expect to be afforded privacy, without that person's consent. It is similarly an offence to observe or visually record another person's private parts, in circumstances where a person would expect to be afforded privacy in relation to his or her private parts. Possession or distribution of prohibited recordings of this nature, without the consent of the person concerned, is also an offence. A "private act" for these purposes means bathing and showering, using a toilet, any other activity where the person is in a state of nudity and intimate sexual activity that is not ordinarily done in public. "Private parts" means a person's genital or anal region when bare or a female's breast when bare. The penalty for all of these offences is "imprisonment for a period of 20 years".[1453]	

The **maximum terms of imprisonment** under the Act seem inconsistent with respect to the severity of the offence – with, for instance, computer fraud or forgery being potentially punished far more heavily than making or distributing child pornography. For any offence under the Act, the criminal court may order the **forfeiture** of any apparatus, article or thing which is the subject matter of the offence or was used to commit the offence.[1454] A court can also order the convicted perpetrator to pay compensation to the victim of an offence under the Act for any injury or property loss

[1453] Penal Code (updated to 1 June 2021).
[1454] Cybercrimes and Other Related Crimes Act 59 of 2021, section 30.

caused by the offence.[1455]

In terms of investigatory powers, any "investigatory authority" (police or any other body empowered to investigate any offence) can issue a **preservation order** for computer data that has been stored by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such computer data is vulnerable to loss or modification. Such an order can remain in force for up to 90 days, and it may be extended by a Court for any period that the Court deems fit. "Computer data" means "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function – and thus appears to include content data. For this purpose, it also explicitly includes traffic data.[1456]

The investigatory authority may, for the purposes of investigation or prosecution of a criminal offence, order the disclosure of all preserved **traffic data**, irrespective of whether one or more electronic service providers were involved in the transmission of the computer data, or sufficient traffic data to identify the electronic service providers and the path through which the computer data was transmitted.[1457] For the purposes of investigation or prosecution of a criminal offence, an investigator authority can also apply to a Court for a **production order** compelling any person to provide specified **computer data** in that person's possession or control, or requiring an electronic service provider to disclose **subscriber information**.[1458] In short, this appears to mean that traffic data can be accessed for investigation purposes without involving a Court, while other forms of computer data or subscriber information require a Court order.

Searches and seizures require a warrant from a court.[1459] An investigatory authority can also apply to a court for an order for the real-time collection of traffic data (as opposed to stored traffic data from past communications).[1460]

Take-down orders (here referred to as "**deletion orders**") are much more limited here than in most other SADC countries which is a positive attribute of this cybercrimes law. Such orders can be issued only by a court, on application by an investigatory authority, and they apply only to "indecent material of a child".[1461] In a related point, an electronic service provider is not criminally liable for information stored at the request of a user of the service, if that service provider expeditiously removes or disables access to the information *after receiving an order from any public authority or court of law* to this effect. If the electronic service provider otherwise becomes aware of specific illegal information being stored, it must *expeditiously inform a public authority to enable that authority to evaluate the nature of the information and if necessary issue an order to remove the content*.[1462]

[1455] Id, section 42 read with sections 25. 30 and 30A of the Penal Code (updated to 1 June 2021).
[1456] Id, section 20 read with the definitions in section 2.
[1457] Id, section 21.
[1458] Id, section 22.
[1459] Id, section 23.
[1460] Id, section 24.
[1461] Id, section 25. We did not locate any broader take-down provisions in any other laws in Seychelles.
[1462] Id, section 41.

B) PENAL CODE

There are several aspects of the Penal Code that are relevant to freedom of expression.[1463]

In 2021, Seychelles repealed the provisions of the Penal Code pertaining to **criminal defamation**,[1464] even though the constitutionality of this crime had been upheld by the Court of Appeal in 2014 in the *Sullivan* case discussed above. The Explanatory Statement published with the Bill gave the following explanation:

> *Criminal defamation has a long and troubled history around the globe. In Seychelles, […] in the last decade only one person in Seychelles was charged with the offence of criminal libel. The review of the concept of criminal libel is overdue. In fact, the Court of Appeal of Seychelles in the case of Sullivan v Attorney General (2014) SLR 417 took the view that:*
>
> *"Since the enactment of the 1993 Constitution, there is no doubt that offences such as criminal libel need to be scrupulously examined in light of the constitutional provision for the right to freedom of speech. Be that as it may, these offences have survived in this country presumably under permissible exceptions under the Constitution. It is the constitutional permissibility of these exceptions that is now in issue."*
>
> *In the contemporary era, there are adequate means and alternative legislative measures to address defamatory statements, malicious communications and anti-social behaviour rather than the more authoritarian contrivance of criminal libel. Further, cases such as Ramkalawan v Parti Lepep [2017] SCSC 446 and Ernesta v Bastienne [2020] SCCA demonstrate that politicians, like any other person in Seychelles, can successfully rely on civil defamation where their reputations are being maliciously lowered. It is also noteworthy that Seychelles has given several international undertakings in the recent past to abolish criminal libel.*[1465]

However, this repeal of the general offence of criminal defamation did not affect **section 62A** of the Penal Code, which makes it an offence to publish any defamatory or insulting matter intended to bring the president into hatred, ridicule or contempt, or **section 63** of the Penal Code on defamation of foreign princes and other dignitaries - which requires intent to disturb peace and friendship between Seychelles and the country in question.

PENAL CODE

62A. Defamation of President
Any person who with intent to bring the President into hatred, ridicule or contempt publishes any defamatory or insulting matter whether in writing, print, word of mouth or in any other manner shall be guilty of an offence and liable to imprisonment for 3 years.

[1463] Penal Code (updated to 1 June 2021), as amended by the Penal Code (Amendment) Act 42 of 2021.
[1464] Penal Code (Amendment) Act 42 of 2021, which repealed Chapter VIII of the Penal Code in its entirety.
[1465] Penal Code (Amendment) Bill, 2021 (Bill No. 42 of 2021), Explanatory Statement, *Supplement to Official Gazette*, 16th September 2021, following page 725.

Other provisions of the Penal Code that could unreasonably restrict freedom of expression include the following:

- **Sections 50-53 of the Penal Code** give the President power, "in his absolute discretion", to declare that a publication or series of publications published *outside* Seychelles is a "prohibited publication" if it is, in the President's view, "contrary to the public interest". Prohibited publications may not be imported, published, disseminated or reproduced, and they may not be possessed "without lawful excuse".
- **Sections 54-56 of the Penal Code** make it an offence to use seditious speech or to publish or disseminate a seditious publication. This applies to speech and publications made with an intention –
-
    - to bring the President into hatred or contempt;
    - to excite disaffection against the Government, the Constitution or the National Assembly;
    - to excite the people of Seychelles to attempt to alter any matter in Seychelles otherwise than by lawful means
    - to bring into hatred or contempt, or to excite disaffection against, the administration of justice in Seychelles;
    - to raise discontent or disaffection amongst the people of Seychelles;
    - to promote feelings of ill-will and hostility between different sections of the population of Seychelles.

There are exceptions for good faith endeavours to show that the persons responsible for the Government have been or are mistaken in any of their counsels, policies or actions; to point out, in good faith, errors or defects in the Government, the Constitution, the National Assembly or the administration of Justice; to encourage another person in good faith to attempt to alter any matter by lawful means; or to point out in good faith any matters contributing to feelings of ill-will or hostility between different classes of persons in order to bring about their removal. It is also illegal to knowingly possess a seditious publication without lawful excuse. When the proprietor, publisher, printer or editor of a newspaper is conviction of sedition, publication of the newspaper can be banned for up to three years. Prosecutions for sedition require the written consent of the Attorney General. As is typical with offences of sedition in the region, the dividing line between what is prohibited and what is acceptable is a thin one, making this offence open to subjective application.

- **Section 62 of the Penal Code** criminalises the publication of false statements, rumours or reports where they are likely to cause fear and alarm to the public or to disturb the public peace, and when the person who makes the statement - but this applies only where the person who made the publication knew or has reason to believe that the information was false. It is not clear how to determine whether speech is "false" or to identify what might cause "fear". "alarm" or disturbance of the "public peace". Thus, this section fails to provide clear guidance and gives an overly wide degree of discretion to law enforcement officials.[1466]

- **Section 128** of the Penal Code makes it an offence to use written or oral speech with the deliberate intention of wounding a person's religious feelings.

PENAL CODE

62. Publication of false news with intent to cause fear and alarm to the public
Any person who publishes, whether orally or in writing or otherwise, any statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace, knowing or having reason to believe that such statement, rumour or report is false, shall be guilty of an offence and liable to imprisonment for 3 years.

C) INVESTIGATORY POWERS AND STATE SURVEILLANCE

In addition to the power given to investigatory authorities under the cybercrimes law, summarised above, the **Electronic Transactions Act 8 of 2001** provides broad authority for the Supreme Court to issue an order allowing any agency of the Government to intercept any information (data, text, images, sound, codes, and databases) transmitted through any computer resource. The justifications for such an **interception order** include the security of the Republic and the interests of public order.[1467]

The **Communications Act 3 of 2023** (not yet in force as of mid-2023) allows the SCRA to monitor, intercept or store communications for the limited purpose of "exercising powers conferred relating to **radio frequency monitoring**". That Act also allows an end user or subscriber to authorise the relevant investigatory authority or an operator to intercept telephone conversations or other electronic communications, traffic data, location data, email messages and any other form of communications when the end user or subscriber reports a **threat of violence or extortion** (directed against that end user or subscriber or any other person).[1468]

According to the US State Department's 2022 report on human rights practices in Seychelles, "there were no reports that the government monitored private online communications without appropriate legal authority".[1469]

[1466] "LEXOTA Country Analysis: Seychelles", last updated July 2022.
[1467] Electronic Transactions Act 8 of 2001, section 45. In the judicial hierarchy I nSeychelles, the Supreme Court is below the Court of Appeal and the Constitutional Court, but above the Magistrates' Courts.
[1468] Communications Act 3 of 2023, section 90.
[1469] "2022 Country Reports on Human Rights Practices: Seychelles ", US State Department, section 2A.

D) SIM CARD REGISTRATION AND OTHER SUBSCRIBER INFORMATION

SIM card registration is mandatory in Seychelles. This is currently authorised by the **Broadcasting and Telecommunication Act,** which states that every person who operates a telecommunication service must furnish directory information in respect of its subscribers to the Minister in such manner as the Minister may direct.[1470]

In future, the **Communications Act 3 of 2023** will require all operators to maintain data necessary for the identification of subscribers and services used. This data may be disclosed without the subscriber's consent only for telephone directory services – or in terms of an authority under some other law.[1471]

Seychelles recently tightened its rules on SIM cards. In December 2020, the sale of SIM cards through general retail shops was discontinued; they can now be accessed only in outlets owned and fully controlled by telecommunications operators. The government reported that the identification and verification process at general retail outlets was ineffective, making it difficult for law-enforcement agencies and operators to connect cards with customers. As of 2020, the government was working on new regulations to give telecommunications operators the burden of responsibility and liability in ensuring SIM registration and providing punitive measures for non-compliance. The government asserted that this move towards stricter prepaid SIM-card registration will help address criminal and anti-social behaviour as well as security concerns.[1472]

[1470] Broadcasting and Telecommunication Act 2 of 2000, section 34.
[1471] Communications Act 3 of 2023, section 95.
[1472] "Stricter SIM card registration to curb criminality", *Seychelles NATION*, 16 December 2020.

CHAPTER 15

SOUTH AFRICA

CHAPTER 15: SOUTH AFRICA

SOUTH AFRICA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **25th globally; 2nd out of 48 African countries** "South Africa guarantees press freedom and has a well-established culture of investigative journalism. In recent years, journalists have often been subjected to verbal attacks from political leaders and activists."
MALABO CONVENTION: Signatory but NOT party
BUDAPEST CONVENTION: Signatory but NOT party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: South African 1996 Constitution, as amended through 2012 There have been no amendments to the Constitution since 2012. **16. FREEDOM OF EXPRESSION** 1. Everyone has the right to freedom of expression, which includes- • freedom of the press and other media; • freedom to receive or impart information or ideas; • freedom of artistic creativity; and • academic freedom and freedom of scientific research. 2. The right in subsection (1) does not extend to - • propaganda for war; • incitement of imminent violence; or • advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm. **36. LIMITATION OF RIGHTS** 1. The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including- • the nature of the right; • the importance of the purpose of the limitation; • the nature and extent of the limitation; • the relation between the limitation and its purpose; and • less restrictive means to achieve the purpose. 2. Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.
KEY LAWS: • Cybercrimes Act 19 of 2020 • Films and Publications Act 65 of 1996, as amended • Electronic Communications Act 36 of 2005

CRIMINAL DEFAMATION: yes, but rarely used in practice[1473]
DATA PROTECTION: South Africa has a data protection law.[1474]
ACCESS TO INFORMATION: South Africa has access to information law.[1475]

15.1 CONTEXT

South Africa has arguably the most vibrant and robust media landscape in the region, and probably on the continent.

Unlike the situation in many other SADC countries, South Africa has no law requiring newspapers and other periodicals to register. The **Imprint Act 43 of 1993** requires that a commercial printer must affix a notice to all printed matter intended for public sale or distribution showing the printer's name (or a registered abbreviation of that name) and business address.[1476]

Films are other publications regulated by the **Films and Publication Act 65 of 1996**, which was amended in 2019 to encompass online content broadly. This law has a troubled history. Its initial approach was to provide a classification system and age restrictions for the distribution of certain films and publications upon the receipt of complaints or applications for classification.[1477]

In 2009, the law was amended to require *all* publishers of material that contains certain sexual conduct or possible prohibited content – advocating propaganda for war, incitement to violence or incitement of hatred based on race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth and nationality – to submit their material for examination *prior to* publication. An administrative board was empowered to ban the publication, to impose restrictions on its distribution (such as age restrictions) or to permit unrestricted distribution. This scheme excluded *bona fide* newspapers (including online newspapers) from its requirements as well as documentaries and publications of "scientific, literary or artistic merit" or on matters of public interest.[1478]

[1473] This offence is not contained in any statute, but is a common-law offence (referring to laws that are developed over time through court decisions). See *Hoho v The State* [2008] ZASCA 98; 2009 (1) SACR 276 (SCA); Motsepe v S (A 816/2013) [2014] ZAGPPHC 1016; 2015 (2) SACR 125 (GP); 2015 (5) SA 126 (GP) (5 November 2014)

[1474] Protection of Personal Information Act 4 of 2013 (popularly known as POPI). The Act came fully into force on 1 July 2020, with a one-year grace period for compliance ending on 30 June 2021. As of mid-2023, there have been no amendments to the law. There is a right of access to information in section 32 of the South African Constitution which requires that national legislation must be enacted to give effect to this right.

[1475] Promotion of Access to Information Act 2 of 2000 (popularly known as PAIA), with its amending acts listed separately (with hyperlinks) on the same webpage. A consolidated version dated 30 June 2021 can be found here.

[1476] Imprint Act 43 of 1993, as amended by the Imprint Amendment Act 18 of 1994.

[1477] Films and Publications Act 65 of 1996, original version.

[1478] Films and Publications Act 65 of 1996, as amended in 2009. The relevant amendments were made by the Films and Publications Amendment Act 3 of 2009.

In the ensuing case of *Print Media South Africa v Minister of Home Affairs,* the Constitutional Court struck down the portion of the amended law that involved prior restraint – which refers to any system that prevents material from being published or requires advance permission for publication. Prior restraints are the most severe inroads into freedom of expression, since they prevent information from ever seeing the light of day. The Constitutional Court held that the requirement that a large number of publications must be submitted for prior classification was not an acceptable limitation of the right to freedom of expression because it was not the least restrictive means of achieving the legislative purpose; application for a court interdict, for instance, was presented as an alternative approach. The case also excluded magazines alongside newspapers from the Act's system, on the grounds that both of these categories of publications fall under the independent, self-regulatory Press Council of South Africa.[1479]

After the Court's judgement, the Act still requires commercial distributors of films and games (including online distribution) to register with the Film and Publication Board and to submit films and games for classification if they do not already bear one. It is an offence to exhibit material with certain classifications altogether, or to violate age restrictions in respect of other classifications.

The Act was further amended in 2019, with particular attention to online materials,[1480] and by the Cybercrimes Act, 2015 which repealed one provision.[1481] This means that the reach of the Act as it currently stands goes beyond commercial distributors to encompass online content distributed for private purposes. Some of its restrictions on publications containing hate speech and other forms of prohibited content will be detailed below.

The Act is administered by a Council appointed by the Minister after consultation with Cabinet.[1482] The Council appoints the Films and Publications Board which in turn appoints classification committees to deal with individual classifications.[1483] The Council also appoints an enforcement committee, which must be chaired by a retired judge, to adjudicate some categories of cases involving contraventions of the Act.[1484] There is also an Appeal Tribunal appointed by the Minister after consultation with Cabinet.[1485] The Act states that the Board, the Council, the Enforcement Committee and the Appeal Tribunal shall be independent and impartial and must perform their functions without fear, favour, or prejudice.[1486]

[1479] *Print Media South Africa v Minister of Home Affairs* 2012 (6) SA 443 (CC).
[1480] Films and Publications Amendment Act 11 of 2019.
[1481] The Cybercrimes Act 19 of 2020 repealed section 24B of the Films and Publication Act 65 of 1996. The version of the Cybercrimes Act linked in this footnote includes full details of all the repeals and amendments to other laws made by Act 19 of 2020.
[1482] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 4, 6.
[1483] Id, sections 9A-10.
[1484] Id, sections 6A- 6B.
[1485] Id, section 5.
[1486] Id, section 3(2).

The South African Constitution requires that "an independent authority to regulate broadcasting in the public interest, and to ensure fairness and a diversity of views broadly representing South African society" must be established by national legislation.[1487]

The **Independent Communications Authority of South Africa Act 13 of 2000** establishes the **Independent Communications Authority of South Africa (ICASA)** which is the regulatory authority for electronic communications, broadcasting and postal services in South Africa.[1488] ICASA administers the Postal Services Act 24 of 1998, the Broadcasting Act 4 of 1999 and the Electronic Communications Act 35 of 2005. It grants licences, monitors compliance with licence conditions and develops regulations and policy documents for the three sectors it covers. It is also mandated to protect consumers in respect of these sectors.[1489] It also has the power to conduct enquiries into matters related to its functions.[1490] The Council of ICASA is appointed by the Minister, subject to approval by the National Assembly, through a process that requires public participation in the nomination process, transparency and openness, and a publicly-revealed shortlist of candidates. Council members can be removed from office only on specified grounds and only upon adoption by the National Assembly of a resolution calling for removal from office.[1491]

The **Broadcasting Act 4 of 1999** has been replaced for the most part by the Electronic Communications Act 35 of 2005. Its remaining provisions relate primarily to the South African Broadcasting Corporation (SABC) as discussed below. However, it does also establish a South African Broadcast Production Advisory Body to advise the Minister on how to support the development, production and display of local television and radio content.[1492]

The **Electronic Communications Act 36 of 2005** provides specific powers and functions for ICASA concerning the electronic communications and broadcasting sectors.[1493] It provides for the licencing of electronic communications services, electronic communications network services and broadcasting services.[1494] The Act requires broadcasting licensees to either comply with the Code of Conduct issued by ICASA and enforced by ICASA's Complaints and Compliance Committee, or to comply with their own industry association's Code of Conduct and enforcement mechanisms where these are approved by ICASA.[1495] ICASA is also responsible for issuing a Code of Conduct for electronic communications service providers, and for setting minimum standards for end-user and subscriber service charters.[1496] The only content provisions in the Act relate to election periods and are discussed in section 14.5 of this chapter.

[1487] South African 1996 Constitution, as amended through 2012, Article 192.
[1488] Independent Communications Authority of South Africa Act 13 of 2000 (current version).
[1489] "Manual issued in terms of section 14 of the Promotion of Access to Information Act 2 of 2000", ICASA, 2020, section 2; Independent Communications Authority of South Africa Act 13 of 2000 (current version), section 4.
[1490] Independent Communications Authority of South Africa Act 13 of 2000 (current version), section 4B.
[1491] Id, sections 5 and 8.
[1492] Broadcasting Act 4 of 1999 (current version). section 38.
[1493] Electronic Communications Act 36 of 2005 (current version).
[1494] Id, section 5
[1495] Id, section 54 read with Independent Communications Authority of South Africa Act 13 of 2000 (current version), sections 17A-17B
[1496] Electronic Communications Act 36 of 2005 (current version), section 69.

The **South African Broadcasting Corporation (SABC)** is generally considered to be a public broadcaster with an independent board rather than a state broadcaster – although it is still vulnerable to political pressures.[1497] It is regulated by the **Broadcasting Act 4 of 1999** and governed by a Board which includes three *ex officio* executive members and 12 non-executive members appointed by the President on the advice of the National Assembly.[1498] A paper published in 2020 made the following observations:

> *The public media consists of the South African Broadcasting Corporation (SABC), which has transformed from a state broadcaster under apartheid to a public entity which reports to parliament. Under apartheid, the SABC provided a platform for government propaganda and was organized according [to] the logic of apartheid, with different radio and television channels for different ethnic groups. In the post-apartheid era, the SABC has as its mandate to serve the broad public interest, although it has also been mired in problems with corruption, mismanagement and political interference in its editorial agendas.*
>
> *[…]*
>
> *Although structures were put in place to ensure its independence, these structures were gradually eroded through internal reorganizations and the growth of a managerial class at the SABC, including interventions in editorial matters. The broadcaster's finances are currently in a very poor state due to mismanagement and corruption spanning many years. Furthermore, political interference into editorial matters manifested again in the democratic era, especially during the Zuma era.*[1499]

In 2023, South African President Cyril Ramaphosa was taken to court over his **failure to appoint a new board for the SABC** after the terms of office of the previous Board expired in October 2022. The delay apparently stemmed from the ruling party's unhappiness with the list of nominees compiled by the National Assembly – perhaps with the 2024 elections in mind. The non-government organizations that brought the case argued that the absence of effective oversight jeopardised the SABC's stability and threatens the 'fundamental right to access to information for millions denied. Before this case moved forward, the President eventually appointed a board in mid-April 2023.[1500]

There are several self-regulating industry bodies all of which issue industry codes of conduct that contain some provisions on content.[1501]

[1497] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, page 285.
[1498] Broadcasting Act 4 of 1999 (current version), section 13.
[1499] Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" and "Political-economic and regulatory shifts" (online unpaginated version).
[1500] Justine Limpitlaw, "Non-appointment of SABC Board raises spectre of lapdog broadcaster for 2024 elections", *Daily Maverick*, 20 February 2023; "Ramaphosa finally appoints SABC board", *IOL*, 18 April 2023; Chris Roper, "South Africa", Reuters Institute for the Study of Journalism, 14 June 2023; Dianne Kohler Barnard (DA Shadow Minister of Communications), "SABC Board: President's conduct "grossly unlawful" – DKB", *Politics Web*, 13 July 2023. The case was brought by Media Monitoring Africa (MMA) and others.
[1501] See generally Joe Thloloe, "Chapter 7: The South African Regulatory Regimes in Print, Broadcasting and Online" in Una Seery, ed, *Media Landscape 2012*, Government Communication and Information System, 2012.

- The **Press Council of South Africa** is a voluntary independent self-regulatory body made up of representatives of the press and the public. It has issued a **Code of Ethics and Conduct for South African Print and Online Media**.[1502] The Press Council has a complaints procedure whereby complaints are made to a Public Advocate who attempts to achieve a settlement of the problem. If this is unsuccessful the complaint is referred to the Ombud for resolution, after a hearing by an Adjudication Panel if a hearing is considered necessary. In some cases, it is possible to appeal the matter to an appeals Committee.[1503]
- The **Broadcast Complaints Commission of South Africa (BCCSA)** is a self-regulatory body set up by the National Association of Broadcasters. It issues three codes of conduct: the **Free-To-Air Code of Conduct for Broadcasting Service Licensees**; the **Code of Conduct for Subscription Broadcasting Service Licensees**; and the **Code of Conduct for Online Content Services for Licensed Broadcasters**.[1504] The BCCSA also has a complaints procedure, with a Tribunal that adjudicates complaints in light of the relevant Code of Conduct after an initial assessment by a Registrar.[1505]
- The **Digital Media and Marketing Association (DMMA)** is a voluntary self-regulating association of online publishers. It issues a **Professional Code of Conduct** for its members. which also sets out a complaint's procedure.[1506]
- The **Internet Service Providers' Association (ISPA)** is the self-regulatory industry body for ISPs. It has a **Code of Conduct**,[1507] a complaints procedure,[1508] and directions for lodging a take-down notification in terms of the Electronic Communications and Transactions Act 25 of 2002.[1509]
- The **Wireless Applications Service Providers' Association (WASPA)** is the industry body for mobile applications and services. It also has a **Code of Conduct** which includes formal and informal complaints procedures, procedures for responding to take-down notification in terms of the Electronic Communications and Transactions Act 25 of 2002 and rules for "adult services" (content or products of a clearly sexual nature) and "children's services" (services aimed at, or particularly attractive to, children).[1510]

A recent **example of the self-regulatory system in practice** is the 2021 decision by the Broadcasting Complaints Commission of South Africa (BCCSA) in the case of *Media Monitoring Africa v. eNCA Channel 403.* The BCCSA Tribunal found that a news channel had violated the BCCSA Code of Conduct by featuring an interview with a COVID-19 conspiracy theorist who made a number of false statements about the pandemic. The Tribunal found that the Code of Conduct did not require that the facts upon which opinions are based must all be true, but it did require that opinions must be made on facts truly stated or fairly indicated and referred to.

[1502] Code of Ethics and Conduct for South African Print and Online Media, 2020.
[1503] "Complaints Procedures", Press Council, effective January 2020.
[1504] All three Codes are available here.
[1505] "Criteria for a complaint", BCCSA, undated.
[1506] DMMA Professional Code of Conduct, 2010.
[1507] ISPA Code of Conduct, Version 3.1 (revised 5 June 2023).
[1508] "Complaints process", ISPA, undated.
[1509] "How to lodge a take down", ISPA, undated.
[1510] WASPA Code of Conduct, Version 17.5 (revised 28 June 2023)

The Tribunal highlighted the fact that the statements aired could have "life-and-death consequences on society at large".

It imposed a fine on the broadcaster and ordered it to broadcast an apology, while noting that it could not order the removal of the broadcast from the news website since it did not have jurisdiction over publication of material on the internet.[1511]

In past decades, the ruling party has floated the option of replacing the system of press self-regulation with a statutory Media Appeals Tribunal, on the grounds that the self-regulatory system was inadequate to protect the privacy and dignity of individuals and too soft on the media. The proposal also signalled a growing intolerance of media criticism about government corruption and mismanagement and put into motion a process of **revision of the self-regulatory system**. [1512]

This proposal was forestalled by a 2011 campaign by the Press Council to solicit public input on how to improve its system of self-regulation. A Press Freedom Commission chaired by the late Chief Justice, Pius Langa, reviewed the system of press regulation in South Africa and issued a report that express two major concerns. The first was that, while broadcasting requires either submission to the statutory regulatory mechanism print, and online media are subject only to the voluntary Press Council and cannot be forced to participate. The second concern was that members of the public often failed to make use of the complaint's procedures for broadcasting, press or online media, instead turning to social media where they often made wild and untested allegations about the media that reduce overall public trust in the media. The only remedy for a journalist or a media outlet is to approach the courts to seek an interdict or to bring a civil action for defamation - which are slow and costly processes. While this review did not result in any changes in overall approach, it did lead to a revised Press Code and a revised Constitution for the Press Council - both of which increased public participation.[1513]

In 2019, South African National Editors' Forum (SANEF) launched a new enquiry into media ethics and credibility by a Commission headed by retired Judge Kathleen Satchwell. This move was inspired by disturbing trends in the industry, including the erosion of public trust in the media in an era of disinformation, and the decline of editorial independence.[1514] This enquiry concluded in what is informally known as the "Satchwell Report" that the current system of press self-regulation and, in the case of broadcasters, co-regulation, was working well overall. It found that "the multiplicity and variety of approaches made by members of the public all point to knowledge of, and trust in, the process". It also noted that the media industry is responsive to

[1511] *Media Monitoring Africa v. eNCA Channel 403*, Case No. 09/2020, 30 June 2021; see the case summary by Global Freedom of Expression here.
[1512] Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "Normative debates" (online unpaginated version); *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.126-ff.
[1513] Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" and "Normative debates" (online unpaginated version); *Report on Press Regulation in South Africa*, Press Freedom Commission, 2012; *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.92-ff (background to Press Freedom Commission), paragraphs 12-155-12.156 (summary of key points in Press Freedom Commission report)
[1514] Id, "Normative debates" (online unpaginated version).

public complaints through the existing mechanisms and the rulings of the Press Ombud, which indicates the good faith of the media industry itself.[1515]
The Commission suggested that the industry could work towards industry-wide agreement on standard practice around editorial policies and standards and complaints procedures for members of the public.[1516] However, its overall conclusion was as follows:

> *What is needed is not more control by the state, or anyone else of the media but more media and more consumers. For this, there needs to be a media-literate audience, whose needs are catered for in their own languages, in a medium that is accessible and affordable and where a multiplicity of views is tendered so that viewers, listeners and readers can make up their own minds on a variety of issues relevant to their lives.*[1517]

It should also be noted that there is a statutory **Media Development and Diversity Agency (MDDA)** formed to promote development and diversity in the media throughout the country. It collects financial contributions through a levy on licensed broadcasters and print media outlets and provides financial support to community and small commercial print and broadcast media. as well as funding for research and training relevant to media development. It defines media to include "all forms of mass communication, including printed publications, radio, television and new electronic platforms for delivering content". However, in recent years there have been allegations that the Agency has mismanaged its funds.[1518]

15.2 CONSTITUTION

The constitutional right to freedom of expression is limited in two different ways. Firstly, section 16(2) of the Constitution states that freedom of expression does not extend to three types of expression: propaganda for war, incitement to imminent violence or advocacy of hatred based on race, ethnicity, gender or religion that constitutes incitement to cause harm. The Constitution does not itself make these forms of expression illegal, but it does not afford them constitutional protection. As one analysis explains: "The effect of this is that the government may prohibit this kind of expression without needing to meet any of the requirements contained in the general limitations clause. As there is no right to make these three types of expression, there is no need to justify limitations on them."[1519]

[1515] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.157, 12.160-12.162.
[1516] Id, paragraph C34.
[1517] Id, paragraph 12.165.
[1518] Media Development and Diversity Agency Act 14 of 2002 (definition of "media" in section 1); Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, page 271; Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" (online unpaginated version).
[1519] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, pages 261-262.

It is useful to consider the three unprotected types of expression more closely.[1520]

(1) **Propaganda for war**: It is argued that this exclusion is vague since neither "war" nor "propaganda" are defined. For example, it is asserted that people "should be able to express support for international conflicts or even South African military intervention". There have been no authoritative pronouncements on this exclusion by the Constitutional Court as yet.

(2) **Incitement of imminent violence**: Refinement of the term "incitement" may be needed. Controversial examples that have been suggested ask whether political statements – such as a call for people should grab land or that the President should be shot – would be construed as inciting violence. In criminal law, incitement requires an attempt to influence the mind of another person towards the commission of a crime. Also, the criteria of inciting "imminent" violence could depend on the context in which the statement was made. Some guidance was provided by the Constitutional Court in its 2019 decision in the *Moyo* case, where it stated that a law forbidding speech that amounts to intimidation could not be equated with "incitement of imminent violence", because it might incite harm distinct from violence (such as damage to property) and because it typically threatens violence by the person who is doing the intimidation rather than inciting a third party to cause imminent harm.[1521]

(3) **Hate speech**: The Constitution uses a narrow formulation: "advocacy of hatred that is based on race, ethnicity, gender or religion, *and* that constitutes incitement to cause harm". [1522] Some controversial examples include promoting Zionism, which could be understood as advocating the ethnic oppression of Palestinians or taking a stand against the admission of immigrants to the country, which could be construed as advocating hatred of persons whose ethnicity is not South African. Much depends on the understanding of "harm". Delineating the contours of hate speech has already been the subject of a fair amount of litigation. Understanding hate speech is complicated by the multiple statutes that contain broader definitions of this concept for different purposes, some of which are discussed below.

Where expression is not unprotected by virtue of section 16(2), it can be limited only in terms of the general limitations clause in section 36 of the Constitution – which sets out the ground rules for limiting *any* of the fundamental rights, including freedom of expression This may be done only in terms of law of general application, and the limitation in that law must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. Section 36(1) sets out factors

[1520] This discussion draws on Eshed Cohen. "Chapter 11: Freedom of Expression" in Allsop et al, eds, *Constitutional Law for Students: Part 2*, UCT Libraries, 2020 (Chapter 11, sections 13(b) and 5).
[1521] *Moyo v Minister of Police* [2019] ZACC 40, 22 October 2019. paragraph 66. The Court went on to invalidate the provision in question on the grounds that it did not pass the test for a justifiable restriction of freedom of expression.
[1522] South African 1996 Constitution, as amended through 2012, section 16(2)(c) (emphasis added).

to guide the assessment of whether the limitation is reasonable and justifiable –

- the nature of the right;
- the importance of the purpose of the limitation;
- the nature and extent of the limitation;
- the relation between the limitation and its purpose; and
- less restrictive means to achieve the purpose.[1523]

In general, court cases in South Africa have provided robust protection for the right to freedom of expression. One telling example is the 2005 *Laugh It Off* case, which involved the right to freedom of expression of a small close corporation that parodied a well-known trademark for purposes of social comment on a t-shirt. The Constitutional Court found that this expression outweighed the right to trademark protection for the world's second largest brewery. In making its finding, the Court noted the necessity of delineating the bounds of the constitutional guarantee of free expression generously.[1524]

Criminal defamation: The common-law crime of defamation is the unlawful and intentional publication of matter concerning another which tends to injure that person's reputation. (Common-law refers to laws that are developed over time through court decisions, as opposed to being set out in statutes enacted by the legislature. Many criminal offences in South Africa are common-law offences; there is no Penal Code as exists in many SADC countries.)

South Africa's Supreme Court of Appeal upheld the common law crime of defamation in 2008 in the *Hoho* case.[1525] A legislative researcher who published several leaflets containing allegations of "corruption, bribery, financial embezzlement, sexual impropriety, illegal abortion and fraud" regarding various politicians had been convicted of criminal defamation.[1526] The Court held that this crime strikes an appropriate balance between the protection of freedom of expression and the value of human dignity.[1527] One aspect of this balance considered by the Court was whether a criminal sanction for defamatory words is "too drastic a means of regulating free speech, especially when there is a relatively well developed civil-law remedy".[1528] The Court noted that a criminal sanction is indeed a more drastic remedy than a civil action for defamation, but held that this disparity "is counterbalanced by the fact that the requirements for succeeding in a criminal defamation matter are much more onerous than in a civil matter".[1529] The Court concluded that criminal defamation is an acceptable method for protecting people's reputations in a democratic society.[1530]

[1523] South African 1996 Constitution, as amended through 2012, section 36(1).
[1524] *Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International* 2006 (1) SA 144 (CC); see paragraph 47.
[1525] *Hoho v The State* [2008] ZASCA 98; 2009 (1) SACR 276 (SCA).
[1526] Id, paragraph 2.
[1527] Id at paragraphs 27-36.
[1528] Id, paragraph 32.
[1529] Id, paragraph 33.
[1530] Id, paragraph 36-37.

A similar approach was recently followed by the High Court in Gauteng in the *Motsepe* case decided in 2014.[1531] A journalist at the *Sowetan* newspaper had published an article that incorrectly stated that a magistrate had imposed different sentences on a black male and a white female for the same offence, asserting that this was a clear indication of the magistrate's racial bias.[1532] The Court stated that "freedom of expression must sometimes take a back seat and may be legitimately '*chilled*' when it intersects with the '*foundational*' Constitution value of dignity".[1533] It agreed that a criminal sanction for defamation is indeed a more drastic remedy than a civil suit for damages due to defamation, but found this to be "counterbalanced by the fact that the requirements for succeeding in a criminal defamation matter are much more onerous than in a civil matter". The essential elements of the crime of defamation are the (i) unlawful (ii) intentional (iii) publication (iv) of matter defamatory of another.[1534] In the case at hand, the Court overturned the conviction on the grounds that the State had filed to prove intention on the part of the journalist,[1535] but in principle it held that "prosecution of the media journalists who committed a crime of defamation is not inconsistent with the constitution". The Court found that the limitation on freedom of expression imposed by the crime to be reasonable and justified in an open and democratic society and consistent with the criteria laid down in section 36 of the Constitution. [1536]

Prosecutions for criminal defamation are rare and convictions even rarer.[1537] However, the South African courts are out of step with the region in their approach to this offence.

SLAPP suits: In 2022, in the *Mineral Sands* case, the South African Constitutional Court made its first ruling ever on a "SLAPP suit".[1538] SLAPP stands for "Strategic Litigation Against Public Participation" and refers to lawsuits initiated in order to limit the expression of others or to deter them from participating in public affairs. As the Constitutional Court elaborated, "Lawsuits of this kind are usually brought for the purpose of preventing or discouraging political expression and comment on public issues. Their objective is to limit protest and dissuade individuals, citizens and activists from political participation […] A common feature of SLAPP suits is that the primary aim of the litigation is not to enforce a legitimate right."[1539]

This case involved three defamation suits instituted by Australian mining companies against environmental lawyers and activists, claiming more than R14 million overall. The Constitutional Court provided the following description of what it termed "abusive litigation", which is a species of the existing doctrine of "abuse of process":

[1531] Motsepe v S (A 816/2013) [2014] ZAGPPHC 1016; 2015 (2) SACR 125 (GP); 2015 (5) SA 126 (GP) (5 November 2014).
[1532] Id, paragraph 3.
[1533] Id, paragraph 40.
[1534] Id, paragraph 46.
[1535] Id, paragraphs 20-22.
[1536] Id, paragraphs 49-50.
[1537] "Criminal Defamation", Bregmann's Law Firm, undated. See also *2022 Country Reports on Human Rights Practices*, "South Africa", US State Department, section 2A. The US State Department notes that the common law also prohibits blasphemy, although reports indicated that the last known prosecution for blasphemy was in 1968.
[1538] See also Koko v Tanton, Johannesburg High Court. Case no 2021/2212, 7 September 2021.
[1539] Mineral Sands Resources (Pty) Ltd v Reddell [2022] ZACC 37, 14 November 2022, paragraphs 42-43.

> *Hypothetically, a plaintiff may sue for defamation in circumstances where there are very little, if any, prospects of establishing a case for defamation. The defendant is in a position to show that the defamation action is being brought not to vindicate the plaintiff's right to a good name and reputation, but to silence the defendant or to burden the defendant in a manner that causes grave harm to the defendant's right of expression and the public interest that is being served by that expression, with the likelihood that pursuing the action will have that negative effect. In that instance, court process is not being used to resolve a genuine dispute, but rather is employed to achieve a result that undermines the rights in the Constitution.*[1540]

The Court held that, to show that the litigation was a SLAPP suit, the defendants would need to prove that it –

(a) is an abuse of process of court;
(b) is not brought to vindicate a right;
(c) amounts to the use of court process to achieve an improper end and to use litigation to cause the defendants financial and/or other prejudice in order to silence them; and
(d) violates, or is likely to violate, the right to freedom of expression entrenched in section 16 of the Constitution in a material way.[1541]

The Court concluded that SLAPP suits appear to be on the increase in South Africa as well as globally and that its holding that the common law doctrine of abuse of process can accommodate a SLAPP suit defence ensures "that courts can protect their own integrity by guarding over the use of their processes" and "that the law serves its primary purpose, to see that justice is done, and not to be abused for odious, ulterior purposes".[1542]

Right to receive information: Other cases have supported the right of the public to receive information as part of the right to freedom of expression. The following are some relatively recent examples which illustrate the positive role of the right to freedom of expression in promoting openness and transparency:

- In the 2017 *Van Breda* case, the Supreme Court of Appeal of South Africa rejected a ban on the audio-visual recording of a criminal proceeding against a high-profile defendant on this basis, ruling that a court could determine the nature and scope of audio-visual broadcasting on a case-by-case basis.[1543]
- In the 2016 *Primedia* case, the Supreme Court of Appeal of South Africa struck

[1540] Id, paragraph 94.
[1541] Id, paragraph 96.
[1542] Id, paragraph 100.
[1543] *Van Breda v Media 24 Ltd*, Supreme Court of Appeal, Case no: 425/2017, 21 June 2017; see the Global Freedom of Expression case summary here. Some other cases on media access to courts and similar proceedings are *Mail and Guardian Ltd v Judicial Service Commission*, Johannesburg High Court, Case No. 09/30894, 29 July 2009; *South African Broadcasting Co. v Thatcher*, High Court, Cape of Good Hope Provincial Division, Case No:8924/2004, 31 August 2005; *Dotcom Trading 121 (Pty) Ltd v King* [2000] 4 All SA 128 (C), 2 August 2000.

down provisions in Parliament's rules and policies that prohibited live television broadcasting of incidents of disorder or altercation when Parliament is in session, on the basis that the right to an open parliament includes the public's right to know about incidents of grave disorder or unparliamentary behaviour.[1544]

- In 2016, ICASA's Complaints and Compliance Committee held that a directive from SABC to cease broadcasting footage of the destruction of public property during protests was an invalid interference with the public's right to information as well as a breach of the SABC's statutory duties.[1545]
- In 2013, the Constitutional Court found that a blanket requirement in the Refugees Act that all information about asylum applications must be confidential was an impermissible limitation on the right to freedom of expression, because it provided no discretion for the Refugee Appeals Board to allow access to its proceedings in appropriate cases.[1546]

Other cases: Some other significant cases involving freedom of expression are discussed below, in connection with specific laws and topics.

15.3 CASE STUDIES

The 2023 World Freedom Index provides the following overview of the media environment in South Africa:

> *The South African media landscape is sturdy, diverse and dynamic. Media outlets do not hesitate to reveal scandals involving powerful figures. […]*
> *Political tension sometimes gives rise to disinformation or smear campaigns against media outlets, especially on social media. […]*
> *The 1996 constitution protects press freedom, but apartheid-era and anti-terrorism laws are used to limit reporting on institutions deemed to be in the "national interest". […]*
> *Journalists are rarely arrested in South Africa, but the police sometimes fail to protect them when they are exposed to violence. The safety of journalists who expose the endemic corruption is threatened by the politicians involved, their associates and their supporters. […]*

[1544] *Primedia Broadcasting v Speaker of the National Assembly*, Supreme Court of Appeal, Case no: 784/2015, 29 September 2016; see the Global Freedom of Expression case summary here.
[1545] Trustees For The Time Being of the Media Monitoring Project Benefit Trust v SABC Soc Ltd, ICASA Complaints and Compliance Committee, Case No. 195/2016, 24 February 2016.
[1546] *M&G Media Ltd v Chipu NO* [2013] ZACC 32; 2013 (6) SA 367 (CC).

According to the US State Department's 2022 Report on Human Rights Practices:

> *The constitution and law provide for freedom of expression, including for members of the press and other media, and the government generally respected this right. An independent press, a generally effective judiciary, and a functioning democratic political system combined to promote freedom of expression, including for members of the press. […]*
>
> *[…] Civil society groups complained regarding a steady shrinking of free expression space with particular concern for backlash received on social media for expressing opinions or publishing articles. Vehement attacks in social media have led some journalists to self-censor or not publish, notably women journalists and foreign journalists who allegedly felt more vulnerable to attack. […]*
> *Government and political officials often criticized media for lack of professionalism and reacted sharply to media criticism. […] Some journalists believed the government's sensitivity to criticism resulted in a higher degree of self-censorship.*[1547]

The Satchwell Report notes a number of incidents where journalists were attacked or robbed by community members or criminals in the course of performing their work,[1548] as well as threats and harassment by politicians and their supporters as well as (in one instance) employees of a private commercial entity linked to dubious tenders awarded by local and national government. [1549] More recent incidents of this nature were listed in the US State Department's 2022 Report,[1550] and reported by the Committee to Protect Journalists.[1551] Both online and physical harassment is disproportionately directed at women journalists.[1552]

In the 2019 case *South African National Editors' Forum (SANEF) v The Economic Freedom Fighters (EFF),* SANEF approached the Equality Court in terms of the Promotion of Equality and Protection against Unfair Discrimination Act 4 of 2000 seeking protection for journalists from alleged **abuse, harassment and hate speech** against them by political figures in connection with their work as journalists.

[1547] "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
[1548] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 10.50-10.56, 10.77-10.80.
[1549] Id, paragraphs 10.57-10.63.
[1550] "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
[1551] "South African journalists attacked, threatened, harassed in separate incidents", Committee to Protect Journalists, 7 April 2023; "Two South African journalists assaulted in separate incidents", Committee to Protect Journalists, 9 March 2023; "News crews harassed, reporter arrested during South Africa's municipal elections", Committee to Protect Journalists, 9 December 2021; "South African journalists attacked and threatened amid civil unrest, 4 radio stations looted", Committee to Protect Journalists, 13 July 2021; "South African EFF party supporters block journalists from covering protest", Committee to Protect Journalists, 29 June 2021; "South African journalists attacked covering farmer protest", Committee to Protect Journalists, 9 October 2020.
[1552] Chris Roper, "South Africa", Reuters Institute for the Study of Journalism, 14 June 2023.

However, the Court dismissed the application on the grounds that the hate speech prohibition in section 10 of the law in question did not apply to journalism which is a profession rather than an immutable personal characteristic like the other grounds listed in the law.[1553]

In terms of **reputational attacks on the media**, one particularly egregious episode involved a campaign to discredit journalists who had exposed corrupt dealings between the Zuma administration and the Gupta family and the resulting "state capture" by the Guptas. At the instance of the Gupta family, the UK-based public relations firm Bell Pottinger ran a campaign beginning in 2016 blaming white-owned businesses for perpetuating 'economic apartheid', creating a narrative that 'white monopoly capital' was standing in the way of the country's ability to achieve its full economic potential. According to the Satchwell Report, "more than 100 fake Twitter accounts were created which retweeted content, involving approximately 220,000 tweets. Three prominent editors (Ferial Haffajee, Peter Bruce, and Adriaan Basson) were targeted by the campaign in a barrage of offensive and threatening Tweets that sought to portray them as biased and lacking in integrity".[1554] The campaign stated that these journalists were paid by their white bosses to criticise the Guptas and were acting in the service of 'white monopoly capital'. The Gupta-funded disinformation campaign eventually "grew its own tentacles and extended into every avenue of socio-politico-economic discourse in South Africa".[1555] Bell Pottinger was accused of stoking racial tension in the country. It was expelled from the UK Public Relations Communications Association and forced into administration (akin to declaring bankruptcy) in the UK.[1556] It is relevant to this discussion that the exposé of the large-scale corruption involving the Gupta family and former President Jacob Zuma's administration was accomplished by investigative *journalists through access to a huge cache of documents leaked from inside the Gupta business empire.*[1557]

There have been several recent court victories against attempts to silence and intimidate freedom of expression. In June 2023, in the case of Maughan v Zuma, the Pietermaritzburg High Court prohibited former South African President Jacob Zuma from continuing the **private criminal prosecution** of journalist Karyn Maughan. The case related to a News24 report on Zuma's medical condition. Zuma's legal team filed criminal charges against Maughan, alleging that she had published private information that was acquired unlawfully. When the State declined to prosecute, Zuma launched a private prosecution against Maughan. (South African law allows a person directly affected by a crime to bring a private criminal prosecution where State prosecutors decline to do so.) Maughan alleged that this step was being taken for the ulterior purpose of intimidating and harassing her. The Court noted that the allegations that formed the basis of the private prosecution against Maughan were

---

[1553] *South African National Editors' Forum (SANEF) v The Economic Freedom Fighters (EFF)* (90405/18) [2019] ZAEQC 6 (24 October 2019).

[1554] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraph 10.17.

[1555] Id, paragraph 10.13.

[1556] Id, paragraphs 10.10-10.18; Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The impact of democratic transition on the media" (unpaginated online version); "Bell Pottinger collapses after South African scandal", *BBC News*, 12 September 2017; "Deal that undid Bell Pottinger: inside story of the South Africa scandal", *The Guardian*, 5 September 2017.

[1557] See Jon Alsop, "Were the Gupta Leaks South Africa's Watergate?", *Daily Maverick*, 24 September 2018.

baseless, given that the allegedly confidential medical documents were public information that had already been filed in court before she published them. Relying on the previous cases concerning SLAPP suits, the Court found that the private prosecution was an abuse of court process and interdicted Zuma from taking any further steps in this regard.[1558]

In June 2023 a High Court judge issued a temporary ex parte gag order prohibiting South African investigative media outlet *amaBhungane* **from publishing any further articles based on a leak of documents from within a South African business conglomerate called the Moti Group.**[1559] An ex parte order refers to an order issued without notice to the other party. This is allowed only where the order is sought for a legitimate objective and notice to the other party would defeat that objective. Ex parte orders are temporary orders that remain in place until a "return date" when both parties to the dispute are heard, and there is a procedure for challenging them on an urgent basis, prior to the return date.[1560] Here, t**he** Moti Group claimed that amaBhungane used stolen digital documents as the basis for damaging articles about conflicts of interest in the company's relations with the Zimbabwean government and the methods it used to promote its Zimbabwean mining operations. Moti accused amaBhungane of having "used the flimsy excuse of 'public interest' to participate in theft; published stolen, altered documents and convoluted conspiracy theories as fact; and has even gone as far as to share private banking details and other personal information on public platforms".[1561] *AmaBhungane* denied that the documents were obtained illegally. The interim order prohibited amaBhungane from publishing any further articles based on the documents in question until the matter was fully ventilated on a return date some four months later.

However, in July, the High Court **overturned the gag order** on the grounds that there was no legitimate basis for allowing the Moti Group to approach the court on an ex parte basis, and that the procedure had been an "abuse of process". There was no reason to suspect that the media outlet would destroy the document in question before the matter could be heard in court, since the documents it relied upon would be necessary to protect it against charges of defamation. The Court also emphasised the "well-established norm against pre-publication restraints on the media", except in cases where the public interest is served by publication.[1562] More pointedly, it stated that a South African court "shall not shut the mouth of the media unless the fact-specific circumstances convincingly demonstrate that the public interest is not served by such publication",[1563] which required that an application prohibiting publication

[1558] *Maughan v Zuma* High Court of South Africa, Kwazulu-Natal Division, Pietermaritzberg, Case No 12770/22P, 7 June 2023; "South African court prohibits former president's private prosecution of journalist Karyn Maughan", Committee to Protect Journalists, 8 June 2023; "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.

[1559] "South Africa judge strikes down gag order against investigative outlet amaBhungane", Committee to Protect Journalists, 3 July 2023.

[1560] *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 1.

[1561] "South African court's gag on amaBhungane raises fears for investigative journalism, sources", Committee to Protect Journalists, 7 June 2023.

[1562] *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 16.

[1563] Id, paragraph 34.

must be brought with notice to the journalist concerned.[1564]

The High Court also held that amaBhungane could not be compelled to return the documents to the Moti Group because of its ethical duty to protect **confidential sources**:

> *[I]t is apparent that journalists, subject to certain limitations, are not expected to reveal the identity of their sources. If indeed freedom of press is fundamental and sine qua non for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded* [1565]

On this issue, the Court concluded that "[a]s a general principle, a journalist who has received information confidence is justified in refusing to perform an act which would unmask the source, unless the refusal would be inconsistent with the public interest.[1566]

15.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) CYBERCRIMES ACT 19 OF 2020

The Cybercrimes Act was first introduced into South Africa's National Assembly as the Cybercrimes and Cybersecurity Bill in 2017. There were extensive comments on the Bill during the public participation period in 2017, and a revised Cybercrimes Bill taking this input into account was published in October 2018. The National Council of Provinces revived the bill after it languished for some time, initiating another period of public participation that produced extensive comments and more proposed changes. It adopted the bill with additional revisions responding to this latest public input and sent the bill back to the National Assembly for concurrence. The bill was then passed by both houses of Parliament in December 2020.[1567]

[1564] Id, paragraph 45.
[1565] *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 25, quoting *Bosasa Operation (Pty) Ltd v Basson* 2013 (2) SA 570 (GSJ) at para 38, which was also quoted with approval by the Constitutional Court in *AmaBhungane Centre for Investigative Journalism v. Minister of Justice and Minister of Police v AmaBhungane Centre for Investigative Journalism* 2021 (3) SA 246 (CC), 4 February 2021, paragraph 115.
[1566] *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 45.
[1567] "Cybercrimes Act in South Africa: Overview and Read", Michaelson's, undated. "The national legislature or Parliament consists of two Houses: the National Assembly and National Council of Provinces, whose members are elected by the people of South Africa. Each House has its own distinct functions and powers, as set out in the Constitution. The National Assembly is responsible for choosing the

In an interview for this report, Murray Hunter, of Intel watch in South Africa, said part of the reasons why the bill had languished between 2018 and 2020 was because of electoral politics, as the country moved to elections in the first half of 2019. At the same time there was the sense that the proposed law was an attempt to criminalise activities where "there is [already] existing law to deal with all of these things", and the suspicion among some was that the state was "trying to invent this new tool that will somehow allow it to kind of clamp down on political conflict", some of which was perpetrated and played out online.[1568]

Note that the wording of the technical offences in the South African **Cybercrimes Act** is substantially different from the formulations used in other SADC counties.

Many of the technical offences refer to a "computer" and a "computer data storage medium". These terms are defined as follows:

- "Computer" means "any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device (section 1).
- "Computer data storage medium" means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system (section 1).[1569]

The technical offences are described with the use of many cross-references. Each cross-reference in the table has been identified with a description to make the parameters of each offence clearer. The cross-referencing technique has been complimented as a good way to give a cybercrime law legal specificity and certainty.[1570]

President, passing laws, ensuring that the members of the executive perform their work properly, and providing a forum where the representatives of the people can publicly debate issues. The National Council of Provinces is also involved in the law-making process and provides a forum for debate on issues affecting the provinces. Its main focus is ensuring that provincial interests are taken into account in the national sphere of government." "Parliament", National Government of South Africa, undated. For an overview of the crimes in the Cybercrimes Act, see Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).

[1568] Murray Hunter was interviewed via Zoom on 13 July 2023.

[1569] Cybercrimes Act 19 of 2020, section 1

[1570] Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 69.

CYBERCRIMES ACT - TECHNICAL OFFENCES	
Section 2: Illegal access	In terms of subsection (1), it is an offence to unlawfully and intentionally perform an act in respect of a computer system or a computer data storage medium which places the person who performed the act or any other person in a position to commit any of these offences - • unlawful access as contemplated in subsection 2(2) • unlawful interception of data as contemplated in subsection 3(1) • unlawful interference with data or a computer program as contemplated in subsection 5(1) • interference with a computer data storage medium or a computer system as contemplated in subsection 6(1). In terms of subsection (2), it is an offence to unlawfully and intentionally access a computer system or a computer data storage medium. • A person "accesses" a computer data storage medium, by using data or a computer program stored on it, or by storing data or a computer program on it. • A person "accesses" a computer system by using data or a computer program held on it, by storing data or a computer program on a computer data storage medium forming part of the computer system, or by instructing, communicating with, or otherwise using the computer system. • A person "uses a computer program" by copying or moving the computer program to a different electronic location, causing a computer program to perform any function, or obtaining the output of a computer program. • A person "uses data" by copying or moving the data to a different electronic location or obtaining the output of data. o According to the *Memorandum on the Objects of the Cybercrimes and Cybersecurity Bill, 2017,* the criminalisation of access is "an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of data, computer programs, data storage mediums or computer systems, and other computer-related offences".[1571] o The formulation of this provision has been praised for providing "a detailed exposition of the instances in which it can accurately be alleged that a person has intentionally and unlawfully secured access to data, a computer program, a computer data storage medium and a computer system".[1572]
Section 3: Unlawful interception of data	It is an offence – • to unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data, which is within a computer system or which is transmitted to or from a computer system (subsection (1))

[1571] *Memorandum on the Objects of the Cybercrimes and Cybersecurity Bill, 2017*, appended to the Cybercrimes and Cybersecurity Bill, 2017 [B6-17]. Note that this is not the final version of the Bill.
[1572] Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 67.

	• to unlawfully and intentionally possesses data or the output of data, with the knowledge that such data was intercepted unlawfully as contemplated in subsection (1) (subsection (2)) • to be in possession of data or the output of data where there is a reasonable suspicion that the data was intercepted unlawfully as contemplated in subsection (1), in the absence of "a satisfactory exculpatory account" of such possession (subsection (3)) "Interception of data" means the "acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder, the sender, the recipient or the intended recipient. It also includes examination or inspection of the contents of the data, and diversion of the data or any part thereof from its intended destination to any other destination. o It has been noted that the drafting of this provision includes all the essential elements of the offence of unlawful or illegal interception, and aligns with the international standards in the Budapest Convention.[1573] o The offence of possession of unlawfully-intercepted data (subsection (2)) could affect the capacity of investigative journalists to use information from whistleblowers or caches of data such as Wikileaks. Note that the defence of being able to give a satisfactory exculpatory account of such possession" does not apply in respect of subsection (2), where the person possessing the data *knows* (as opposed to suspects) that is was illegally intercepted.
Section 4: Unlawful acts in respect of software or hardware tool	In terms of subsection (1), it is an offence to unlawfully and intentionally use or possess any software or hardware tool for purposes of – • performing an act in respect of a computer system or a computer data storage medium which places the person who performed the act or any other person in a position to commit any of these offences in subsections 2(2), 3(1), 5(1) or 6(1), as contemplated in subsection 2(1) • unlawful access as contemplated in subsection 2(2) • unlawful interception of data as contemplated in subsection 3(1) • unlawful interference with data or a computer program as contemplated in subsection 5(1) • interference with a computer data storage medium or a computer system as contemplated in subsection 6(1) • acquiring or using a password, an access code or similar data or device for committing one of a list of offences, as contemplated in subsection 7(1)(a) or (d). A "software or hardware tool" means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designed or adapted primarily for the purpose of - • "access as contemplated in section 2(1) or 2(2)" • interception of data as contemplated in section 3(1)

[1573] Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 72.

	• interference with data or a computer program as contemplated in section 5(1) • interference with a computer data storage medium or a computer system as contemplated in section 6(1) • acquiring, making available or using a password, access code or similar data or device as defined in section 7(3). o The cross-referenced offence in section 2(1) is referred to here as "access" but is in fact performing an act in respect of a computer system or a computer data storage medium which places the person who performed the act or any other person in a position to commit any of these offences in subsections 2(2), 3(1), 5(1) or 6(1). o This section has been praised for criminalising only the unlawful and intentional securing of access. The most commendable aspect is that it crucially relates the criminalised act to the commission of other specific offences under the Act.[1574] o This provision, because it refers to tools "*primarily*" designed or adapted for unlawful purposes, avoids capturing dual-use tools. This provision is also appropriately narrowed by its reference to the use of the tools in question for the purpose of committing specific offences.
Section 5: Unlawful interference with data or computer program	In terms of subsection (1), it is an offence to unlawfully and intentionally interfere with data or a computer program. The meaning of "interfere with data or a computer program" in this section is to permanently or temporarily do any of the following acts to data or a computer program held in a computer data storage medium or a computer system - • delete it • alter it • render it vulnerable, damage or deteriorate • render it meaningless, useless or ineffective • obstruct, interrupt interfere with its lawful use or deny access to it.
Section 6: Unlawful interference with computer data storage medium or computer	It is an offence to unlawfully and intentionally interfere with a computer data storage medium or a computer system. The meaning of "interfere with a computer data storage medium or a computer system" in this section is to permanently or temporarily do any of the following acts to a computer data storage medium or a computer system: • alter any resource • interrupt or impair its functioning, confidentiality, integrity, or availability. o It is been noted that unlawful activities such as website defacement would fall within the ambit of sections 5 and 6.[1575]
Section 7: Unlawful acquisition, possession, provision,	In terms of subsection (1), it is an offence to unlawfully and intentionally acquire, possess, provide to another person or use a password, an access code or similar data or device for purposes of committing any of the following offences: • performing an act in respect of a computer system or a computer

[1574] Id, page 69.
[1575] Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).

receipt or use of password, access code or similar data or device	data storage medium which places the person who performed the act or any other person in a position to commit any of these offences in subsections 2(2), 3(1), 5(1) or 6(1), as contemplated in subsection 2(1) • unlawful access as contemplated in subsection 2(2) • unlawful interception of data as contemplated in subsection 3(1) • interference with data or a computer program as contemplated in subsection 5(1) • interference with a computer data storage medium or a computer system as contemplated in subsection 6(1) • cyber fraud as contemplated in section 8 • cyber forgery as contemplated in subsection 9(1). In terms of subsection (2), it is an offence to be in possession of a password, an access code or similar data or device in regard where there is a reasonable suspicion that it was acquired, is possessed, is to be provided to another person or was or may be used for purposes of committing any of the listed offences, in the absence of "a satisfactory exculpatory account": • performing an act in respect of a computer system or a computer data storage medium which places the person who performed the act or any other person in a position to commit any of these offences in subsections 2(2), 3(1), 5(1) or 6(1), as contemplated in subsection 2(1) • unlawful access as contemplated in subsection 2(2) • unlawful interception of data as contemplated in subsection 3(1) • interference with data or a computer program as contemplated in subsection 5(1) • interference with a computer data storage medium or a computer system as contemplated in subsection 6(1) • cyber fraud as contemplated in section 8 • cyber forgery as contemplated in subsection 9(1). In this section "password, access code or similar data or device'" includes any of the following which are used for financial transactions or user-authentication in order to access or use data, a computer program, a computer data storage medium or a computer system: a secret code or pin, an image, a security token, an access card, any device, biometric data, a word or a string of characters or numbers. o This provision has been praised for criminalising the possession and use of computer devices and tools only for purposes of committing particular prohibited acts.[1576] o Another positive element is that the offence of possession set out in subsection (2) "offers a basis to exculpate certain legitimate action that may constitute the offence" where a person found in possession of a password or access code "is able to give 'a satisfactory exculpatory account of such possession'" [1577].

[1576] Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, pages 73, 74.
[1577] Id, page 74.

Section 8: Cyber fraud	It is an offence, unlawfully and with the intention to defraud, to make a misrepresentation by means of data or a computer program, or through specified forms of interference with data or a computer program, which causes actual or potential prejudice to another person. The forms of interference with data or a computer programme which constitute this offence are deleting it, altering it, obstructing it, interrupting it or interfering with the lawful use of it (section 5(1)(a), (b) or (e)) The forms of interference with a computer data storage medium or a computer system which constitute this offence are altering any resource (section 6(1)(a)). o This form of cybercrime will often take the form of "phishing" or "spoofing".[1578] o It has been asserted that there was no need for a crime of cyber fraud as the acts it covers could be prosecuted under the common law crime of fraud.[1579]
Section 9: Cyber forgery and uttering	*Cyber forgery:* In terms of subsection (1), it is an offence, unlawfully and with the intention to defraud, to make false data or a false computer program, to the actual or potential prejudice of another person. *Cyber uttering:* In terms of subsection (2), it is an offence, unlawfully and with the intention to defraud, to pass off false data or a false computer program to the actual or potential prejudice of another person.
Section 10: Cyber extortion	It is an offence, unlawfully and intentionally, to commit or threaten to commit certain offences under the Act for the purpose of obtaining any advantage from another person, or compelling another person to perform or to abstain from performing any act. The offences listed are - • unlawful interception of data as contemplated in subsection 3(1) • interference with data or a computer program as contemplated in subsection 5(1) • interference with a computer data storage medium or a computer system as contemplated in subsection 6(1) • acquiring or using a password, an access code or similar data or device for committing one of a list of offences, as contemplated in subsection 7(1)(a) or (d). o Ransomware attacks are good examples of cyber extortion crimes.[1580]
Section 12: Theft of incorporeal property	The common law offence of theft must be interpreted to incudes theft of incorporeal property. o This would apply to theft of things such as data, passwords, computer codes, etc.

In terms of content-related offences, note that **child pornography, grooming and the non-consensual publication of intimate images ("revenge porn")** – covering

[1578] Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
[1579] Id.
[1580] Id.

electronic communications as well as other channels of communication – are addressed in the **Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007,** with many of these provisions having been added as amendments to that law by the Cybercrimes Act.[1581] Depictions of sexual assault and violence against children, are also addressed in the **Films and Publications Act 65 of 1966**, along with "revenge porn"**.**[1582]

Cyber harassment is covered, along with other forms of **harassment**, in the **Protection from Harassment Act 17 of 2011**. That Act creates no new crimes, but rather provides an accessible mechanism for obtaining a protection order to stop the harassment - and making a breach of such a protection order a crime. [1583]

Note that the Cybercrimes Act covers certain forms of **hate speech** in sections 14 and 15 even though hate speech is also covered by **several other laws and Codes of Conduct** (discussed below).

CYBERCRIMES ACT – CONTENT-BASED OFFENCES THE ACT REFERS TO THESE AS "MALICIOUS COMMUNICATIONS".	
Section 13: Definitions	This part of the Act (sections 14-16) relies on definitions specific to this part alone. The definitions of "disclose" and "group of persons" in particular depart from the ordinary meanings of those terms. "**Damage to property**" means damage to any corporeal or incorporeal property, "**Disclose**" in respect of a data message means to • send the data message to a person who is the intended recipient of the electronic communication or any other person. • store the data message on an electronic communications network, where the data message can be viewed, copied or downloaded; or • send or otherwise make available to someone a link to the stored data message. "**Group of persons**" means characteristics that identify an individual as a member of a group, which characteristics include without limitation, race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth or nationality. **"Related person**" means any member of the family or household of a person or any other person in a close relationship with that person.

[1581] Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, as amended up to July 2022; this includes the amendments by the Cybercrimes Act 19 of 2020 (with effect from 1 December 2021) and the subsequent amendments by the Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act 13 of 2021 (with effect from 31 July 2022). The Cybercrimes Act inserts Part 3A into that Act, comprising section 11A on **Harmful disclosure of pornography,** and related provisions 11B-11D. It also inserts section 19A on **Offences relating to child pornography**. For more information on the amendments made by the Cybercrimes Act, this version of the Cybercrimes Act 19 of 2020 includes full details of all its repeals and amendments to other laws.
[1582] See the discussion of the Films and Publications Act 65 of 1996 below.
[1583] Protection from Harassment Act 17 of 2011, as amended by the Domestic Violence Amendment Act 14 of 2021.

	"**Violence**" means bodily harm.
Section 14: Data message which incites damage to property or violence	It is an offence to disclose, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite damage to property belonging to a person or a group of persons or violence to a person or a group of persons. o With respect to a "group of persons", this is a form of hate speech. Where an individual is involved, the offence appears to take the form of incitement to harm, without a hate speech component.
Section 15: Data message which threatens persons with damage to property or violence	It is an offence to unlawfully and intentionally discloses a data message by means of an electronic communications service that. • threatens a person with damage to property belonging to that person or a related person, or violence against that person or a related person. • threatens a group of persons or any individual in or associated with that group with damage to property belonging to such group or individual, or violence against such group or individual. The offence requires that a reasonable person in possession of the same information and with due regard to all the circumstances, would perceive the data message (either by itself or in conjunction with any other data message or information) as a threat of the nature described. o As above, with respect to a "group of persons" or an individual member of that group, this is a form of hate speech. Where an individual is involved without reference to a "group of persons", the offence appears to take the form of incitement to harm, without a hate speech component.
Section 16: Disclosure of data message of intimate image	It is an offence to unlawfully and intentionally disclose, by means of an electronic communications service, a data message of an intimate image of a person without that person's consent. The offence takes place where the individual can be identified as displayed in the data message, is described as being the person who is displayed even if this is not obvious or can be identified from other information as being the person displayed. An "intimate image" can be real or simulated. It means. • a depiction of a person who is nude or with the genital organs or anus displayed, or - in the case of a female person, transgender person or intersex person – the breasts are displayed. • a depiction that displays the covered genital or anal region of a person, or –in the case of a female person, transgender person or intersex person – their covered breasts. However, the depiction qualifies as an intimate image only if the person depicted retained a reasonable expectation of privacy at the time that the data message was made, *and* the image was made in a manner that violates or offends the sexual integrity or dignity of the person depicted or amounts to sexual exploitation.

	○ A "data message" is "data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form" (section 1). ○ "One of the criticisms levelled against the revenge porn provision of the Cybercrimes Act is that criminal consequences are only against the original perpetrator who first disseminates the sexually graphic images, and there are no real consequences for any subsequent sharing by third parties." [1584] ○ The Cybercrimes Act inserts **section 11A** on **Harmful disclosure of pornography** into the **Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007**. This section creates three related offences that use the same definition of disclose that appears in the Cybercrime Act, thus concerning electronic communications: • *Harmful disclosure of pornography*: It is an offence to unlawfully and intentionally disclose pornography in which another person appears or is described where such disclosure (a) takes place without the consent of that person *and* (b) causes any harm - including mental, psychological, physical, social or economic harm – to that person (or to any member of their family or any other person with whom they have a close relationship). • *Threatening to disclose pornography that will cause harm:* It is an offence to unlawfully and intentionally threaten to commit harmful disclosure of pornography. • *Harmful disclosure of pornography related extortion:* It is an offence to unlawfully and intentionally threaten to commit harmful disclosure of pornography for the purposes of obtaining any advantage from the person depicted or described (or from any member of their family or any other person with whom they have a close relationship). "Pornography" has a long and detailed definition but it is essentially "any image, however created, or any description of a person, real or simulated, who is 18 years or older, of an explicit or sexual nature that is intended to stimulate erotic feelings". ○ It is not clear why the offences relating to "intimate images" are in one law and those related to "pornography" are in another. ○ This provision overlaps with section 24E of the Films and Publications Act 65 of 1966, as amended, on the non-consensual distribution of private sexual photographs and films.

Attempting to commit any of the technical or content-based offences is also an offence, as is **conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring another to commit any of these offences**.[1585]

The **penalties** set out in section 19 of the Act provide for enhanced penalties for two categories of "**aggravated offences**" described in section 11 (relating only to certain technical offences). The first category is where certain listed offences are committed in respect of a "restricted computer system", where the perpetrator knew, or reasonably ought to have known or suspected, that the system was a restricted

[1584] Sizwe Snail ka Mtuze andMelody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
[1585] Cybercrimes Act 19 of 2020, section 17.

computer system. A "restricted computer system" means any data, computer program, computer data storage medium or computer system of a financial institution or an organ of state as set out in section 239 of the Constitution, but including a court, [1586] where the system in question is protected by security measures against unauthorised access or use. The second category is where the perpetrator knew, or reasonably ought to have known or suspected, that the offence will cause a danger of serious bodily injury or death, cause a serious risk to health or safety or create a serious public emergency situation. Prosecution of an offence as an aggravated offence requires the authorisation of the Director of Public Prosecutions.

In addition, section 19 provides certain "**aggravating factors**" for the purpose of sentencing:

- committing the offence by electronic means;
- the extent of the prejudice and loss suffered by the complainant or any other person as a result of the offence;
- the extent to which the perpetrator gained financially or otherwise from the offence
- committing the offence in concert with one or more persons.

Section 19 also requires a court to impose a **sentence of imprisonment in respect of certain listed technical offences committed by a perpetrator who has control or access to the data, computer, computer program, computer data storage medium or computer system in question**, or colluded with another person in such a position. A court can impose a sentence other than imprisonment in these circumstances only if there are "substantial and compelling circumstances" for this.

There are certain **protective provisions for victims of malicious communications offences.** While the criminal case is pending, the complainant may apply to a magistrate *ex parte* for a protection order that prohibits disclosure (or further disclosure) of any data message that relates to the criminal charge, or orders an electronic communications service provider to remove or disable access to such a data message.[1587] Once the criminal proceeding is finalised, a trial court which has convicted a person of a malicious communications offence must order that person to refrain from further disclosure of any data message relating to the offence or to destroy the data message and any copies of it. The court must also order the relevant electronic communications service provider to remove or disable access to the data message in question.[1588] In addition, the trial court may, after holding an enquiry, issue a protection order as contemplated in the Protection from Harassment Act, 2011 against a convicted person – or even against an acquitted person – if there is evidence of harassment or attempted harassment of the complainant.[1589]

[1586] In this section of the Constitution, an "organ of state" means any department of state or administration in the national, provincial or local sphere of government, or any other functionary or institution that is exercising a power or performing a function in terms of the Constitution, a provincial constitution or any legislation, but does not include a court or a judicial officer. South African 1996 Constitution, as amended through 2012, section 239.
[1587] Cybercrimes Act 19 of 2020, section 20. *Ex parte* means that the application can be made without notice to the other party.
[1588] Id, section 22(2).
[1589] Id, section 22(1).

In respect of the investigation of offences under the Act, a magistrate or a judge can issue a **search warrant** on the basis of an affidavit made by a police official.[1590] In urgent cases, a search warrant can be issued by a magistrate or judge on the basis of an oral application by a "specifically designated police official",[1591] which is a police official of the rank of captain or higher who has been designated in writing by the National Commissioner and the National Head of the Directorate for this purpose.[1592] **Searches without a warrant** can be conducted where a police official reasonably believes that a search warrant would be issued, but that the delay in obtaining the warrant would defeat the object of the search,[1593] as in the case of other offences.[1594]

The Cybercrimes Act also authorises the interception of "indirect communications" and "real-time communication-related information", through the procedures in the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (discussed below).[1595] The Act also provides for the issue of **expedited preservation orders** by a "specifically designated police official" for 21-day periods, and for the issue of preservation of evidence directions by a magistrate or judge for up to 90 days, which can be made in urgent or exceptional cases on the basis of an oral application by a police official.[1596] A police official made also apply to a magistrate or a judge for a warrant for a "disclosure of data direction", which is a form of **production order**.[1597]

The police are obliged by the Act to establish a designated "**Point of Contact**" to provide immediate assistance with the cybercrimes created by the Act, as well as other computer-related crimes, and to serve as a liaison point for international cooperation.[1598]

The Act also places **reporting obligations on electronic communications service providers and financial institutions** to ensure that they promptly inform police of any suspicion of certain technical cybercrime offences involving their electronic communications system or network. The Cabinet member responsible for policing must issue a list of the offences covered by this duty in the *Government Gazette*.[1599]

The National Director of Public Prosecutions is required by the act to keep **statistics** on all prosecutions for cybercrimes under the Act, and their outcomes.[1600]

[1590] Id, section 29.
[1591] Id, section 30.
[1592] Id, section 1, definition of "specifically designated police official".
[1593] Id, section 32.
[1594] Criminal Procedure Act 51 of 1977, section 25.
[1595] Cybercrimes Act 19 of 2020, section 40.
[1596] Id, sections 41-43. As noted above, a "specifically designated police official".is a police official of the rank of captain or higher who has been designated in writing by the National Commissioner and the National Head of the Directorate for this purpose. Id, section 1, definition of "specifically designated police official".
[1597] Id, section 44.
[1598] Id, sections 48, 52.
[1599] Id, section 54.
[1600] Id, section 56.

B) ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

The **Electronic Communications and Transactions Act 25 of 2002,** which initially contained some provisions on cybercrimes, still covers some issues more typically found in cybercrime laws:

- It contains provisions on **identification and protection of critical databases**. "Critical data" is defined as data that is declared by the Minister to be "of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens". The Minister is empowered to declare certain classes of information as being critical data by notice in the *Government Gazette*, and to establish procedures to be followed in the identification of critical databases where critical data is collected in electronic form.[1601]
- It establishes a register of **cryptography providers**.[1602]
- It provides for the appointment of **cyber inspectors** by the Director-General of the Department of communications and sets out their powers. It gives these inspectors authority to monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authority. It also provides for search and seizure powers, subject to a warrant issued by a magistrate or a judge; however, this power is made subject to section 25 of the Criminal Procedure Act 51 of 1977 which includes a procedure for acting without a warrant where there are reasonable grounds to believe that a warrant would be issued, but the delay in obtaining the warrant would defeat the object of the search.[1603] Some believe that these wide-ranging powers are overbroad, creating the potential for infringements of the right to privacy.[1604]

This Act also provides a **take-down notification procedure**. A complainant must issue a notice to the relevant service provider identifying the allegedly unlawful content. A service provider is not obligated to act on a take-down notification, but a prompt response protects the service provider from liability for caching, hosting or linking to the material in question. The service provider bears no liability for wrongful take-down in response to a take-down notification.

Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down, although this is not a criminal offence.[1605]

One commentator notes that this take-down notification procedure makes no provision for representations to be made by the alleged infringer before the removal of the material in question, and that there is no in-built right of appeal. "These lacunae

[1601] Electronic Communications and Transactions Act 25 of 2002 (current version), sections 53-ff, read with definition of "critical data" and "critical database" in section 1.
[1602] Id, sections 29-ff.
[1603] Id, sections 80-ff.
[1604] Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.
[1605] Electronic Communications and Transactions Act 25 of 2002 (current version), section 77.

are significant in view of the propensity recognised in other jurisdictions for take-down notices to be based on contestable grounds." Furthermore, the fact that service providers are not liable for wrongful takedowns "acts as a disincentive to scrutinise requests for take-downs carefully", particularly This system "which incentivises them to err on the side of caution and 'take down first and ask questions later', irrespective of the legitimacy of the complaint". [1606]

C) FILMS AND PUBLICATIONS ACT 65 OF 1966

The **Films and Publications Act, 1996**[1607] has been expanded to apply to films,[1608] games,[1609] and publications (defined broadly to include "any content made available using the internet").[1610] The 2019 amendments to the Act also make some of its provisions applicable to **"non-commercial online distributors"**, which means any person who distributes content using the internet, for personal or private purposes – which captures any social media user.

Murray Hunter, of Intel watch, stated that some legal opinion was that the 2019 amendments of the Act constituted "mission creep", in that the Films and Publications Board (FPB) saw that "media has spread in different formats and to different platforms, so they have just gradually assumed that their mandate should spread into those locations as well". According to Hunter, the latest iteration of the Act appears to cause confusion on the regulatory landscape, as some of the activities the Act criminalises are already addressed in other laws. Hunter stated that the broadened mandate of the FPB was unworkable in that there was "actually no practical way for them to enforce that mandate". There also appeared to be a "mandate overreach", according to Murray, where the FPB was tasked with regulating "criminal matters", such as those discussed below.

[1606] Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.

[1607] Films and Publications Act 65 of 1996, updated to 1 March 2022. Note that (as of mid-2023) the PDF on this page contained the Act as updated only to 2009, while the "rtf" download contained the Act as updated to March 2022.

[1608] "Film" means "any sequence of visual images recorded in such a manner that by using such recording, such images will be capable of being seen as a moving picture, and includes any picture intended for exhibition through any medium, including using the internet, or device". Id, section 1

[1609] "Game" means "a computer game, video game or other interactive computer software for interactive game playing, including games accessed or played using the internet, where the results achieved at various stages of the game are determined in response to the decisions, inputs and direct involvement of the game player or players". Id.

[1610] "Publication" means, and includes where applicable, "any of the following, published using the internet -

(a) any newspaper, magazine, book, periodical, pamphlet, poster or other printed matter;
(b) any writing or typescript which has in any manner been duplicated;
(c) any drawing, picture, illustration or painting;
(d) any print, photograph, engraving or lithograph;
(e) any record, magnetic tape, soundtrack or any other object in or on which sound has been recorded for reproduction;
(f) computer software which is not a film;
(g) the cover or packaging of a film; and
(h) any figure, carving, statue or model;
(i) any content made available using the internet, excluding a film or game". Id.

The Act prohibits child pornography, provides for certain restrictions on content involving sexual conduct and also regulates **"prohibited content" –** which echoes the South African Constitution by covering content which amounts to propaganda for war, incitement of imminent violence, or advocacy of hatred that is based on an identifiable group characteristic and that constitutes incitement to cause harm. However, whereas the Constitution refers only to "race, ethnicity, gender or religion" in respect of hate speech, this Act covers "race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth and nationality".[1611]

Commercial online distributors have certain duties relating to the classification of materials for commercial distribution. However, more broadly, any person can allege that a publication contains prohibited content, including prohibited content in relation to "services" being offered online by any person, including "non-commercial online distributors". It is not clear what is meant by "services". which is not defined. The complaint goes to the Films and Publications Board (FPB), which can issue a take-down notification in terms of section 77 of the Electronic Communications and Transaction Act, 2002 if it determines that there is "prohibited content". One lawyer comment:

> *The amendments effectively empower the FPB to make decisions as to what is and is not allowed speech under the South African Constitution, which is an issue that the courts struggle to deal with. The FPB will not be appropriately equipped to make such decisions and this provision effectively amounts to online censorship. As such, this may be the subject of constitutional challenge in due course.*[1612]

The Act makes it an offence for any person to knowingly distribute in any medium - including the internet and social media - any film, game or publication that contains **prohibited content**.[1613]

This Act also makes it a criminal offence to create, produce or in any way contribute to any film or photograph that *depicts or describes* **sexual assault and violence against children**, or to create, produce or distribute a film or photograph that *depicts* sexual violence and violence against children. There is no exception which could apply, for instance, to training materials for law enforcement officers or social workers.[1614]

Further offences relate to "**revenge porn**". It is an offence to knowingly expose or distribute private sexual photographs and films in any medium, including the internet and social media, without prior consent of the person depicted and with the intention to cause such person harm.[1615] There is a higher penalty where individuals in the

[1611] Id, definition of "identifiable group characteristic" in section 1.
[1612] John Paul Ongeso, "South Africa: Films and Publications Amendment Act comes into Operation", Bowmans, 3 March 2022.
[1613] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G.
[1614] Id, sections 18G and 24F.
[1615] Id, sections 18F and 24E.

photographs or films are identified or identifiable.[1616] "Private" means that the context indicates that the photograph or film was not intended to be seen by others. "Sexual" refers to material that shows all or part of an individual's exposed female breasts, anus, genitals or pubic area, or anything that a reasonable person would consider to be sexual in nature.[1617]

Each of these three offences is covered by overlapping provisions – one in the chapter on classifications and one in the chapter on exceptions – and there are some subtle distinctions, but the underlying rationale for the multiple statements of the offences is not immediately clear.

An internet service provider must disclose the identity of a person who publishes prohibited content, a film or photograph depicting sexual assault and violence against children or a private sexual photograph or film.[1618]

Internet service providers are also required to register with the FPB and take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography.[1619] It has been observed that it is not clear "what would be considered reasonable steps" - especially in light of the fact that the Electronic Communications and Transaction Act, 2002 specifically provides that there is no general obligation on service providers to monitor data that they transmit or store, or to actively seek facts or circumstances indicating unlawful activity.[1620]

D) HATE SPEECH

An analysis of this complex issue is beyond the scope of the paper.[1621] As already noted, one form of entirely unprotected expression in terms of the **South African Constitution** is "advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm".[1622] Aspects of hate speech are covered by sections 14 and 15 of the **Cybercrimes Act, 2020**.

However, other laws and codes of conduct also address hate speech under a range of definitions.

- The **Promotion of Equality and Prevention of Discrimination Act 4 of 2000 (PEPUDA)** addresses hate speech, which means words based on one or more of the prohibited grounds, that could reasonably be construed to demonstrate a clear intention to be hurtful or harmful, to incite harm or to promote or

[1616] Id, section 24E.
[1617] Id, section 18F(4) and (5).
[1618] Id, section 18E(3).
[1619] Id, section 27A.
[1620] Wilmari Strachan and Naledi Ramoabi, "Amendments to the Films and Publications Act, 1996 are now in force", ENSight, ENS Africa law firm, 17 March 2022, referring to the Electronic Communications and Transactions Act 25 of 2002, section 78(1)
[1621] For information on South African jurisprudence on hate speech, see Jacob Mchangama & Natalie Alkiviadou, "South Africa The Model? A Comparative Analysis of Hate Speech Jurisprudence of South Africa and the European Court of Human Rights" 1 *Journal of Free Speech Law* 543 (2022).
[1622] South African 1996 Constitution, as amended through 2012, section 16(2).

propagate hatred. The "prohibited grounds" are "race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth and HIV/AIDS status" as well as "any other ground where discrimination based on that other ground causes or perpetuates systemic disadvantage, undermines human dignity or adversely affects the equal enjoyment of a person's rights and freedoms in a serious manner". There is an exception for "*bona fide* engagement in artistic creativity, academic and scientific inquiry, fair and accurate reporting in the public interest". Claims of violation of this prohibition are adjudicated by an Equality Court which can impose a range of remedies that are civil in nature.[1623] The reference in this law to hate speech that is "hurtful" was found to be unconstitutional by the Constitutional Court in 2021, on the grounds that, while its inclusion protects the right to dignity, it covers expression which need not spread hatred and so it is not a proportionate limitation of the right to freedom of expression.[1624]

- The **Films and Publications Act 65 of 1996** makes the publication of hate speech an offence. This covers advocacy of hatred that is based on an identifiable group characteristic and that constitutes incitement to cause harm, with "identifiable group characteristic" meaning "race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth and nationality".[1625]

- The **Code of Conduct for Broadcasting Service Licensees** prohibits the broadcast of material that, judged within context, "sanctions, promotes or glamorises violence or unlawful conduct based on race, national or ethnic origin, colour, religion, gender, sexual orientation, age or mental or physical disability". It is also prohibited to broadcast material that advocates hatred based on race, ethnicity, religion or gender and that constitutes incitement to cause harm.) Gratuitous violence is also prohibited, as well as material that sanctions, promotes or glamorises violence or unlawful conduct.[1626]

- Various **codes of conduct issued by industry self-regulatory bodies** also cover hate speech.

[1623] Promotion of Equality and Prevention of Discrimination Act 4 of 2000 (PEPUDA), section 10 read with the definition of "prohibited grounds" in section 1 and the proviso to section 12.
[1624] *Qwelane v South African Human Rights Commission*, [2021] ZACC 22, 30 July 2021; see case summary by Global Freedom of Expression here. See also *AfriForum v EFF, Malema and Ndlozi*, Equality Court, 25 August 2022 and *Afriforum NPC v. Nelson Mandela Foundation Trust*, Supreme Court of Appeal(Case no 371/2020) [2023] ZASCA 58 (21 April 2023).
[1625] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G, definition of "identifiable group characteristic" in section 1.
[1626] Code of Conduct for Broadcasting Service Licensees, 2009, issued in terms of section 54 of the Electronic Communications Act No. 6 of 2005, regulation 3.

- In future, the **Prevention and Combating of Hate Crimes and Hate Speech Bill** that has been under consideration for some time may possibly to be added to the list. This Bill includes a crime of hate speech based on a long list of prohibited grounds, It was passed by the National Assembly in March 2023 and sent to the National Council of Provinces for concurrence, after a long process of discussion and debate.[1627]

E) REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION RELATED INFORMATION ACT 13 OF 2002 (RICA)

The **Regulation of Interception of Communications and Provision of Communication related Information Act 13 of 2002 (RICA)** provides for the registration of SIM cards and contains procedures for the interception of communications by law enforcement officials.[1628]

The Act regulates the **interception of both direct and indirect communications that are transmitted through a postal service or telecommunication system**, including oral conversations, emails and mobile phone communications (including data, text and visual images). Interception of such communications requires authority from a designated Judge, which can apply to real-time or archived communications information. It is also possible for a High Court judge or a magistrate to give authority for interception when only archived communication information is sought. Virtually all of the possibilities for state surveillance involve serious offences: actual or potential threats to public health or safety, national security or compelling national economic interests, organised crime or terrorism) or efforts to locate property which is or could be an instrumentality of a serious offence or the proceeds of crime.[1629] It directs the relevant minister to establish Interception Centres for this purpose.[1630]

The Act also requires **SIM card registration**, by giving telecommunication service providers a duty to collect identifying information in respect of their customers. For individuals, the required information is full name, identity number, residential and business or postal address, and a certified photocopy of his or her identification document which must contain a photo. Similar information is required from the person representing a juristic person who is a customer, along with the juristic person's business name and address, and registration number if it is a registered entity. The identifying information must be verified by the service provider and stored in a

[1627] Prevention and Combating of Hate Crimes and Hate Speech Bill [B9B-2018]; see the *Memorandum on the Objects of the Prevention and Combating of Hate Crimes and Hate Speech Bill* appended to the Bill and the history prepared by the Parliamentary Monitoring Group on the same webpage. "The national legislature or Parliament consists of two Houses: the National Assembly and National Council of Provinces, whose members are elected by the people of South Africa. Each House has its own distinct functions and powers, as set out in the Constitution. The National Assembly is responsible for choosing the President, passing laws, ensuring that the members of the executive perform their work properly, and providing a forum where the representatives of the people can publicly debate issues. The National Council of Provinces is also involved in the law-making process and provides a forum for debate on issues affecting the provinces. Its main focus is ensuring that provincial interests are taken into account in the national sphere of government." "Parliament", National Government of South Africa, undated.

[1628] Regulation of Interception of Communications and Provision of Communication related Information Act 13 of 2002 (RICA), as amended to 1 December 2021. There have been no further amendments as of mid-2023.

[1629] Id, Chapters 2-3.

[1630] Id, Chapter 6.

prescribed manner.[1631] Failure on the part of the service provider to collect the required information is an offence.[1632] ICASA has reportedly proposed linking SIM cards to biometric data.[1633]

The provisions of the Act on surveillance were challenged on the grounds that they interfered with the constitutional right to privacy, in a case that went all the way to the Constitutional Court. The Court found numerous problems with this aspect of the legislation:

1. **It failed to provide for safeguards to ensure that the designated Judge is sufficiently independent.** The Act allows the relevant minister to designate a retired judge for the purposes of the Act. Most of the interception directions provided for in the Act are to be issued on the authority of a designated judge. The Court held that the open-ended discretion for the appointment of a designated judge and the lack of any external oversight of accountability meant that the independence of this judge could not be assured.

2. **It failed to provide for post-surveillance notice to the subject of the surveillance**, which is an important safeguard against abuse of surveillance powers.

3. **It failed to adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte**. While informing the subject of the surveillance would negate its purpose, the Court held that some adversarial process needed to be introduced, perhaps by the introduction of a "public advocate" who could argue the other side.

4. **It failed to adequately prescribe procedures to protect the data that was intercepted**, to prevent unlawful disclosure or abuse. Procedures were needed to regulate examining, copying, sharing, sorting, using, storing and destroying the data.

5. **It failed to provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist,** to protect attorney-client privilege in respect of lawyers and the confidentiality of sources in respect of journalists.

The Constitutional Court thus found RICA unconstitutional in these respects but suspended the declaration of unconstitutionality for 36 months to afford Parliament an opportunity to cure the defects (a time period that will expire in early 2024). It also read certain safeguards into the law as an interim measure: a requirement for post-surveillance notification to the subject within 90 days of the end of the surveillance, and a provision aimed at the confidentiality issues for lawyers and journalists.[1634]

In addition, the Court held that the **bulk surveillance** that was being undertaken in

[1631] Id, Chapter 7.
[1632] Id, section 51(3)(a).
[1633] Ruan Jooste, "Rica SIM card registration laws in SA are ineffective in reducing crime", IOL Business Report, 30 August 2022.

[1634] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* [2021] ZACC 3, 4 February 2021; see the case summary by Global Freedom of Expression here.

practice by the National Communication Centre was not authorised by the law and was therefore unlawful and invalid.[1635]

The government has proposed a new law, the **General Intelligence Laws Amendment Bill (GILAB)**, to fill that gap. The bill proposes amendments to the **National Strategic Intelligence Act 39 of 1994** concerning the National Communications Centre which would set the stage for mass surveillance of the sort that RICA was found not to have authorised.[1636]

F) TAKE-DOWN NOTIFICATIONS

Take-down notifications are authorised by section 77 of the **Electronic Communications and Transactions Act 25 of 2002** and have been discussed above. It is worth noting that the Internet Service Providers' Association (ISPA) keeps statistics on take-down notifications which indicate that all but a tiny proportion of them result in the removal of the material in question.[1637]

15.5 ELECTION LAW AND FREEDOM OF EXPRESSION

South Africa is scheduled to hold general elections in May 2024, for provincial legislatures and the National Assembly. The National Assembly, the upper house of the country's bicameral Parliament, then elects the President. The 400-seat National Assembly is elected by party-list proportional representation. The 90 members of the upper chamber, the National Council of Provinces, are selected by provincial legislatures. Municipal elections are held separately from the national and provincial elections.[1638]

Elections in South Africa are administered by the **Electoral Commission**, also referred to as the "Independent Electoral Commission" (**IEC**). The Constitution sets out the basic framework for this body, which is further regulated by the **Electoral Commission Act 51 of 1996**.[1639] Elections are governed by the **Electoral Act 73 of 1998**.[1640] According to Freedom House: "The Independent Electoral Commission (IEC) is largely considered independent, and the electoral framework is considered fair."[1641]

[1635] Id, paragraphs 124-135
[1636] General Intelligence Laws Amendment Bill; Heidi Swart, "GILAB: New Intelligence Bill a blueprint for State Capture 3.0", *News24*, republished by *Intelwatch*, 11 July 2023. For more detailed information on potential law reforms on communications surveillance in South Africa, see Catherine Kruyer, "Reforming Communication Surveillance in South Africa: Recommendations in the wake of the *AmaBhungane* judgment and beyond", Intelwatch & The Media Policy and Democracy Project Report, May 2023
[1637] The ISPA statistics can be found here.
[1638] See "Freedom in the World 2023: South Africa", Freedom House, sections A1-A2.
[1639] Electoral Commission Act 51 of 1996.
[1640] Electoral Act 73 of 1998.
[1641] "Freedom in the World 2023: South Africa", Freedom House, section A3.

SOUTH AFRICAN CONSTITUTION

190. Functions of Electoral Commission

1. The Electoral Commission must -
- manage elections of national, provincial and municipal legislative bodies in accordance with national legislation.
- ensure that those elections are free and fair; and
- declare the results of those elections within a period that must be prescribed by national legislation and that is as short as reasonably possible.

2. The Electoral Commission has the additional powers and functions prescribed by national legislation.

191. Composition of Electoral Commission

The Electoral Commission must be composed of at least three persons. The number of members and their terms of office must be prescribed by national legislation.

Apartheid South Africa was replaced by the new dispensation in 1994, when the country held its first democratic elections. The national liberation movement, the African National Congress (ANC), emerged as the majority party with 62.7% of the vote. Its support peaked at 70% in 2004 and then began to decline in successive elections, from 62% in 2014 to less than 58% in 2019, as citizens have become increasingly frustrated with state corruption and the slow pace of socioeconomic development. The 2019 elections did, however, confirm public support for President Cyril Ramaphosa, who was first inaugurated in 2018 after former President Jacob Zuma resigned prematurely in the wake of his involvement in serious corruption. It is widely predicted that the ANC will lose its majority in 2024 and be forced to form a coalition to remain in power.[1642] Looking at the wider political context:

> *Political parties are institutionalized and highly organized. While the ANC has dominated national politics and achieved comfortable majorities in each national election, the last decade has seen the emergence of two notable opposition parties, namely the centre-right DA, which controls the Western Cape province and won 21% of the national vote in 2019, and the populist left-wing EFF, which increased its national share of votes from 6% to 10% in the last two elections and is now the main opposition party in several provinces. The DA's rise has been driven by dissatisfaction with the ANC, primarily around corruption and poor services, among urban residents in the major cities, while the EFF has outflanked the ANC on issues of radical economic change, courting the interest of younger black and primarily male voters. The 2019 elections were also notable for the increase in votes to smaller opposition parties, demonstrating voters' dissatisfaction with the major parties, including from the opposition.*
>
> *The biggest challenge of the political parties remains to attract the increasing number*

[1642] "Namibia and South Africa's ruling parties share a heroic history - but their 2024 electoral prospects look weak", *The Conversation*, 10 May 2023; "South Africa Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".

of non-voters. Taking registered and non-registered voters into account, the voter turnout is only 49%. The most prominent reasons are dissatisfaction with the political parties in general and lack of confidence that any different voting behaviour might outnumber the ANC in parliament. Political parties are not very deeply rooted in civil society, with some exceptions like the relationship between trade unions and the ANC. Moreover, many civil society organizations prefer an antagonistic relationship with political parties.[1643]

In 2020, the Constitutional Court ruled that a section of the Electoral Act that prohibits independent candidates from contesting elections without a partisan affiliation was unconstitutional and ordered parliament to amend the legislation to allow for independent candidates […]. Although it is unlikely that this amendment to the law will have any significant consequence for party politics or elections in South Africa, it is nevertheless a positive sign in a young democracy that there are possibilities to reform legislation to ensure equal opportunities to seek political office.[1644]

The **Electoral Act 73 of 1998** contains several provisions pertaining to speech. Violation of any of the following prohibitions is an offence in terms of section 97:

- Section 89(2) prohibits any person from publishing any false information with the intention of disrupting or preventing an election, influencing the conduct or outcome of an election , or creating hostility or fear in order to influence the conduct or outcome of an election.
- Section 90(2) prohibits anyone from disclosing any information about voting or the counting of votes except as permitted in terms of this Act.
- In terms of section 92, no person may deface or unlawfully remove any billboard, placard or poster published by a registered party or candidate during the election period.
- In terms of section 107, any printed matter (billboard, placard, poster or pamphlet) intending to affect the outcome of an election must state clearly the full name and address of the printer and publisher if issued during the election period, and paid material originating from a political party or its members or supporters must be clearly labelled as an advertisement.
- Section 108 prohibits holding or participating in any political meeting, march, demonstration or other political event, or engaging in any other political activity (other than voting) within the boundary of a voting station on voting day.
- Section 108 prohibits printing, publishing or distributing the result of any exit poll taken in respect of an election during the prescribed hours for the election.[1645]

There is an extensive range of potential penalties and remedies for violation of the Electoral Act.[1646]

While all these restrictions appear to have legitimate aims, some are formulated in a way that could allow for selective implementation - especially in terms of

[1643] "South Africa Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political and Social Integration".
[1644] Id, "Executive Summary".
[1645] Electoral Act 73 of 1998.
[1646] Id, section 96(2).

understanding precisely what is forbidden in terms of false information intended to influence an election outcome or disclosing information "about voting".

The Electoral Act also contains an Electoral Code of Conduct.[1647] Every registered party and every candidate must comply with this Code and take reasonable steps to ensure that their party members, representatives and supporters also comply with the Code and any applicable electoral laws.[1648]

Focusing on the provisions related to freedom of expression, this Code obligates every registered party and every candidate to state publicly state that everyone has these rights -

(i) to freely express their political beliefs and opinions;
(ii) to challenge and debate the political beliefs and opinions of others;
(iii) to publish and distribute election and campaign materials, including notices and advertisements;
(iv) to lawfully erect banners, billboards, placards and posters;
(v) to canvass support for a party or candidate;
(vi) to recruit members for a party;
(vii) to hold public meetings; and
(viii) to travel to and attend public meetings.[1649]

Parties and candidates are also required to publicly condemn any action that may undermine the free and fair conduct of elections.[1650]

No registered party or candidate may –

- use language or act in a way that may provoke violence or intimidation during an election;
- publish false or defamatory allegations about a party, a candidate or their representatives or members; or
- plagiarise the symbols, colours or acronyms of other registered parties.[1651]

No person may deface or unlawfully remove or destroy the billboards, placards, posters or any other election materials of a party or candidate.[1652]

There is also a specific provision on the role of the media in elections.[1653].

ELECTORAL CODE OF CONDUCT

8. Role of media
Every registered party and every candidate -
(a) must respect the role of the media before, during and after an election conducted in terms of this Act;
(b) may not prevent access by members of the media to public political meetings, marches, demonstrations and rallies; and
(c) must take all reasonable steps to ensure that journalists are not subjected to harassment, intimidation, hazard, threat or physical assault by any of their representatives or supporters.

[1647] Electoral Code of Conduct, Electoral Act 73 of 1998, Schedule 2.
[1648] Id, item 3.
[1649] Id, item 4(1)(a).
[1650] Id, item 4(1)(b).
[1651] Id, item 9(1)(a)-(c).
[1652] Id, item 9(2)(d).
[1653] Id, item 8.

An example of the difficulties of interpretation can be seen in the case of ***Democratic Alliance v African National Congress***.[1654] In the run-up to the 2014 elections, the Democratic Alliance (DA) (the official opposition party) sent this SMS to 1.5 million voters ahead of the 2014 elections, referring to then-President Zuma: "The Nkandla report shows how Zuma stole your money to build his R246m home. Vote DA on 7 May to beat corruption. Together for change."[1655]

The African National Congress (ANC) (the ruling party) argued that the publication was prohibited under the Electoral Act as a **false statement intended to influence the outcome of the elections** in violation of both the Electoral Act and the Electoral Code of Conduct. The DA conceded that the SMS was intended to influence the outcome of the elections, but took the view that it was not a false statement but rather a fair comment or an opinion that was honestly and genuinely held.

In a split decision, the Constitutional Court held that the publication was not a statement of fact, but a valid opinion about the report, and so was not prohibited by the Electoral Act or the Electoral Code of Conduct. An opinion joined by five justices stated that "freedom of expression to its fullest extent during elections enhances, and does not diminish, the right to free and fair elections. The right individuals enjoy to make political choices is made more meaningful by challenging, vigorous and fractious debate".[1656] These justices found that the kind of false statements prohibited by section 89(2) of the Electoral Act are "those that could intrude directly against the practical arrangements and successful operation of an election" – such as false statements that a candidate has died, or that voting hours have been changed, or that a bomb has been placed at a particular voting station.[1657] It also found that section 89(2) of the Electoral Act and the prohibition on false or defamatory allegations about a party or a candidate in the Electoral Code of Conduct both apply only to false statements of fact and not to opinions.[1658] Two other justices agreed with the outcome, expressing the view that a statement of opinion *can* constitute false information but that the SMS in question in this case did not.[1659] Three justices were of the opinion that the SMS would have been understood by the ordinary reader as a statement of fact and not as a comment and that it was a false statement of the contents of the Nkandla report.[1660] The differing opinions in this case illustrate the difficulty of applying the prohibitions on false statements.

[1654] *Democratic Alliance v African National Congress* [2015] ZACC 1, 19 January 2015; see the case summary by Global Freedom of Expression here.
[1655] Nkandla is the name of then-President Zuma's private residence. The Nkandla Report was the report of an investigation by South Africa's Public Protector [Ombud] into complaints about the enormous costs of installing security measure at that residence. Id, paragraphs 7-ff and footnote 7 (dissenting opinion of Zondo, J).
[1656] Id, paragraph 135 in the joint opinion of Cameron J, Froneman J and Khampepe J (Moseneke DCJ and Nkabinde J concurring), which begins at paragraph 116:
[1657] Id, paragraphs 139-140.
[1658] Id paragraphs 144-147.
[1659] Opinion of Van der Westhuizen J (Madlanga J concurring), paragraphs 170-ff.
[1660] Opinion of Zondo J (Jafta J and Leeuw AJ concurring), starting at paragraph 1.

In 2019, in the case of ***Brown v Economic Freedom Fighters***, the High Court considered the **obligations of political parties and their leaders under the Electoral Code of Conduc**t. South African political journalist Karima Brown erroneously sent a WhatsApp message to a group established by the spokesperson of the Economic Freedom Fights (EFF), a registered South African political party. The President of the EFF, Julius Malema, published a screenshot of the message on Twitter, where he had over 3 million followers, with Brown's name and personal mobile telephone number circled in black and a claim that Brown was "sending moles to EFF events". The following day, the EFF released a statement claiming that Brown was not a legitimate journalist but an operative for the South African ruling party. EFF supporters subjected Brown to a barrage of harassment and threats, including threats of rape, violence and murder. Malema held a press conference where he stated that no person should be threatened with rape and violent crime, but continued to maintain that Brown was a state intelligence operative and not a legitimate journalist. The Court ruled that the EFF and its leaders needed to take reasonable steps to condemn and stop the harassment of the journalist in order to comply with its obligations under the Electoral Code of Conduct. However, it also noted that the "strident and political tone adopted by Ms Brown in her responses on social media to the EFF, only fuelled the flames of discord and did little to garner the respondents' sympathy for her plight. Whilst the conduct of the respondents must be severely criticised and the supine attitude, they adopted to their obligations condemned, the provocative stance adopted by Ms Brown constitutes a weighty mitigating factor in determining an appropriate sanction". The Court issued a formal warning to the EFF.[1661]

Another significant election-related case concerns the **right to information about political party funding**. In the 2018 case of ***My Vote Counts v Minister of Justice and Correctional Services***, the Constitutional Court declared that "information on the private funding of political parties and independent candidates is essential for the effective exercise of the right to make political choices and to participate in the elections". It declared that such must be recorded, preserved and made reasonably accessible to the public. Furthermore, it declared the Promotion of Access to Information Act 2 of 2000 constitutionally invalid to the extent that it failed to provide for this and ordered Parliament to amend the law to this effect within 18 months.[1662]

In terms of broadcasting during election periods, there are several detailed provisions in the **Electronic Communications Act 36 of 2005**, reproduced below. The requirement of equitable treatment and the right of reply contained in section 59 are particularly noteworthy.

[1661] Brown v Economic Freedom Fighters, High Court of South Africa, Gauteng Local Division, Johannesburg, Case No: 14686/2019, 6 June 2019; see the case summary by Global Freedom of Expression here. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, pages 333-334.
[1662] *My Vote Counts v Minister of Justice and Correctional Services* [2018] ZACC 17, 21 June 2018.
see the case summary by Global Freedom of Expression here.

ELECTRONIC COMMUNICATIONS ACT 36 OF 2005

56. Prohibition on broadcasting of party election broadcasts and political advertisements except in certain circumstances

A party election broadcast and a political advertisement must not be broadcast on any broadcasting service except during an election period and then only if, and to the extent authorised by the provisions of sections 57 and 58.

57. Broadcasting of party election broadcasts on public broadcasting services

(1) Subject to the provisions of this section, a public broadcasting service licensee must permit a party election broadcast only during an election period and then only if such a broadcast is produced on behalf of the political party in question at the instance of its duly authorised representative.

(2) The Authority [ICASA] must determine the time to be made available to political parties for the purposes of subsection (1), including the duration and scheduling of party election broadcasts, taking into account the financial and programming implications for the broadcasting services in question.

(3) The Authority must consult with the relevant public broadcasting service licensee and all the political parties prior to making any determination in terms of subsection (2).

(4) In making any determination in terms of subsection (2), the Authority may impose such conditions on a public broadcasting service licensee with respect to party election broadcasts as it considers necessary, having due regard to the fundamental principle that all political parties are to be treated equitably.

(5) A party election broadcast may not contain any material which may reasonably be anticipated to expose the broadcasting service licensee to legal liability if such material were to be broadcast.

(6) A party election broadcast must conform to a technical quality acceptable to the Authority.

(7) No party election broadcast may be broadcast later than 48 hours prior to the commencement of the polling period.

(8) A commercial or community broadcasting service licensee is not required to broadcast party election broadcasts, but if he or she elects to do so, the preceding provision of this section applies, with the necessary changes.

58. Political advertising on broadcasting services

(1) A broadcasting service licensee is not required to broadcast a political advertisement, but if he or she elects to do so, he or she must afford all other political parties, should they so request, a like opportunity.

(2) A broadcasting service licensee may broadcast a political advertisement only during an election period and then only if it has been submitted to such licensee on behalf of a political party by its duly authorised representative.

(3) In making advertising time available to political parties, no broadcasting service licensee may discriminate against any political party or make or give any preference to any political party or subject any political party to any prejudice.
(4) A political advertisement may not contain any material which may reasonably be anticipated to expose the broadcasting service licensee to legal liability if such material were to be broadcast.
(5) A political advertisement must conform to a technical quality acceptable to the Authority.
(6) No political advertisement may be broadcast later than 48 hours prior to the commencement of the polling period.
(7) This section is subject to the provisions of any law relating to the expenditure of political parties during an election period.

59. Equitable treatment of political parties by broadcasting service licensees during election period

(1) If, during an election period, the coverage of any broadcasting service extends to the field of elections, political parties and issues relevant thereto, the broadcasting services licensee concerned must afford reasonable opportunities for the discussion of conflicting views and must treat all political parties equitably.

(2) In the event of any criticism against a political party being levelled in a particular programme of any broadcasting service -
(a) without such party having been afforded an opportunity to respond thereto in such programme; or
(b) without the view of such political party having been reflected therein, the broadcasting services licensee concerned must afford such party a reasonable opportunity to respond to the criticism.

(3) If, within 48 hours before the commencement of the polling period or during the polling period, a broadcasting services licensee intends broadcasting a programme in which a particular political party is criticised, the licensee must ensure that the political party in question is given a reasonable opportunity to -
(a) respond thereto in the same programme; or
(b) respond thereto as soon as is reasonably practicable thereafter.

(4) Subsection (3) does not apply in relation to the contents of any party election broadcast in the circumstances contemplated in section 57 and any political advertisement in the circumstances contemplated in section 58.

CHAPTER 16

TANZANIA

CHAPTER 16: TANZANIA

TANZANIA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **143rd globally; 45th out of 48 African countries** (lowest ranking in SADC) "After the sudden death in March 2021 of President John Magufuli, who had become increasingly authoritarian and hostile towards the media, Samia Suluhu Hassan's rise to power brought initial hopeful signs that have yet to come to fruition."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: United Republic of Tanzania's 1977 Constitution, as amended through 2005 The quoted provisions apply to the United Republic of Tanzania, including mainland Tanzania and Zanzibar. (See Article 29.) However, Zanzibar retains a degree of autonomy in its laws and government, and the Zanzibar Constitution 1984 similarly protects freedom of expression in Article 18, subject to limits set out in Article 24. **18. FREEDOM OF EXPRESSION** Every person – a. has a freedom of opinion and expression of his ideas; b. has a right to seek, receive and, or disseminate information regardless of national boundaries; c. has the freedom to communicate and a freedom with protection from interference from his communication; d. has a right to be informed at all times of various important events of life and activities of the people and also of issues of importance to the society. **30. LIMITATIONS UPON, AND ENFORCEMENT AND PRESERVATION OF BASIC RIGHTS, FREEDOMS AND DUTIES** 1. The human rights and freedoms, the principles of which are set out in this Constitution, shall not be exercised by a person in a manner that causes interference with or curtailment of the rights and freedoms of other persons or of the public interest. 2. It is hereby declared that the provisions contained in this Part of this Constitution which set out the basic human rights, freedoms and duties, do not invalidate any existing legislation or prohibit the enactment of any legislation or the doing of any lawful act in accordance with such legislation for the purposes of – a. ensuring that the rights and freedoms of other people or of the interests of the public are not prejudiced by the wrongful exercise of the freedoms and rights of individuals;

b. ensuring the defence, public safety, public order, public morality, public health, rural and urban development planning, the exploitation and utilization of minerals or the increase and development of property or any other interests for the purposes of enhancing the public benefit; c. ensuring the execution of a judgment or order of a court given or made in any civil or criminal matter; d. protecting the reputation, rights and freedoms of others or the privacy of persons involved in any court proceedings, prohibiting the disclosure of confidential information, or safeguarding the dignity, authority and independence of the courts; e. imposing restrictions, supervising and controlling the formation, management and activities of private societies and organizations in the country; or f. enabling any other thing to be done which promotes or preserves the national interest in general.
KEY LAWS: • The Cybercrimes Act 14 of 2015 • Media Services Act 12 of 2016, as amended in 2023[1663] • Electronic and Postal Communications (Online Content) Regulations, 2020, as amended by the Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022 • The Penal Code [*Chapter 16*], Revised Edition 2022 (selected provisions) and Zanzibar Penal Act 6 of 2018 (selected provisions)
CRIMINAL DEFAMATION: Yes, although the East African Court of Justice found the provisions on criminal defamation in the Media Services Act, 2016 to be an unjustifiable infringement of freedom of expression[1664]
DATA PROTECTION: Tanzania has a data protection law.[1665]
ACCESS TO INFORMATION: Tanzania has access to information law.[1666]

16.1 CONTEXT

The **United Republic of Tanzania** consists of "**Mainland Tanzania**" and "**Tanzania Zanzibar**";[1667] these are the official legal terms, although it is more common to refer simply "Mainland Tanzania" and "Zanzibar". There are some different laws that regulate the media and impact freedom of expression in Mainland Tanzania and in the semi-autonomous area of Zanzibar, while some laws – including the Cybercrime

[1663] See The Written Laws (Miscellaneous Amendments) Act, 2023 (published in bill form); the final amendment Act could not be located online.
[1664] *Media Council of Tanzania & 2 Others v Attorney General of the United Republic of Tanzania*, East African Court of Justice, Case No 2 of 2017, 28 March 2019. Some amendments to the Act in question were made in 2023 but they did not remove criminal defamation.
[1665] The Personal Data Protection Act 11 of 2022.
[1666] The Access to Information Act 6 of 2016.
[1667] United Republic of Tanzania's 1977 Constitution, as amended through 2005, Article 2(1).

Act,[1668] the Tanzania Communications Regulatory Authority Act[1669] the Electronic and Postal Communications Act[1670] and the Tanzania Telecommunications Corporation Act 12 of 2017[1671] - apply throughout the United Republic of Tanzania.

The **Tanzania Communications Regulatory Authority Act, 2003** creates the **Tanzania Communications Regulatory Authority (TCRA)**, which is an amalgamated body that brings together the former Tanzania Communications Commission and the former Tanzania Broadcasting Commission. The TCRA is charged, amongst other things, with issuing licences and setting standards for the "regulated sector", which includes telecommunications, radio and television broadcasting, postal services, and electronic technologies including the internet and other ICT applications. It also monitors the performance of the regulated sectors and facilitates the resolution of disputes and complaints.[1672] The President appoints the Chairman and Vice-Chairman of the Board, while the relevant minister appoints the other Board members and the Director-General. However, all appointments must be from amongst candidates short-listed by a Nomination Committee made up of government and private sector representatives.[1673] Interestingly, the TCRA is required to conduct an annual consultation process with stakeholders (identified by the TCRA) for the purpose of effectively carrying out its functions.[1674] It is also required to maintain a Public Register of key decisions and information that is open to public inspection.[1675] Amongst the subsidiary bodies set up under the law is a "Content Committee" appointed by the minister to advise the Sector Minister on broadcasting policy and to monitor and regulate broadcast content,[1676] and a "Consumer Council" to consult with industry, government and other consumer groups and to represent consumer interests.[1677]

The **Tanzania Communications Regulatory Authority Act, 2003** establishes the **Tanzania Broadcasting Services** (TBC or TUT, based on its Kiswahili name) as a state broadcaster. The President appoints the Chairperson and the Director-General of the TBC, while the relevant minister appoints the other board members.[1678]

Another key piece of legislation is the **Electronic and Postal Communications Act (Revised Edition 2022)**, which is aimed at providing a comprehensive regulatory

[1668] The Cybercrimes Act 14 of 2015, section 2: "Save for section 50 [on the compounding of offences], this Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar."
[1669] The Tanzania Communications Regulatory Authority Act 12 of 2003, section 2(3)-(4). The Act does not apply to Tanzania Zanzibar with respect to broadcasting and content matters.
[1670] The Electronic and Postal Communications Act [Chapter 306 R E. 2022], section 2 (with an exception for the activities that fall within the jurisdiction of the Zanzibar Broadcasting Commission under the Zanzibar Broadcasting Commission Act 7 of 1997). The initial Electronic and Communications Act was Act 3 of 2010, but it has been amended several times since it was passed.
[1671] The Tanzania Telecommunications Corporation Act 12 of 2017, section 2.
[1672] The Tanzania Communications Regulatory Authority Act 12 of 2003 as amended by The Electronic and Postal Communications Act, 2010 (amending sections 3, 15, 21, 26-27, 33-35, 41-42, 45, 47-48, 51 and the Schedule), Part II read with the definition of "regulated sector" in section 3.
[1673] Id, section 13.
[1674] Id, section 22.
[1675] Id, section 23.
[1676] Id, Part IV.
[1677] Id, Part VII.
[1678] Further details regarding the TBC are set out in the Public Corporation (The Tanzania Broadcasting Services) (Establishment) Order, 2002, G.N. No. 239 of 2002 (not located online), See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 37-39. The TBC is established under section 4 of the Public Corporation Act.

regime for electronic communications service providers under the TCRA. It provides for the licensing of different categories of "content services" and provides for the imposition of a range of content restrictions – which are discussed in detail below.[1679]

The **Tanzania Telecommunications Corporation Act, 2017** sets up a public telecommunications corporation aimed at enhancing the safety, security, economic and commercial viability of national telecommunications services and telecommunications infrastructure.[1680]

The **Media Council of Tanzania** is a self-regulatory body established in 1995 which operates in respect of both Tanzania and Zanzibar. It has developed a Code of Ethics for Media Professionals and a Professional Code for Journalists.[1681] MISA-Tanzania recommends that this body "should take more initiative in tackling the problem of declining professional standards and ethics among Tanzanian journalists without depending on government support.[1682]

A) TANZANIA

The **Media Services Act, 2016**, which applies only to Mainland Tanzania,[1683] provides for the licensing of print media and the accreditation of journalists through a Journalists Accreditation Board. It also contains provisions on the rights and obligations of media houses (which include print media, radio and television broadcasters and online content providers). The Act gives the relevant minister broad powers to ban or suspend publications on national security or public safety grounds,[1684] and this power has been applied in practice against various media outlets.[1685] The Act also contains a chapter on criminal defamation,[1686] and a number of other offences concerning content that could inhibit freedom of expression (discussed in more detail below).[1687] It also sets up an **Independent Media Council** which is tasked to adopt a Code of Ethics for professional journalists, review the performance of the media sector, promote media accountability and handle complaints relating to print media only. All accredited journalists are members of the Council, which elects its own leadership. The Council is expected to adhere to "national unity, national security, sovereignty, integrity and public moral" in carrying out its functions.

In March 2019, the **East African Court of Justice** directed Tanzania to amend the

[1679] The Electronic and Postal Communications Act [Chapter 306 R E. 2022]. Note that section 167A of this law repeals the Broadcasting Services Act 6 of 1993 and the Tanzania Communications Act 18 of 1993. See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 30-ff.
[1680] The Tanzania Telecommunications Corporation Act 12 of 2017.
[1681] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 68-ff and 122. The Media Council of Tanzania recently produced an analysis of the Electronic and Postal Communications (Online Content) Regulations 2020 which is discussed below.
[1682] "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 31.
[1683] Media Services Act 12 of 2016, section 2.
[1684] Id, section 59.
[1685] "Tanzania: Victory for media freedom as ban on four newspapers lifted", Amnesty International, 11 February 2022.
[1686] Media Services Act 12 of 2016, Part V.
[1687] Id, Part VII.

Media Services Act after finding a number of its provisions - including those on sedition, criminal defamation, and the publication of false news - to be contrary to the Treaty for the Establishment of the East African Community and the right to freedom of expression. The offending sections were as follows:

- Sections 7(3)(a), (b), (c), (f), (g), (h), (i) and (j): Section 7(3) of the Act requires media houses to make sure that the information they issue complies with a list of requirements – such as ensuring that information does not undermine national security or lawful investigation; "constitute hate speech"; "involve an unwarranted invasion of an individual's privacy" or cause substantial harm to the Government's ability to manage the economy. The Court found that eight of the ten categories of content restrictions were invalid under Tanzania's international obligations regarding freedom of expression because they did not adequately define what was prohibited by the legislation and had not been shown to be a proportionate response to a legitimate aim.
- Section 19-21: These sections concerning the accreditation of journalists were also held to be invalid restrictions on freedom of expression. Although the accreditation of journalists is not necessarily objectionable, the scheme in the Media Service Act relies on a definition of "journalist" that is too difficult to define with precision and was not tied to a legitimate state aim.
- Sections 35-40: Section 35 deals with criminal defamation, as detailed in the following sections. The Court the use of criminal sanctions had a chilling effect on journalists' freedom of expression and was thus a disproportionate limitation on freedom of expression.
- Section 50(1)(c)(i): This provision makes it an offence to use a media service to publish any statement that threatens "the interests of defence, public safety, public order, the economic interests of the United Republic, public morality or public health". The Court held that this restriction was too broad and imprecise to pass muster.
- Section 54: This restriction on publishing any false statement, rumour or report "likely to cause fear or alarm to the public or to disturb the public peace" was also found to be too vague to enable individuals to regular their conduct accordingly.
- Sections 52-53: These provisions concern seditious speech or publications, described as those which inspire hatred, contempt or disaffection against government or the administration of justice, incite people to attempt to use unlawful means to alter any matter, raise discontent or disaffection between people or groups. or promote ill-will and hostility between different categories of the population. It is permissible to use speech or a publication to show that the Government has been misled or mistaken in any of its measures; or to point out errors or defects in government, in legislation or in the administration of justice with a view to remedying such errors or defects. The Court found that these provisions also failed the test of clarity and certainty.

- Sections 58-59: Section 58 allows the relevant minster to prohibit the import of any publication the minister considers to be "contrary to the public interest", while section 59 allows the minister to "prohibit or otherwise sanction the publication of any content that jeopardises national security or public safety". The Court found these powers too far-reaching and subjective to be a proportional limitation on freedom of expression.[1688]

In August 2021, three Tanzanian human rights organizations filed a lawsuit against the government at the **East African Court of Justice** in respect of the government's failure to amend the Media Services Act in the wake of the 2019 ruling.[1689] In 2023, Parliament passed some amendments to the Media Services Act, but these failed to address all of the issues identified by the East African Court of Justice.[1690] The provisions on criminal defamation and some other problematic content-based offences will be discussed below.

The **Films and Stage Plays Act, 1976,** governs, among other things, making and exhibiting films in Tanzania, both of which require permits from the relevant minister. The film permit application must include a full description of the scenes and the full script of the entire film. In terms of the **Films and Stage Plays Regulations, 2020** issued under this Act, the definition of a film is "the arrangement of images of objects recorded and linked to the sounds of words or music and stored in the device in a digital format, or in any format that the image can be moved and includes any images in the form of various film or video but does not include video developed in the context of journalism". The law empowers the minister to order that a public officer must be present at the making of the film, with authority to stop the filming of any scene which, in the opinion of the officer, is objectionable. Amendments to the law in 2019 require foreign content producers to submit all raw footage, information about where it was shot, and a final copy of the production to the Tanzania Film Board, and to sign a prescribed clearance form before leaving Tanzania.[1691] Amnesty International described this as a "dangerous step deeper into censorship",[1692] while one law firm said that the 2019 amendments will mean that "the film and stage plays industry will be coming under increasingly close scrutiny and regulatory oversight".[1693]

A number of local songs have been banned by the National Arts Council of Tanzania (known as *Baraza la Sanaa Tanzania* (BASATA) in Kiswahili) under the **National Arts**

[1688] *Media Council of Tanzania & 2 Others v Attorney General of the United Republic of Tanzania*, East African Court of Justice, Case No 2 of 2017, 28 March 2019; see the case summary by Global Freedom of Expression here.
[1689] "Tanzania ruling party newspaper Uhuru returns after two-week suspension", Commitee to Protect Journalists, 10 September 2021.
[1690] See The Written Laws (Miscellaneous Amendments) Act, 2023, published as a bill in January 2023; the version of the bill that was actually passed by Parliament could not be located online. See also "What media law changes mean", *The Citizen*, 14 June 2023. According to one source: "After a tireless discussion with the state actors, the Coalition on the Right to Information (CoRI) proposed about 35 changes desired in the Media Services Act of 2016 to increase media freedoms and individual freedoms. However, the amendment Bill that the Attorney General of the Government submitted to the parliament in 2023 has proposed changes to eight sections, leaving critical sections such as the ones that criminalise defamation." Francis Nyonzo, "Tanzania's Media Services Act: A Manifestation of the Man With the Hammer Syndrome?", The Chanzo Initiative, 27 March 2023.
[1691] The Films and Stage Plays Act 14 of 1976, as amended by the Local Government (District Authorities) Act 7 of 1982 (which amends section 9) and the Written Laws (Miscellaneous Amendments) (No 3) Act, 2019; see also "Corporate Commercial Law Update: The Tanzania Film Regulations of 2020; Implications to Businesses as far as Video Ads and Digital Content Regulation is Concerned in Tanzania", Breakthrough Attorneys, 21 March 2021.
[1692] "Tanzania: Discard new law restricting human rights", Amnesty International. 28 June 2019.
[1693] Francis Kamuzora, "Amendments to Copyright and Film Laws set the Scene for Change", Bowman's. 14 August 2019.

Council Act 23 of 1984, for being deemed to be against the country's norms and values, in violation of broadcasting services content regulations or unsuitable for public consumption.

The power to take such steps is not set out explicitly in the law but has been exercised under a provision of the law that gives BASATA discretionary power to do all such acts as appear to it to be requisite, advantageous or convenient in connection with the exercise of its functions.[1694]

B) ZANZIBAR

Note that the information in this subsection comes from secondary sources as the legislation discussed here could not be located online.

The **Registration of Newsagents, Newspapers and Books Act 5 of 1988** requires the registration of all newspapers in Zanzibar, with "newspaper" being defined as "any printed matter containing news, or intelligence, or reports of occurrences of interest to the public or any section thereof, or any views, comments or observations thereon, printed for sale or distribution and published in Tanzania periodically or in parts or numbers". This Act empowers the relevant minister to suspend the publication of a newspaper if this is in the public interest, in the minister's opinion. This law also prohibits any person who does not hold a written authorisation issued by the Director of Information Services from collecting or distributing any news or news material in Zanzibar. The registration of a journalist under this law can be suspended or revoked in the public interest.[1695]

In 2016, the **East African Court of Justice** considered the suspension of *Mseto*, a weekly Tanzanian newspaper, under the previous law on the registration of newspapers, the Newspaper Act, 1979. The newspaper was ordered to cease publication, including any electronic communication, for three years after it carried an article alleging that a government official had taken bribes to raise funds for the election campaign of President John Magufuli. The Court found that the suspension order violated the right to freedom of expression in Article 18(1) of the Constitution of Tanzania, Article 19(3) of the International Covenant on Civil and Political Rights and Article 27(2) of the African Charter on Human and People's Rights. It found that the Minster had acted unlawfully by issuing orders restricting the freedom of expression based merely on subjective opinion.[1696]

The **Zanzibar Arts and Censorship Council Act 7 of 2015** regulates the making of films in Zanzibar. It establishes the Zanzibar Arts and Censorship Council (BASSFU),

---

[1694] Leonard Chimanda, "Law and Censorship of Artistic Works in Tanzania: The Case of BASATA", Sanaa: Journal of African Arts, Media and Cultures, 3(1), 2018, pages 13-26. The underlying law, which could not be located online, was amended by the Written Laws (Miscellaneous Amendments) (No. 5) Act 2019.

[1695] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 97-101.

[1696] *Mseto v Attorney General*, East African Court of Justice, Case No 7 of 2016, 21 June 2018; see the case summary by Global Freedom of Expression here.

appointed by the relevant minister with the duty (amongst other things) to preserve, maintain and promote the values and norms of Zanzibar culture, to ensure that all films are censored before they are presented to the public and to "suspend any cinematographic exhibition, stage play and any other entertainment which is inconsistent with the righteous conduct of Zanzibar". No films may be exhibited or distributed without a permit.[1697]

Broadcasting in Zanzibar is regulated by the **Zanzibar Broadcasting Commission Act 7 of 1997**, which establishes a Zanzibar Broadcasting Commission made up of two members appointed by the President and additional members appointed by the relevant minister. The Commission issues broadcasting licences, regulates various broadcasting activities and protects "the policy, security, culture and tradition of Zanzibar". In addition to having a duty to present news and current affairs in an impartial and balanced manner, broadcasting licences must contribute to shared national consciousness, identity and continuity.[1698]

The Zanzibar Broadcasting Corporation (ZBC) is established as Zanzibar's national broadcaster by the **Zanzibar Broadcasting Corporation Act, 2013**, and operates under the direction of a Board with a chairperson appointed by the President and members appointed by the relevant minister.[1699]

16.2 CONSTITUTION

Article 18 of the **Constitution of the United Republic of Tanzania**, which applies to both Mainland Tanzania and Zanzibar, provides for freedom of speech but does not explicitly provide for freedom of expression for members of the press and other media.[1700]

The general limitations clause in Article 30 (quoted on the first page of this chapter) is problematic because it provides very wide grounds for limiting basic rights – including promoting the national interest and controlling the activities of private societies and organizations. There is no explicit requirement that limitations on rights must be proportional, justifiable, reasonable or the least restrictive means of achieving the aim in question.[1701]

It should be noted that as of mid-2023, a review process was underway that could lead to constitutional reforms.[1702]

[1697] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 101-102. The Bill is available here.
[1698] Id, pages 102-110,113.
[1699] Id, pages 110-113.
[1700] Article 18 is quoted in the table on the first page of this chapter.
[1701] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, page 7.
[1702] "The constitutional reform as a reason for optimism about the future of democracy in Tanzania", Robert Lansing Institute, 17 May 2023. According to this article, President Samia Suluhu Hassan appointed a task team in 2022 to review the political situation in the country, and this task team a revival of the constitution-writing process that had stalled in 2014-2015. A round of public consultations held by the task team on this issue was concluded in September 2022.

Article 18 of the **1984 Zanzibar Constitution** also protects freedom of expression:

> *18. (1) Without prejudice to the relevant laws of the land, every person has the right to freedom of opinion and expression, and to seek, receive and impart or disseminate information and ideas through any media regardless of national frontiers and also has the right of freedom from interference with his communications.*
> *(2) Every citizen has the right to be informed at all times of various events in the country and in the world at large which are of importance to the lives and activities of the people and also of issues of importance to society.* [1703]

In terms of Article 24, these rights can be limited by law if that limitation is "necessary and agreeable in the democratic system". The "foundation" of the right in question may not be limited, and the limitations may not bring about more harm to society than is already present.[1704] Again, these are broad criteria for the limitation of rights, with no explicit requirements that the limitations must be proportional, justifiable, reasonable or the least restrictive means of achieving the aim in question.[1705]

No seminal court cases applying the constitutional rights to freedom of expression were located.

16.3 CASE STUDIES

Tanzania experienced a sharp decline in press freedom during the rule of late president John Magufuli, who died in March 2021. There were hopes for change under the succeeding rule of Samia Suluhu Hassan, the country's first female president.[1706] In June 2022, the Committee to Protect Journalists reported that there were indications that the new government was taking a friendlier stance towards the press, with newspaper and online television bans having been lifted and reviews of problematic laws announced. However, at the same time, this group noted that the "old habits of media shutdowns and arbitrary arrests have not been fully abandoned" and worried that the new administration has not yet fully embraced "a vision of press freedom in which journalists can independently report, including on uncomfortable topics or from a dissenting position".[1707]

[1703] The Constitution of Zanzibar, 1984 [Revised Edition 2006], Article 18.
[1704] Id, Article 24.
[1705] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, page 82.
[1706] Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 49.
[1707] "CPJ returns to Tanzania", *CPJ Insider: June 2022 edition*, 2 June 2022.

In 2022, the US State Department reported significant human rights concerns that included credible reports of "serious restrictions on free expression and media, including unjustified arrests or prosecutions of journalists, censorship, and enforcement of criminal libel laws" and "serious restrictions on internet freedom". Its report noted that the rights of free expression were limited through both formal legislative and regulatory measures and informal actions by government and police.

The report cited as particular problems laws that give the government the authority to shut down media outlets and the use of criminal penalties for libel to stifle freedom of expression.[1708]

In some positive news in 2022, it was reported that a five-year suspension of the newspaper *Mawio* was lifted. The newspaper had been suspended in 2017 for "jeopardizing national security" by reporting on two former presidents' alleged links to mining misconduct. The licences of newspapers *MwanaHALISI, Mseto* and *Tanzania Daima* were also restored in 2022, after they had been banned or suspended from publishing online and in print under former President Magufuli.[1709]

More problematically, in February 2022, police and wildlife officers detained six journalists (from *Mwananchi Digital*, *Nipashe*, *Wasafi TV*, *Daily News Digital*, and *Start TV*) in the Ngorongoro Conservation Area who were covering a village meeting regarding the ongoing land dispute between pastoralist residents and law enforcement officials. They were allegedly arrested for **failing to follow proper media procedures** but were released from custody a few hours later.[1710]

In January 2022, police **arrested** journalists in Loliondo for attempting to cover an ongoing land dispute between Maasai pastoralists and authorities. In June 2022, when tensions re-emerged in the area, independent media did not report on the situation due to fear of government reprisals. Journalists were also regularly prohibited from accessing the area for media coverage. In July 2022, the TCRA **temporarily suspended the online media outlet *DarMpya***, following complaints about content relating to demonstrations on the same issue outside of the Kenyan Embassy in Dar es Salaam, and Kenyan journalist Julius Kuyioni was **arrested on a charge of illegal entry into Tanzania,** apparently also as part of authorities' attempts to stop journalists covering the community protests in Loliondo.[1711]

[1708] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, "Executive Summary" and section 2A.
[1709] Muthoki Mumo, "'A rush of relief': Tanzanian investigative newspaper allowed to publish after 5-year ban". Committee to Protect Journalists, 21 March 2022.
[1710] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
[1711] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A; "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023; "Tanzanian regulator suspends DarMpya online news outlet, citing expired license", Committee to Protect Journalists, 12 July 2022.

In September 2022, the TCRA Content Committee fined *Zama Mpya TV* (a rebranding of *DarMpya* after its previous difficulties) for allegedly publishing inflammatory and unsubstantiated content regarding the government's introduction of fees on electronic banking. The Committee accused the media outlet of **endangering the peace, unity, and safety of the country** and placed it under TCRA supervision and monitoring for three months.[1712]

In June 2022, during an interview with a local media outlet, politician Baraka Shamte made comments critical of Zanzibar President Hussein Mwinyi, suggesting he was not a good leader and did not deserve a second term. Shamte was arrested on a charge of **sedition** for allegedly making statements demeaning to government officials. He was released on bail but kidnapped and beaten by unknown assailants the next day.[1713]
In August 2021, Tanzania's Information Services Department suspended the ruling party-owned *Uhuru Newspaper* for 14 days in response to allegations that it had published a false and seditious report about President Samia Suluhu Hassan. The report in question stated that she did not intend to run for office in the next general election in 2025. The suspension was based on **sections 50(1)(a),(b),(d) and 52(d) of the Media Services Act, 2016 concerning publication of false, falsified or fabricated information raising discontent or disaffection amongst the people of Tanzania**. The ruling party distanced itself from the article, saying that it was false and that three senior managers at *Uhuru* had been suspended pending an investigation.[1714]

In September 2021, Tanzania's Information Services Department suspended publication of the *Raia Mwema* newspaper for a month, citing several articles they had published relating to government figures or policies. The **suspension was made under section 52 of the Media Services Act, 2018 relating to seditious intent, along with section 54 relating to the publication of false statements or rumours likely to cause public disturbance**.[1715]

Also in September 2021, cartoonist Opptertus John Fwema, was **arrested** days after publishing on his Instagram page a political cartoon that was critical of President Samia Suluhu Hassan. Police apparently stated that Fwema was under investigation for **cybercrime offences**.[1716]

In July 2021, journalist Ephraim Bahemu of *The Citizen* newspaper was **arrested and questioned** by police in Dar es Salaam **under the authority of the Cybercrimes Act 4 of 2015** in connection with an article on new mobile phone levies introduced by the government.[1717]

[1712] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
[1713] Id.
[1714] "LEXOTA Country Analysis: Tanzania", last updated December 2022; "Tanzania ruling party newspaper Uhuru returns after two-week suspension", Committee to Protect Journalists, 10 September 2021.
[1715] "LEXOTA Country Analysis: Tanzania", last updated December 2022; "Tanzanian authorities suspend Raia Mwema newspaper for 1 month", Committee to Protect Journalists, 15 September 2021.
[1716] "Tanzania police arrest cartoonist, journalists on cybercrime and illegal assembly allegations", Committee to Protect Journalists, 7 October 2021.
[1717] "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 10.

In September 2021, independent cartoonist Opptertus John Fwema was arrested by police in Dar es Salaam because of a political cartoon that he posted on Instagram.[1718]

Between January and April 2020, at least 13 media workers, including seven journalists and bloggers, were arrested and prosecuted for allegedly contravening the **Electronic and Postal Communications (Online Content) Regulations, 2018**. It was reported that the charges included failure to register websites and YouTube channels at the TCRA.[1719]

In April 2020, the *Mwananchi* newspaper was banned from publishing online for six months and fined five million Tanzanian shillings after it circulated an online video showing then-President John Magufuli buying fish in an open market during the Covid-19 pandemic. The newspaper was charged with **publication of false news in violation of regulation 12(I) of the Electronic and Postal Communications (Online Content) Regulations, 2018**. These regulations have since been replaced by the Electronic and Postal Communications (Online Content) Regulations, 2020, which contain a similar prohibition against "prohibited content" in regulation 16.[1720]

In June 2020, the government **revoked the licence** of the Swahili daily tabloid, *Tanzania Daima*, citing alleged repeated violations of national laws and journalism ethics.[1721]

In July 2020, the TCRA **suspended the licence** of *Kwanza Online TV* for 11 months for **generating and disseminating biased, misleading and disruptive content in violation of regulation 12(1) of the Electronic and Postal Communications (Online Content) Regulations, 2018** (now replaced by regulation 16 of the Electronic and Postal Communications (Online Content) Regulations, 2020. This action was a response to the news outlet's sharing on Instagram of a US embassy health alert about the government's failure to publish any Covid-19 figures, which TCRA claimed to be aimed at causing panic and damaging the national economy. This suspension followed on a previous six-month suspension of *Kwanza Online TV's* operations in September 2019, also for allegedly publishing misleading information.[1722]

[1718] Id, pages 10-11.
[1719] Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 48.
[1720] "LEXOTA Country Analysis: Tanzania", last updated December 2022.
[1721] Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 48.
[1722] "LEXOTA Country Analysis: Tanzania", last updated December 2022.

Tanzanian comedian, Idris Sultan was arrested twice during the reign of the late President John Magufuli. He was first arrested in October 2019 and charged with **impersonating the president** for posting what was been described as "a face-swap picture" of Magufuli on Twitter. He was arrested again in May 2020, after he posted a video of himself laughing at a picture of Magufuli in an oversized suit. On that occasion. he was charged with **using a SIM card that was not registered in his name**.[1723]

In 2019, an investigative journalist at *Watetezi TV*, Joseph Gandye, was arrested for **disseminating false information in violation of section 16 of the Cybercrimes Act, 2015**. The journalist had reported on police brutality against young people in police custody and alleged that police officers had forced six young people in custody to "sodomize each other". He was reportedly released several days later, and it was unclear whether charges were being pressed.[1724]
Also in 2019, Sebastian Atilio was arrested for allegedly spreading false news on a WhatsApp group known for commentary on politics and social issues. The information he published related to a claim that villagers in the Iringa region were potentially facing eviction and relocation to make way for the Unilever Tea Tanzania Company Limited. Atilio was charged with **publishing false information contrary to section 16 of the Cyber Crimes Act, 2015**, and for **performing journalist activities without a permit from the Tanzania Journalists Board contrary to section 50(2)(b) of the Media Services Act, 2016**. He was held for nearly three weeks before being released on bail. The charges were withdrawn about five months after the arrest.[1725]
There are reports that government has restricted **access to the internet** and **monitored websites and internet traffic**.[1726]

16.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) CYBERCRIMES ACT, 2015

Tanzania's **Cybercrimes Act, 2015** has been described as a close copy of the SADC Model Law, including aspects of that law which have been criticised as being problematic.[1727] Tanzania's law was met with sharp criticism from stakeholders who worried that it would be applied by government to muzzle the right to online freedom of expression. Indeed, it has been applied repeatedly against social media users and bloggers who have expressed criticism of government figures.[1728] One analysis commented: "Ever since it was passed, the Act has been (ab)used by the

[1723] *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page Misa state of press freedom 2020-2020, page 9.
[1724] "LEXOTA Country Analysis: Tanzania", last updated December 2022.
[1725] Id.
[1726] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
[1727] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 33.
[1728] "Freedom of expression in Tanzania is on a downward spiral", Global Voices, 6 December 2022; "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 30.

government to arrest citizens that used online media to express criticism of President Magufuli. In this regard, the Cybercrime Act is perceived more as a tool to oppress the freedom of expression and the closely related right to privacy".[1729] Another commented that the "overall heavy-handedness of the law has led to it being described as an 'anathema to democracy and free speech'".[1730]

For every offence in the Act, both technical and content-based, the Act provides ***minimum*** fines and prison sentences. This is particularly worrying in respect of some of the vaguely defined offences.

There are also enhanced minimum penalties when an offence under the Cybercrimes Act or any other written law is committed in relation to **critical information infrastructure** – which includes "assets, devices, computer system, or networks, whether physical or virtual so vital to the United Republic of Tanzania that their incapacitation affect national security or the economy and social wellbeing of citizens". The relevant minister "may" designate a computer system as a "critical information infrastructure" by notice in the *Gazette*.[1731] In the absence of such a notice, it could be difficult for persons affected by the laws to know when the enhanced penalties would apply.

The law also provides for the forfeiture of property associated with an offence, and for the payment of compensation to the victim of the offence by the convicted offender.[1732]

CYBERCRIMES ACT, 2015 - TECHNICAL OFFENCES	
Section 4: Illegal access	It is an offence to intentionally and unlawfully access a computer system or cause a computer system to be accessed. o "Access" in relation to a computer system is defined in section 3 as "entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium". This wording is somewhat ambiguous as to whether it criminalises entry on its own, or only entry to do one of the other listed acts (instruct, communicate with, store data, etc). This should be clarified.[1733]
Section 5: Illegal remaining	It is an offence to intentionally and unlawfully, remain in a computer system or continue to use a computer system after the expiration of time which was authorised.

[1729] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 29.
[1730] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 33.
[1731] The Cybercrimes Act 14 of 2015, sections 28-29.
[1732] Id, section 48.
[1733] One commentator reads it in the broad sense as criminalising initial entering of a computer system, as well as conduct done after access is gained. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 14.

	○ It has been asserted that "illegal-remaining" offences are unnecessary because they are covered by the offence of unauthorised access.[1734]
Section 6: illegal interception	It is an offence to intentionally and unlawfully intercept by technical or any other means a non-public transmission to, from or within a computer system, a non-public electromagnetic emission from a computer system or a non-public computer system that is connected to another computer system. It is also an offence to intentionally and unlawfully circumvent the protection measures implemented to prevent access to the content of non-public transmission. ○ Section 3 defines "interception" in relation to a function of a computer to include "acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device". ○ This offence "captures the essence of interception as envisioned in the Budapest Convention". [1735] ○ One commentator points out it was unneccesary to refer to interception of a non-public computer system that is connected to another computer system, as this was already covered by the types of interception listed.[1736]
Section 7: Illegal data interference	It is an offence to intentionally and unlawfully - • damage or deteriorate computer data; • delete computer data; • alter computer data; • render computer data meaningless, useless or ineffective; • obstruct, interrupt or interfere with the lawful use of computer data; • obstruct, interrupt or interfere with any person in the lawful use of computer data; or • deny access to computer data to any person authorized to access it. It is an offence to communicate, disclose or transmit any computer data, program, access code or command to an unauthorized person, or to internationally and unlawfully receive unauthorised computer data. It is an offence to intentionally and unlawfully destroy or alter any computer data, where such data is required to be maintained by law or is evidence in any proceeding under this Act by - • mutilating, removing or modifying the data, program or any other form of information existing within or outside a computer system; • activating, installing or downloading a program that is designed to mutilate, remove or modify data, program or any other form of information existing within or outside a computer system; or • creating, altering, or destroying a password, personal identification number, code or method used to access a computer system/

[1734] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
[1735] Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 16.
[1736] Id.

	○ The offence of receiving unauthorised computer data could affect media access to data acquired by a whistleblower or placed in a cache such as Wikileaks.
Section 8: Data espionage	Without prejudice to the National Security Act, it is an offence to obtain computer data protected against unauthorized access without permission. ○ This offence appears to overlap with the aspect of section 7 that covers unlawfully receiving unauthorised computer data. As in that case, this offence could be applied to data that has been shared after being obtained by whistleblowers.
Section 9: Illegal system interference	It is an offence to intentionally and unlawfully hinder or interfere with the functioning of a computer system or the usage or operation of a computer system. ○ Section 3 defines "hinder" in relation to a computer system to include causing electromagnetic interference, corrupting the computer system by any means, or by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Section 10: Illegal device	It is an offence to unlawfully deal with or possess - • a device, including a computer program, that is designed or adapted for the purpose of committing an offence; • a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed with the intent that it be used by any person for the purpose of committing an offence. ○ "Device" is defined in section 3 as including a computer program, code, software or application; a component of computer system such as a graphic card, memory card, chip or processor; a computer storage component; or input and output devices. ○ It has been noted that the first part of this provision risks over-criminalisation, since the targeted conduct consists of dealing with or possessing a device that is designed or adapted to commit an offence and could thus include dual-use devices (meaning devices that are capable of being used for both lawful and unlawful purposes). There is also no requirement that the person must act without lawful excuse or justification, meaning that dealing with or possessing the device is an offence even if there was not malicious motive." It should have been made clear in the definition that the person must deal with or possess the device without lawful excuse or justification, and that the device itself must be primarily designed or adapted to commit an offence."[1737] ○ The second part of this provision is narrower because it expressly requires an intent that the item (password, access code, etc) will be used for the purpose of committing an offence.[1738]
Section 11: Computer-related forgery	It is an offence to intentionally and unlawfully input, alter, delay transmission or delete computer data, resulting in unauthentic data, with the intent that it be acted upon as if it were authentic, regardless of whether or not the data is readable or intelligible.

[1737] Id, page 21.
[1738] Id.

	○ The required intent helps to ensure that this offence is properly targeted.
Section 12: Computer-related fraud	It is an offence to cause a loss of property to another person, with fraudulent or dishonest intent, by - • any input, alteration, deletion, delaying transmission or suppression of computer data; or • any interference with the functioning of a computer system. ○ "Property" is defined in section 3 to include tangible and intangible property, including money and information. ○ The required intent helps to ensure that this offence is properly targeted.

As in most of the other countries examined, it is the content-based offences that are so far being used to stifle free expression.

CYBERCRIMES ACT, 2015 - CONTENT-BASED OFFENCES	
Section 13: Child pornography	It is illegal to publish child pornography, through a computer system, or to make available or facilitate the access of child pornography through a computer system. ○ "Child pornography" is defined in section 3 to mean "pornographic material that depicts presents or represents: * a child engaged in sexually explicit conduct; * a person appearing to be a child engaged in sexually explicit conduct; or * an image representing a child engaged in sexually explicit conduct. ○ "Child" means a person below the age of 18. ○ "Pornographic material" is not defined nor "sexually explicit conduct". The lack of clear definition could be problematic in practice. ○ "Publish" is defined in section 3 as "distributing, transmitting, disseminating, circulating, delivering, exhibit[ing], exchanging, barter[ing], printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way". ○ There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose. ○ Because publishing includes "transmitting", this offence would appear to capture "sexting" between children of similar ages, even where the material is shared only between the two of them.
Section 14: Pornography	It is an offence to publish pornography or cause pornography to be published through a computer system or through any other information and communication technology. There is an enhanced penalty where the pornography is lascivious or obscene. ○ "Publish" is defined in section 3 as "distributing, transmitting, disseminating, circulating, delivering, exhibit[ing], exchanging, barter[ing], printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way". Because publishing includes "transmitting", this offence

	would appear to capture even private sharing of material between consenting adults. o None of the other key terms in this offence are defined ("pornography", "lascivious" or "obscene"). which is likely to make enforcement very subjective. o There is no defence for materials with a genuine artistic, educational, legal, medical, scientific or public benefit purpose. o This is one of the few cybercrime laws in the SADC region that widely captures pornography that does not involve children. (There is also a broad provision on pornography in the chapter on cybercriminality in the Comorian Penal Code.)
Section 15: Identity related crimes	It is an offence to use a computer system to impersonate another person. o This offence makes no reference to intention and so could inhibit some instances of investigative journalism. o MISA-Tanzania points out that the existing phrasing could capture acceptable forms of communication, such as political satire in which an actor impersonates a public official.[1739] o MISA-Tanzania suggests that any crime linked to identity must have been done with malice aforethought, and the intent to inflict substantial injury as a result. It also suggests the addition of defences based on acting in the public interest.[1740]
Section 16: Publication of false information	Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or councelling [sic] commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both. o As one analysis notes, it is not clear how to determine whether information is "false" or "misleading". Section 16 therefore does not provide sufficient guidance and gives an overly wide degree of discretion to those who enforce this law. Section 16 also goes beyond legitimate aims by restricting speech which is intended to mislead or deceive without causing any other harm. The minimum penalties are likely to be disproportionate, particularly for less serious offences where little or no harm actually occurs.[1741] o The fact that the intent required can be merely an intent to "insult" means that this factor does not narrow the offence sufficiently. o MISA-Tanzania asserts that this provision could put online media outlets in "an unreasonable amount of danger", and reports that there have been thousands of reports of alleged violations of this provision.[1742]

[1739] "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 23.
[1740] Id.
[1741] "LEXOTA Country Analysis: Tanzania", last updated December 2022.
[1742] "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, pages 23-24.

	○ The US State Department's 2022 report on Human Rights Practices in Tanzania cites this provision as one of concern, stating: "While the number of arrests of individuals who made critical comments on electronic media regarding the government diminished under President Samia Suluhu Hassan, individuals were still publicly threatened for publishing critical remarks or opinions, even if they were factually true."[1743] ○ As an example of the application of this provision, five persons were reportedly charged (in separate incidents) with insulting the late President John Magufuli on social media in 2016, while four persons were reportedly charged in 2021 with spreading false reports on social media claiming that President John Magufuli was seriously ill.[1744]
Section 17: Racist and xenophobic material	It is an offence, through a computer system, to produce racist or xenophobic material for the purposes of distribution, to offer or make available such material, or to distribute or transmit such material. ○ "Racist or xenophobic material is defined in section 3 as "any material which advocates, promotes or incites hatred, discrimination or violence, against any person or group of persons based on race, colour, descent, national or ethnic origin or religion". ○ Note that this offence, unlike some other versions in the region, does not require that material based on religion is actionable only if religion is used as a pretext for one of the other grounds.
Section 18: Racist and xenophobic motivated insult	It is an offence to insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion. ○ There is no definition or qualification of the term "insult". ○ Although this provision is based on the Malabo Convention, criminalising "insult" seems extremely vague and overbroad. ○ Note that there is no requirement of an intention to insult another person, meaning that it could be possible for the crime to be inadvertently committed (based on a statement intentionally made, but made without the aim of insulting another). ○ Such a broad offence could easily lead to subjective enforcement, which is particularly worrying given the minimum sentence of a three million shilling fine or one year's imprisonment or both.
Section 19: Genocide and crimes against humanity	It is an offence to unlawfully publish or cause to be published, through a computer system, material which incites, denies, minimises or justifies acts constituting genocide or crimes against humanity. For the purpose of this section, "genocide" has the meaning ascribed to it under the Convention on the Prevention and Punishment of the Crime of Genocide, 1948. ○ There is no definition of "crimes against humanity". ○ "Publish" is defined in section 3 as "distributing, transmitting, disseminating, circulating, delivering, exhibit[ing], exchanging, barter[ing], printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way". Because publishing includes "transmitting", this offence

[1743] "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
[1744] "Freedom of expression in Tanzania is on a downward spiral", Global Voices, 6 December 2022.

	would appear to capture even a private message from one individual to another denying or minimising genocide or crimes against humanity if sent through a computer system. Communication with even a single individual *inciting* genocide or crimes against humanity is clearly justifiable, but merely expressing an opinion about historical events in a private communication raises harder questions about privacy and freedom of expression. The Malabo Convention does not specify whether or not the communication must be public; it merely calls on States to make it a criminal offence to "deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system".
Section 20: Unsolicited messages	It is an offence to do any of the following acts "with intent to commit an offence under this Act" - • initiate the transmission of unsolicited messages. • relay or retransmit unsolicited messages, or • falsify header information in unsolicited messages. o The required intent to commit another offence under the Act narrows this offence considerably.
Section 23: Cyber bullying	A person shall not initiate or send any electronic communication using a computer system to another person with intent to coerce, intimidate, harass or cause emotional distress. o This is a very broadly defined offence. There is no further detail about the meaning of "intimidate", "harass" or "cause emotional distress". It also appears that the offence could be committed by a single communication. o This vague provision could lead to selective enforcement, which is particularly worrying given the minimum penalties of a five million shilling fine or three years' imprisonment or both.
Section 24: Violation of intellectual property rights.	It is an offence to use a computer system with intent to violate intellectual property rights protected under any written law. There are different minimum penalties, depending on whether the offence is committed on a commercial or a non-commercial basis. o "Intellectual property rights" are defined in section 3 to mean "the rights accrued or related to copyright, patent, trademark and any other related matters". o The requirement that there must be an intent to violate intellectual property rights helps to prevent innocent persons from being prosecuted.

In general, **attempting, abetting or conspiring to commit any offence under the Act** – whether technical or content based – is also an offence.[1745]

In respect of investigations, the law authorises the police officer in charge of a police station or a law enforcement officer of a similar rank to issue an order for **search and seizure** in respect of a computer system, with no judicial involvement.[1746]

The same procedure applies to an order compelling a person to disclose data relevant to the investigation of an offence. Disclosure of data includes obtaining **subscriber information** from service providers.[1747]

The police officer in charge of a police station or a law enforcement officer of a similar rank can issue an **expedited preservation order** that is valid for up to 14 days, and a court may extend the order for "such period as the court may deem necessary". [1748]

The same law enforcement officials may issue an order requiring the disclosure, collection or recording of **traffic data** associated with a specified communication during a specified period, or an order to collect or record **content data** associated with specified communications, including through the use of technical means. [1749]

Court involvement is required only where the data disclosure or preservation cannot be done without the **use of force** due to resistance,[1750] or where law enforcement officers want to use a "**forensic tool**" for evidence collection (which can be authorised by a court for 14 days at a time).[1751]

The Act includes procedures for a **take-down notification**. A person can provide a notification to a service provider that there is data or activity that infringes the rights of the complainant or a third party, or that there is some unlawful material or activity online. It is a criminal offence for a person to lodge a take-down notification with a service provider knowing that it materially misrepresents the facts. If the service provider fails to act upon the notification, the complainant may request a competent authority to take appropriate action.[1752]

A service provider that does not take action on a take-down notification becomes liable for the material in question as if they had initiated the content.[1753] However, the protection against liability for hosting, caching or providing a hyperlink to content appears to work a bit differently. A hosting provider is not liable for information stored at the request of a user of the service if that provider immediately removes or disables

[1745] The Cybercrimes Act 14 of 2015, sections 25-27. Section 2 defines "abetting" as "to encourage or assist someone to commit a crime or other offence".
[1746] Id, section 31.
[1747] Id, section 32.
[1748] Id, section 33.
[1749] Id, section 34-35.
[1750] Id, section 38.
[1751] Id, section 39. A "forensic tool" is defined in section 3 as "forensic tool" means "an investigative tool or device including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks which includes keystroke logging or collection of investigation information about a use of a computer or computer system".
[1752] Id, section 45.
[1753] Id, section 45(4).

access to the information *after receiving an order to do so from any competent authority or court*, and also immediately informs the relevant authority upon becoming aware of illegal information.[1754] The duties of the hyperlink provider are similar.[1755] A caching provider can avoid liability by acting immediately to remove or to disable access to stored information upon obtaining actual knowledge that access to the information has been removed or disabled at the initial source of the transmission, or that a court or the relevant authority has ordered removal or disablement.[1756]

The concerns identified by an analysis of the take-down notification procedure under the Electronic and Postal Communications (Online Content) Regulations, 2020 are also applicable here.[1757]

B) ELECTRONIC AND POSTAL COMMUNICATION ACT, 2010

Section 118 of the Electronic and Postal Communications Act makes it an offence to use network facilities, network services, applications services or content services to knowingly make, create, solicit or initiate the transmission of any comment, request, suggestion or other communication which is "**obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person**". It is also an offence to use any applications service **to initiate a communication "with intent to annoy, abuse, threaten or harass any person at any number or electronic address**". This applies whether the communication is continuous, repeated or otherwise, and regardless of whether actual communication ensues. It also applies regardless of whether the person initiating the communication discloses his or her identity. In addition. it is an offence to use any network services or applications service to provide an **obscene communication** to any person.[1758]

As with many of the content-based offences in the Cybercrime Act, these provisions are very broad in scope, leaving an overly wide degree of discretion to those charged with the enforcement of this law.[1759]

C) ELECTRONIC AND POSTAL COMMUNICATIONS (ONLINE CONTENT) REGULATIONS, 2020

The **Electronic and Postal Communications (Online Content) Regulations, 2020**[1760] were made in terms of section 103 of the Electronic and Postal Communication Act, 2010, which sets a number of parameters for such regulations.[1761] The 2020 regulations

[1754] Id, section 41.
[1755] Id, section 43.
[1756] Id, section 42.
[1757] Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 4 and pages 12-13, discussed below.
[1758] The Electronic and Postal Communications Act [Chapter 306 R E. 2022], section 118(a)-(c).
[1759] See "LEXOTA Country Analysis: Tanzania", last updated December 2022.
[1760] Electronic and Postal Communications (Online Content) Regulations, 2020.
[1761] The Electronic and Postal Communications Act [Chapter 306 R E. 2022], sections 103-ff.

replaced a 2018 set of regulations with the same title. The current regulations were amended in 2022.[1762]

These regulations apply to both online content service providers (which covers internet content broadcasting to the public through television, radio, blog, weblog, instant messaging tools, social media and other apps) and online content users, as well as others. The regulations define "content" as information in the form of "speech or other sound, data, text or images whether still or moving except where transmitted in private communications". [1763]

The regulations as amended make it an offence to provide "online media services" without a licence, with this being defined as "online content services provided for the purpose of news and current affairs in a manner similar to, or in a manner that resembles service providers licensed under the Act.[1764] The licencing requirement has been referred to as "tactical censorship" which may be used to constrain press freedom. It has also been suggested that it violates Article 18 of the Constitution as an unreasonable restriction of individuals' right to seek, receive and impart information regardless of national frontiers – given that the Internet is a key mechanism for realising that right.[1765] The organization "Article 19" makes the following point about licencing online content:

> *The UN Human Rights Committee has underlined that regulatory systems should take into account the differences between the print and broadcast sectors and the internet. Broadcast media rely on a limited resource: the electromagnetic spectrum. Different users (radio and TV stations, mobile phone services, radar etc.) compete for scarce frequencies, and the State must establish a system to allocate them, or the result would be chaos on the airwaves. No such necessity exists with regard to print and online media; the number of such publications that can exist alongside each other is technically unlimited. Nor can concerns about content justify the imposition of a licence requirement.*[1766]

The regulations also forbid the online publication of any "prohibited content", which is described in a long list set out in the Third Schedule to the regulations.[1767] This entire list is reproduced below because the breadth of the prohibited topics is truly shocking. The publication of any prohibited content is an offence punishable by a minimum fine of five million shillings or 12 months' imprisonment or both. If a licensee has published prohibited content, the Content Committee may issue a warning, require an apology

---

[1762] Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022.
[1763] Electronic and Postal Communications (Online Content) Regulations, 2020, as amended by the Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, regulation 2 read with the definition of "online content service providers" and "content" in regulation 3.
[1764] Id, as amended by the Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, regulation 4 read with the definition of "online media services" in regulation 3.
[1765] Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, pages 3 and 6.
[1766] "The Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2021: Submission to the Tanzania Ministry of Information, Culture and Sports", Article 19, section B(ii) (footnote omitted).
[1767] Id, section 16(1).

to the public and the individual victim (if any), order the removal of the offending content or impose a fine.[1768]

PROHIBITED CONTENT

Any of the following shall be considered as prohibited content for purposes of these Regulations:

1. SEXUALITY AND DECENCY

(a) content that motivates, promotes or facilitates publishing or exchanging child pornography, actual pornography, explicit sex acts, nudity and vice, save for related scenes approved by the body responsible for film classification and certification;
(b) content that depicts, motivates, promotes or facilitates publishing or exchanging of homosexuality, adultery, prostitution, sex crimes, rape or attempted rape and statutory rape, or bestiality;
(c) content that motivates, supports or promotes practices or trading of sexual or immoral goods such as movies, photos, drawings, books, stories, sexual games, toys and related things.

2. PERSONAL PRIVACY AND RESPECT TO HUMAN DIGNITY

(a) content that impersonates or claims status of others for fraudulent purposes;
(b) content that insults, slanders and defames other persons, or exposes news, photos or comments related to a person's privacy, or publication of private information regardless of whether the information is true where publishing the same may harm the person;
(c) content that motivates or promotes phone tapping, espionage, data theft, tracking, recording or intercepting communications or conversation without right; and
(d) content that promotes, motivates or encourages practices of witchcraft, enchantment, or sorcery.

3. PUBLIC SECURITY, VIOLENCE AND NATIONAL SAFETY

(a) content against the State and public order including content that aims to or publishes information, news, statements or rumours for the purpose of ridicule, abuse or harming the reputation, prestige or status of the United Republic, the flag of the United Republic, the national anthem or the United Republic's symbol, national anthem or its logos;
(b) content that calls for or motivates, promotes or provokes noncompliance to the laws and regulations;
(c) content that is involved in planning, organizing, promoting or calling for demonstrations, marches or the like which may lead to public disorder;

[1768] Id, regulation 21.

(d) content that would threaten the security of the United Republic or affect public order;
(e) content that includes news of official confidential communications or military affairs;
(f) content that would harm the national currency or lead to confusion about the economic condition in the country;
(g) content that incites, encourages or enables the commission of a crime against the United Republic or its citizens;
(h) content that is likely to threaten the stability of the United Republic or its safety, unity or security, or harming national unity or social peace;
(i) content that portrays violence, whether physical, verbal or psychological, that can upset, alarm and offend viewers and cause undue fear among the audience or encourage imitation;
(j) content that portrays sadistic practices and torture, explicit and excessive imageries of injury and aggression, and of blood or scenes of executions or of people clearly being killed;
(k) content that causes annoyance, threatens harm or evil, encourages or incites crime or leads to public disorder or that may threaten national security or public health and safety;
(l) content which advocates hate propaganda or promotes genocide or hatred against an identifiable group;
(m) content that promotes or favours what would raise sedition, hatred or racism or sectarianism or harming national unity or social peace or disturb the public order or public morals.

4. CRIMINAL ACTIVITIES AND ILLEGAL TRADE ACTIVITIES

(a) content that motivates, promotes or facilitates illicit drugs, criminal acts and skills including content that calls for, promotes or provides information about how to carry out acts of crime or felony or contributes to or facilitates carrying out or supporting the same such as theft, fraud, robbery, forgery, faking, bribery, killing, suicide, blackmail, threat, rape, commercial cheating and breaching the properties of others, abduction, evasion from application of law, money laundering, smuggling prohibited content and other crimes punishable by the law;
(b) content that promotes or contributes to trading with drugs and mind affecting substances and the manner of using or manufacturing the same or obtaining drugs or facilitating their circulation in circumstances that are not legally authorized;
(c) content that motivates, promotes or facilitates trading in prohibited or restricted goods, commodities or services in the United Republic, including illicit drugs, prostitution, or goods that require licence from the competent authorities and are being promoted or circulated without authorization from the competent authorities;
(d) content that promotes gambling and similar activities such as bets and lottery and those related to electronic gambling activities;
(e) content that motivates, promotes or facilitates terrorist groups or any illegal group, association, organization or body;

(f) content that publishes methods of making fire or explosive devices or any other tools used in terrorist acts.

5. HEALTHY [SIC] AND PUBLIC SAFETY

(a) content of health establishments, medical and pharmaceutical practices in violation of the laws;
(b) content that includes health advertisements in violation of Cabinet resolutions concerning health advertisements;
(c) content that is used in promoting or trading pharmaceuticals that are issued against prescription and to provide the same without asking for the medical prescription;
(d) content that promotes medicine and medical products that are prohibited or unlicensed including dietary supplements, weight loss products, weight increase and unlicensed cosmetic pills and creams.

6. PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

(a) content that infringes the rights of intellectual property such as providing and publishing movies, photos, drawings, books, electronic programs and games, encrypted TV and radio channels and other intellectual property rights without permission from right owner;
(b) content that provides information, tools and methods aiming to infringing [sic] intellectual property rights and penetrating the protection means used for protecting such rights such as decoding movies and coded TV channels and operation of copied magnetic diskettes and copied electronic programs and games and deactivation of protection systems designed exclusively for combating piracy.

7. RESPECT TO RELIGION AND PERSONAL BELIEFS

(a) content which contains or promotes offending, defaming, insulting, ridiculing or violating any of the religions or any of its rites, sanctities or divine books, or interfering with freedom to practice one's religion by violence or threat;
(b) content that motivates, promotes or facilitates incitement, or ridicule, hatred against a certain religious belief or expression that motivates, promotes or facilitates religious subjugation or apostasy;
(c) content that would make any form of discrimination and provoke hate speech or inciting [sic] tribal or religious prejudices with intent to incite hatred between individuals and groups;
(d) content that exploits religion to disbelief individuals or groups by using one of the methods of expression or using any of the means in order to achieve special interests or illegal purposes.

8. PUBLIC INFORMATION THAT MAY CAUSE PUBLIC HAVOC AND DISORDER

(a) content that promotes, advocates, encourages, or makes available instructions and guidance on illegal activities such as bomb-making, illegal drug production or counterfeit products;

(b) circulating or making available information with regards [to] possible terrorist attacks, droughts, weather forecasts or occurrence of natural calamities without the approval of the respective authorities;
(c) content with information with regards to the outbreak of a deadly or contagious diseases in the country or elsewhere without the approval of the respective authorities;
(d) circulating or making available information with regards to promotion of medical drugs and general medical products not approved by respective authorities.

9. USE OF BAD LANGUAGES AND DISPARAGING WORDS

Content that uses bad language, such as the use of disparaging or abusive words which is calculated to offend an individual or a group of persons, crude references words, in any language commonly used in the United Republic, which are considered obscene or profane including crude references to sexual intercourse and sexual organs, and hate speech,

10. FALSE, UNTRUE, MISLEADING CONTENT

Content that is false, untrue, [or] misleading which is likely to mislead or deceive the public unless where it is clearly pre-stated that the content is a satire, parody or fiction; and where it is preceded by a statement that the content is not factual.

Portions of the list of prohibited content (paragraph 2(b)) constitute criminal defamation in another guise, which, even if applied with moderation, still casts "a long shadow: the possibility of being arrested by the police, held in detention and subjected to a criminal trial will be in the back of the mind of a journalist when he or she is deciding whether to expose, for example, a case of high-level corruption".[1769] It has also been noted that paragraph 2(b) appears to eliminate the defence of truth.[1770]

Regarding the list of prohibited content, one analysis states:

> *The prohibited content is provided in overly broad terms prone to multiple interpretation[s] and manipulation. There are no clear definitions of some of the prohibited content and some are worded in open-ended fashion inviting the subjective interpretation of the enforcers. These may be used to restrict or censor certain information as prohibited content in case the Authority or Government doesn't like them.*[1771]

[1769] Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 11.
[1770] Id.
[1771] Id, page 3.

Another commentary asserts that, while some of the types of prohibited content are targeted at the legitimate aims of protecting public order, public health and the rights of others, there are broad categories of prohibited speech that do not advance legitimate aims according to international human rights standards.[1772]

The 2020 regulations contain an ever more rigorous **take-down notification** procedure than the Cybercrime Act. A person affected by prohibited content can notify a licensee of this, and the licensee is then required to take steps to remove the prohibited content *within two hours*. If the subscriber who initiated the prohibited content fails to remove it within the two-hour period, the licensee must suspend or terminate the subscriber's account. The licensee is required to take the same steps if the TCRA orders the removal of prohibited content.[1773] A local commentary identifies the following concerns:

> *This is problematic in two ways. First, the Regulations do not contain any safeguard against malafide intention by individuals who may use that loophole to affect the rights of other individuals to express their opinions. This is because under the regulation the licensee or host is under legal obligation to take down the impugned post within 2 hours after notification. Then the overriding question is who judges or decides whether the content is actually a prohibited content? Is it the offended person, TCRA or licensees? In actual sense, the intermediaries seem to assume the role of the courts or judges and have been empowered to restrict the right of others to express their opinions. Second, there is no […] express prescribed mechanism to challenge such take down, e.g appeals etc. What if the person is aggrieved by such decision to take down his or her posts? What is the remedy? The Regulations are silent on this.*[1774]

The same commentary goes on to assert that it is unacceptable for third parties such as internet service providers "to act on behalf of the authorities as censors" by taking down content. Such parties are not judicially qualified to determine whether a certain website or content might contravene the law and, due to the legal provisions on liability, they are likely to err on the side of caution in borderline cases. Furthermore, there are no safeguards to ensure that such third parties do not abuse their powers.

The absence of any requirement for a court order or due process safeguards such as a right to notice and appeal by the author of the content is "deeply inappropriate" and contrary to international standards on freedom of expression.[1775]

The 2020 regulations also restrict **anonymity**. Regulation 9(d) requires licensees to have in place mechanisms that can identify the source of all content. It has been noted that this makes it virtually impossible to post anonymous content online, and that with

[1772] "LEXOTA Country Analysis: Tanzania", last updated December 2022.
[1773] Electronic and Postal Communications (Online Content) Regulations, 2020, regulation 11(3)-(4).
[1774] Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 4.
[1775] Id, pages 12-13. See also "Tanzania: Electronic and Postal Communications (Online Content) Regulations 2018: Legal Analysis", Article 19, April 2018, at pages 21-15, making similar points about a similar take-down notification procedure in the previous 2018 regulations.

"no guarantee of anonymity, individuals may not be free to express their opinion and thus their right to freedom of expression is impacted".[1776]

Licensees are also required under regulation 9(c) to employ **content filtering mechanisms** to safeguard against prohibited content. This requirement may result in restricted access to certain information that is not actually prohibited, based on differing interpretations of the broad definitions of prohibited content.[1777]

D) MEDIA SERVICES ACT, 2016

As indicated above, despite the ruling of the East African Court of Justice and some amendments made to the Act in 2023, all of the provisions identified as being unjustifiable restrictions on freedom of expression remain in place.[1778]

The 2023 amendments to section 50 of the Act removed references to publications that are "injurious to the reputation, rights and freedom of other persons" – but criminal defamation continues to be covered by section 35 of the Media Services Act, and defamatory content is still treated as prohibited content under the Electronic and Postal Communications (Online Content) Regulations, 2020 discussed above.

Also, section 50 still contains a broad prohibition on the publication of information that is intentionally or recklessly falsified – or in fact any statement – which threatens "the interests of defence, public safety, public order, the economic interests of the United Republic, public morality or public health", as well as false statements in general.[1779]

E) THE PENAL CODE [REVISED EDITION 2022]

There are several provisions of the Penal Code that are relevant to freedom of expression.[1780] Some of the key offences of this nature are briefly described below:

- Section 63B concerns the offence of **raising discontent and ill-will for unlawful purposes**. This involves making a statement to any assembly (defined as a gathering of seven or more persons) that is "likely to raise discontent amongst any of the inhabitants of the United Republic or to promote feelings of ill-will between different classes or communities of persons of the United Republic". There are a number of exceptions, including statements made solely to show that the Government has been misled or mistaken in any of its measures or to point out errors or defects in the Government or its policies, the Constitution, legislation or the administration of justice with a view to remedying those errors

[1776] Id, pages 5, 6-7. Note that regulation 9(d) was initially 9(e), prior to the 2022 amendments (Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022).
[1777] Id. Note that regulation 9(c) was initially 9(d), prior to the 2022 amendments (Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022).
[1778] See the discussion of this ruling in section 16.1 above.
[1779] Media Services Act 12 of 2016, as amended by The Written Laws (Miscellaneous Amendments) Act, 2023
[1780] The Penal Code [*Chapter 16*], Revised Edition 2022.

or defects. Prosecution for this offence requires the written consent of the Director of Public Prosecutions.

- Section 63C makes **hate speech** an offence. This applies to various forms of expression (words, behaviour, publications, performances, programmes and online speech) where there was an intent "to stir up ethnic hatred", or where that result was likely. Despite the reference to "ethnic hatred", "hatred" is more broadly defined as "hatred against a group of persons defined by reference to colour, race, gender, disability, conscience, belief, nationality or ethnic or national origins".
- Section 89(1) makes it an offence to use **obscene, abusive or insulting language** to any other person, in a manner that is likely to cause a breach of the peace.
- Section 129 makes it an offence to utter words or sounds, or to use gestures or objects with "the **deliberate intention of wounding the religious feelings of any person**". The offending words or actions must take place in the presence of the person in question to constitute the offence.
- Section 169 makes it an offence, with a few narrow exceptions, to make or share (via any form of communication) photos, pictures, videos or images of **corpses, dead persons, victims of crimes or gruesome incidents.**
- Section 175 makes it an offence to distribute or possess any writing, drawing, painting, poster, photograph or cinematograph film that is "**obscene**" or "**tending to corrupt morals**". These key terms are not defined and could be very widely or subjectively interpreted.
- The provisions on **criminal defamation** (sections 187-194) have been repealed. However, as discussed above, some other legal provisions that remain in force are tantamount to forms of criminal defamation.

F) ZANZIBAR

The **Zanzibar Penal Act 6 of 2018** also contains some offences which might be applied to limit freedom of expression. [1781] Some of the key provisions are the following, although the list is not exhaustive:

- Section 43 makes it an offence to publish or reproduce any **false statement which is likely to cause fear and alarm to the public or disturb the public peace**.
- Section 45 makes it an offence to publish anything that might degrade, revile or expose to hatred or contempt a **foreign ambassador or dignitary** with the intent to disturb peace and friendship between Zanzibar and the country in question.
- Section 104 makes it an offence to write any word, utter words or sounds, or to use gestures or objects, with "the **deliberate intention of wounding the religious feelings of any person**". Unlike the corresponding offence in the Tanzanian Penal Code, this offence covers offensive writings.

[1781] Zanzibar Penal Act 6 of 2018.

- Section 106 makes it an offence to **promote disharmony, enmity, hatred or ill-will** between different groups on the basis of race, religion, place of birth, residence, language, community "or any other ground whatsoever".

Despite the fact that the Cybercrimes Act applies to both Mainland Tanzania and Zanzibar, the **Zanzibar Penal Act 6 of 2018** contains a chapter on "Offences connected with Computers" which overlaps to some extent with parts of the Cybercrimes Act, 2015. Briefly, this chapter covers the following:

- **section 369: offences against intellectual property** (which also covers modification, destruction or disclosure of data for purposes of a scheme to defraud or to obtain property)
- **section 370: offences against computer equipment or supplies** (unauthorised modification of such items regardless of intent, with an enhanced penalty where there is an intent to defraud or to obtain property)
- **section 371: destruction of computer equipment** (unauthorised destruction of damage is an offence regardless of intent)
- **section 372: interfering with data** (where this is done intentionally or recklessly, without lawful excuse or justification)
- **section 373: interfering with computer system** (where this is done intentionally or recklessly, without lawful excuse or justification)
- **section 374: illegal interception of data** (where there is intentional interception, without lawful excuse or justification, of any non-public transmission or an electromagnetic emission that is carrying data)
- **section 375: illegal devices** (covering production, sale and other dealings in (a) a device designed or adapted for the purpose of committing an offence, or (b) a computer password, access code or other data with intent that it be used for the commission of an offence; possession of a device as described is an offence if done with the intent that it be used for the commission of an offence)
- **section 376: offences against computer users** (covering unauthorised access and denial of service, with an enhanced penalty where there is an intent to defraud or to obtain property)
- **section 377: fraud and related activities on Government computers** (unlawful access via a computer to various categories of Government information)
- **section 378: definitions.**

According to a secondary source, **The Registration of Newsagents, Newspapers and Books Act 5 of 1988** contains a provision on seditious publications (section 48(1)), provision on criminal libel (sections 53-ff) and an offence regarding publication of anything that might degrade, revile or expose to hatred or contempt a foreign ambassador or dignitary with the intent to disturb peace and friendship between Zanzibar and the country in question (section 61).[1782]

[1782] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 117, 120-122.

Also, according to a secondary source, the **Zanzibar Arts and Censorship Council Act 7 of 2015** contains several offences relating to pornography and child pornography (sections 46, 47 and 53). [1783]

G) SIM CARD REGISTRATION

The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020 were issued in terms of The Electronic and Postal Communications Act. They require all SIM cards to be "biometrically registered". Individual customers must present their national ID cards, which will be verified with the National Identification Authority (NIDA) against the customer's online or electronic fingerprint. The service provider is required to keep records of the subscriber with the details electronically retrieved from NIDA. Company SIM cards must be registered against the fingerprint of a company representative, along with valid certified copies of the company's Taxpayer Identification Number Certificate and other incorporation or registration documents. There are also rules for identity verification of other categories of customers, including foreign visitors, institutions, minors, refugees and diplomats. A licenced service provider is not allowed to activate an unregistered SIM card. The regulations also place limits on the maximum number of SIM cards that can be registered by one individual, company or institution without authorisation from the TCRA. [1784]

H) TAKE-DOWN NOTIFICATIONS

Take-down procedures are contained in both the **Cybercrimes Act** and the **Electronic and Postal Communications (Online Content) Regulations, 2020** and have already been discussed above.

[1783] Id, page 118.
[1784] The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020.

CHAPTER 17

ZAMBIA

CHAPTER 17: ZAMBIA

ZAMBIA KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **87th globally; 22nd out of 48 African countries** "Hakainde Hichilema's election as president in August 2021 has improved the situation for the media after some difficult years. But the legislative framework still needs improving and Zambia's economic problems continue to hold back journalistic independence."
MALABO CONVENTION: Party
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Zambia's 1991 Constitution, as amended through 2016 **20. PROTECTION OF FREEDOM OF EXPRESSION** 1. Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to impart and communicate ideas and information without interference, whether the communication be to the public generally or to any person or class of persons, and freedom from interference with his correspondence. 2. Subject to the provisions of this Constitution no law shall make any provision that derogates from freedom of the press. 3. Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this Article to the extent that it is shown that the law in question makes provision – a. that is reasonably required in the interests of defence, public safety, public order, public morality or public health; or b. that is reasonably required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, regulating educational institutions in the interests of persons receiving instruction therein, or the registration of, or regulating the technical administration or the technical operation of, newspapers and other publications, telephony, telegraphy, posts, wireless broadcasting or television; or c. that imposes restrictions on public officers; and except so far as that provision or, the thing done under the authority thereof as the case may be, is shown not to be reasonably justifiable in a democratic society.

KEY LAWS:
• The Cyber Security and Cyber Crimes Act, 2021 • Penal Code, 1930 [*Chapter 87*] (specific provisions)
CRIMINAL DEFAMATION: Yes
DATA PROTECTION: Zambia has a data protection law.[1785]
ACCESS TO INFORMATION: Zambia has no access to information law as yet, although a bill is under discussion.

17.1 CONTEXT

Print media publications are required to register under the **Printed Publications Act**.[1786] This applies to all newspapers, with a "newspaper" being defined as "any periodical publication published in intervals of not more than one month and consisting wholly, or for the greater part, of political or other news" or "other current topics" – with an exception for publications which are not intended for public sale or dissemination.[1787] It is a criminal offence to publish a newspaper that is not registered.[1788]

Broadcasting in Zambia is regulated by the **Independent Broadcasting Authority Act 17 of 2002.**[1789] The Board of **the Independent Broadcasting Authority (IBA) is appointed by the relevant minister**, on the recommendation of an appointments committee and subject to ratification by the National Assembly.[1790] The IBA issues broadcasting licences, develops a code of professional standards for broadcasters and deals with complaints relating to broadcasting services.[1791] It has the power to cancel a broadcasting licence if it considers this to be necessary "in the interest of public safety, security, peace, welfare or good order: or "otherwise appropriate in the circumstances of the case".[1792]

In June 2021, the IBA reportedly threatened to revoke the broadcasting license for private television station *Muvi TV* over alleged professional misconduct related to interviews with opposition politicians, asserting that the station had not offered government officials a right of reply to allegations made against them. [1793] It is also reported that the IBA cancelled the broadcasting license of the privately owned *Prime TV* after the ruling party and a government minister accused the broadcaster

[1785] The Data Protection Act 3 of 2021.
[1786] Printed Publications Act, 1947, as amended [*Chapter 161*].
[1787] Id, section 2.
[1788] Id, section 5.
[1789] Independent Broadcasting Authority Act 17 of 2002, as amended by the Independent Broadcasting Authority (Amendment) Act 26 of 2010 and the Independent Broadcasting Authority (Amendment) Act 18 of 2017
[1790] Id, section 7.
[1791] Id, sections 19-31, and sections 33-34.
[1792] Id, section 29(1)(j)-(k), as amended in 2010.
[1793] "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022; "Zambia's broadcasting regulator threatens to revoke Muvi TV's license", Committee to Protect Journalists, 16 June 2021.

of being "unpatriotic."[1794] The Minister of Information announced in 2021 that the government intended to repeal and replace the **Independent Broadcasting Authority** Act,[1795] but this has not yet taken place.[1796]

The state broadcaster, the Zambia National Broadcasting Corporation (ZNBC), is regulated by the **Zambia National Broadcasting Corporation Act**.[1797] The ZNBC Board is appointed by the relevant minister, subject to ratification by the National Assembly.[1798] In 2002, Parliament passed amendments to this Act to transform ZNBC from a state to a public broadcaster – but that Amendment Act was never fully operationalised, and the ZNBC reportedly continues to report to the Ministry of Information and Broadcasting Services. The current status of ZNBC was cemented with the passage of 2010 and 2017 amendments that entrenched executive influence over the ZNBC.[1799]

Information and communications technology is regulated by the Information and Communication Technologies Act 15 of 2009, which replaces the Telecommunications Act, 1994, and the Radio-Communications Act, 1994 and transforms the previous Communications Authority into the Zambia Information and Communication Technology Authority (ZICTA).[1800] The ZICTA Board is appointed by the relevant minister,[1801] but is supposed to operate as an autonomous body that is not subject to the direction of any other person or authority.[1802] ZICTA issues licences for electronic communications services and networks.[1803] ZICTA has a broad power to suspend or cancel such licences "in the "public interest".[1804] It is a general offence under this Act for anyone to use any electronic communications apparatus for the purposes of an offence against public order or morality in the Penal Code.[1805]

In 2018, ZICTA announced a new rule requiring WhatsApp group administrators to register their groups and set up codes of ethics, with violation of these ethics being a criminal offence. This development was widely perceived by many as a government

[1794] "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022; "Zambia cancels broadcaster Prime TV's license, police shutter office", Committee to Protect Journalists, 13 April 2020.
[1795] "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022.
[1796] Id.
[1797] Zambia National Broadcasting Corporation Act 16 of 1987 [Chapter. 154], as amended by Zambia National Broadcasting Corporation (Amendment) Act 16 of 2002, Zambia National Broadcasting Corporation (Amendment) Act 16 of 2010, Zambia National Broadcasting Corporation (Amendment) Act 17 of 2017.
[1798] Id, section 4.
[1799] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 154; see the 2002, 2010 and 2017 amendment acts cited above.
[1800] Information and Communication Technologies Act 15 of 2009 as amended by the Information and Communication Technologies (Amendment) Act 3 of 2010 (substituting sections 43, 47 and 48).
[1801] Id, First Schedule.
[1802] Id, section 6.
[1803] Id, sections 9-10.
[1804] Id, section 18(1)(h).
[1805] Id, section 85.

effort to control free speech.[1806] However, this initiative was reportedly withdrawn.[1807]

The Zambia Media Council (ZAMEC) is an independent, self-regulatory body for the media in Zambia which was launched in 2012.[1808] According to a 2019 report of the Parliamentary Committee on Media, Information and Communication Technologies:

> *ZAMEC was a culmination of a sustained campaign by the media fraternity to establish a voluntary self-regulatory, but non-statutory media body to oversee the enforcement of media ethics. A board was appointed and had a constitution and a code of ethics, but it had financial challenges and lacked the authority to impose sanctions and because of that, it was difficult to operationalise it. ZAMEC sought to conciliate, mediate and arbitrate upon the public and media's alleged abrogation of ethics.*[1809]

In 2019, government pushed the media sector to come up with a formal regulatory framework, failing which the government would propose a statutory framework. The media sector held consultations and proposed a draft "ZAMEC Bill" which was submitted to the Ministry of Information and Broadcasting Services. This bill was designed to preserve the independent nature of the body, while giving the body more "teeth". [1810] However as the draft moved forward, it inspired differing opinions amongst the various stakeholders.[1811] MISA-Zambia provided the following update in mid-2022:

> *In 2019, the state and media bodies agreed to establish a media regulation mechanism for Zambia that upholds media freedoms under a hybrid model i.e., self-regulation backed by a law. A layman's bill dubbed ZAMEC Bill was drafted and submitted to the state. However, media associations reached a stalemate with the previous government which had redrafted the Bill and included clauses which were dangerous to the protection of media freedom and freedom of expression in Zambia. The former administration changed the ZAMEC Bill and included clauses such as jail terms and fines, and the mandatory registration of all journalists. The current ZAMEC bill still includes these contentious clauses despite going against recognized international and regional best practices. After having learnt from the process and the New Dawn government's positive pronouncements on media freedom and freedom of expression, we are convinced that a purely self-regulatory mechanism is the best model for Zambia. Self-regulation will guarantee that media houses and journalists can operate*

[1806] Abraham Kalito, "WhatsApp group admins will be required to register, warns ZICTA", *News Diggers!*, 31 May 2018; Nahashon Musungu, "Zambia: New Rule Compels Whatsapp Admins in Zambia to Register Groups or Be Arrested", *Nairobi News*, 2 June 2018.
[1807] Jasper Mangwana, Twitter post, 15 November 2019. ZICTA issued a press release in 2018 entitled "Response to Correct the Allegation that ZICTA was Pushing for the Law to Start Registering WhatsApp Administrators". "ZICTA Annual Report 2018, page 46.
[1808] Naomi Hunt, "IPI welcomes launch of Zambia Media Council", International Press Institute, 6 July 2012.
[1809] *Report of the Committee on Media, Information and Communication Technologies for the Third Session of the Twelfth National Assembly*, June 2019, section 9.5.
[1810] "Zambia media self–regulation; what the media must know!", MISA-Zambia, 20 March 2020; "State of the Media in Zambia". MISA-Zambia, July-September 2021.
[1811] Some of the views on the Bill's pros and cons are canvassed in the *Report of the Committee on Media, Information and Communication Technologies for the Third Session of the Twelfth National Assembly*, June 2019. See also, for instance, "The Disquieting Questions about ZAMEC as Means for Media Self-Regulation in Zambia", *Lusaka Times,* 13 August 2022; Media Owners Reject Draft Bill", *Nation*, 16 June 2022; "State of the Media Regulation Roadmap", MISA-Zambia statement, 10 June 2022; Michael Kaumba, "Resubmit Zamec Bill To Ministry Of Justice, Media Stakeholders Told", ZNBC, 5 April 2022; "Ministry of Justice wants Self-Regulation Bill to include the regulation of visiting international journalists", *Lusaka Times,* 7 March 2022.

> *freely and professionally without fear of government censorship and ensure that standards and public trust are maintained. […] Therefore, MISA Zambia wishes to support a pure self-regulatory mechanism that allows media houses and practitioners to take the lead in setting up their own media regulatory mechanism.*[1812]

Commenting on this topic for this report, Richard Mulonga, the Chief Executive Officer of the Bloggers of Zambia, indicated that an uneasy consensus had been reached within the media sector since the issuing of the above-quoted statement by MISA Zambia in 2022 to support the development and passing of the "ZAMEC Bill", but that this consensus collapsed in early 2023 when MISA Zambia and some media owners split with others in the sector and announced that they would not be supporting the process and reiterated that self-regulation was the only way to go.[1813] According to Mulonga there was "a lot of confusion" on the media landscape at the time because of the rift between those in favour of self-regulation and those in favour of self-regulation backed by a law, and that the "process has just been going around in circles" as a result of the impasse. Mulonga, who supports self-regulation, stated that there was "a lot of political interference" at play in the stalled "ZAMEC Bill" process, which did not bode well for encouraging unity around the positions of either of the sides on the issue. This was a developing situation that was hard to pin down at the time of finalising this report.

17.2 CONSTITUTION

Article 20 of the Zambian Constitution on freedom of expression is quoted on the first page of this chapter. According to one legal commentator, although the recital of the limitations provisions in Article 20(3) is more extensive than the statement of the right itself, most of the grounds for limitation of the right are consistent with internationally accepted standards. However, there are two limitations grounds that appear problematic:

1. The possibility to restrict the speech of public officers' stems from the duty of confidentiality that applies to many public officials but could be applied to discourage whistleblowers in the public service to make illegal conduct public.
2. The rationale behind the possibility of restricting the speech of educational institutions is unclear, given that academic freedom is often specifically cited as a component of the right to freedom of expression.[1814]

In 1995, Article 20 was relied upon in the Mwape case as the basis for challenging the constitutionality of **section 69 of the Penal Code dealing with the offence of defamation of the President**. Two journalists charged with this crime argued that the provision violated their right to freedom of expression. The High Court disagreed, on the basis that the freedom of expression was protected since legitimate criticism

[1812] "State of the Media Regulation Roadmap", MISA-Zambia, 10 June 2022.
[1813] Richard Mulonga was interviewed via Zoom on 21 July 2023.
[1814] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 131.

would not constitute an offence under the provision, as opposed to speech that might inflame public passions and incite unrest in a fragile young democracy. The Court also rejected the argument that the offence violated the principle of equality since it applied only to one official and not generally, holding that it is justifiable for Parliament to give special protection to certain categories of people based on their status. According to the Court, "The repercussions that follow the defaming of the President or a foreign potentate are not the same as those that follow the defamation of an ordinary person. To put it graphically one could say that the President is a big rock in a small pond. On the other hand, the ordinary person is a small stone in a lake. When dropped into the lake, it only causes ripples. Hence the emphasis that a separate section should deal with defamation of the President."[1815] Another attempt to secure a court ruling on this provision in 2020 also failed when a magistrate refused a request to refer the question of the constitutionality of this section to a higher court.[1816]Section 69 of the Penal Code was repealed in December 2022,[1817] but it has been noted that defamation against the President would still be an offence under the general crime of criminal defamation in Chapter 18 of the Penal Code.[1818]

In 2008, in the Clarke case, the Supreme Court stopped the government's attempt to deport a **British journalist**, Roy Clarke, after he wrote a satirical article that was critical of the President of Zambia and two government ministers. Although the Court did not find any infringement of the constitutional right to freedom of expression, it held that the deportation was an unreasonable and disproportionate response to the publication of the article, which cited allegations of vote-rigging by the President and two government ministers and referred to these officials as animals (in a reference to George Orwell's famous novel, *Animal Farm)*. The government, in ordering the deportation, cited protection of "national security" as the reason, asserting that the article threatened peace and good order because the description of Zambian people as animals could incite hatred and lead to violence. Although the Court set aside the decision to deport Clarke, it noted that its decision should not be understood to permit crude and insulting satirical articles, emphasising that Clarke should respect the cultural norms of Zambia.[1819]

In 2014, in the Chipenzi case, the High Court found section 67 of the Penal Code to be an unconstitutional restriction on the right to freedom of expression. This provision made it an offence to **disseminate false information "likely to cause fear and alarm to the public or to disturb the public peace**". Two journalists were charged with this crime after they published an article in a Zambian newspaper alleging that Zambia's secret police had recruited members of foreign militia into the police service. The Court found section 67 impermissibly overbroad because it could prohibit not only the intentional publication of false news, but also false news that was published in the good faith belief that it was true – which meant that the offence could be abused by

[1815] *The People v Bright Mwape and Fred Mmembe* (1995) S.J., 17 March 1995; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 187.
[1816] "Freedom on the Net 2022: Zambia", Freedom House, section C3.
[1817] Penal Code (Amendment) Act 23 of 2022, section 11; Marisa Lourenço and Mwai Daka, "You Have The Right to Insult a President: Repealing Zambia's Penal Code Section 69", Oxford Human Rights Hub, 26 January 2023.
[1818] "Repeal Of Section 69 Of The Penal Code Is A Job Half Done For President Hichilema….the Police still has power to arrest and charge any person with criminal defamation of the President", *Zambian Observer*, 24 December 2022.
[1819] *Attorney General v Clarke*, 2008 ZR 38, 24 January 2008; see the case analysis by Global Freedom of Expression here.

being applied in respect of news that was unpopular with those in authority. The Court rejected the state's argument that the law was reasonably related to the protection of public order since the provision did not require any actual showing of public fear or disturbance.[1820] Lexota reports that, despite this ruling, Zambian authorities continue to reference section 67 as if it remains in force.[1821]

*In 2014, in a rather astonishing case, prominent h*uman rights activist Paul Kasonkomona was charged with **soliciting in a public place for immoral purposes under section 178(g) of the Penal Code** after he appeared on a television program advocating for human rights of the LGBT community in Zambia. The State appealed the acquittal of Kasonkomona by the Magistrate's Court. The High Court agreed with the lower court that the defendant was advocating and discussing the rights of the LGBT community and not attempting to persuade anyone to practice prohibited sexual activity, and that he was legitimately exercising his right to freedom of expression.[1822]

In August 2021, during the run-up to Zambia's general elections, local media reported that the President intended to shut down **access to social media** during the voting period "in an effort to maintain peace and order. The Zambian non-governmental organization asked the High Court to review the decision of the Zambian Information and Communications Technology Authority to interrupt internet access during this period. The case was resolved by a consent decree in which the Zambian Information and Communications Technology Authority (ZICTA) undertook not "do any act or make any omission outside of their legal regulatory powers and authority which may inhibit or interrupt the flow of and uninhibited access to information on all available telecommunication platforms under their control and/or regulation where the interest of consumers and their consumer and constitutional rights are threatened". ZICTA also undertook to inform the public of the reason for any interrupted or inhibited access to services under their control within 36 hours of the disruption.[1823]

In February 2022, the Supreme Court ruled that **the forced liquidation of the independent newspaper**, *The Post*, which took place in 2015 (shortly before national elections) was illegal. The Court found that *The Post*'s editor-in-chief at the time was excluded from the liquidation process, which was marked by irregularities. One commentator noted that while this ruling "does not undo the damage done", it is a belated acknowledgement of the serious irregularities that took place that will hopefully encourage "greater respect for press freedom and the rule of law in Zambia".[1824]

[1820] *Chipenzi v The People*, HPR/03/2014, 4 December 2014; see the case analysis by Global Freedom of Expression here.
[1821] "LEXOTA Country Analysis: Zambia", last updated July 2022.
[1822] *The People v Kasonkomona*, HPA/53/2014, 15 May 2015; see the case analysis by Global Freedom of Expression here.
[1823] Chapter One Foundation v Zambian Information and Communications Technology Authority, 2021/HP/0955, 21 March 2021; see the case analysis by Global Freedom of Expression here.
[1824] Kelsey Carolan, "Zambian Supreme Court rules liquidation of The Post was illegal", International Press Institute, 3 March 2022.

17.3 CASE STUDIES

*According to the US State Department's 2022 report on human rights practice in Zambia, t*he government "showed high levels of sensitivity to criticism, particularly from political opposition figures, and restricted the ability of individuals to criticize it freely or discuss matters of public interest", stating that "government officials and members of the ruling party harassed journalists and used threats to intimidate independent media".[1825]

In March 2023, journalists Namo Phiri and Abel Musonda, who were covering a protest by opposition party members in Lusaka, were **arrested along with protesters**, they **were released without charge** about six hours later. Police confiscated a phone used to film the protest but returned it the next day.[1826]

In November 2022, journalist Innocent Phiri and camera operator Obvious Kapunda were arrested as they filmed officers preparing to arrest an opposition party leader at his home in Lusaka. They were charged with **disorderly conduct under section 60 of the Zambia Police Act**. they were held for 21 hours and released after paying admission of guilt fines. Police apparently considered a charge of **obstruction of police under the Penal Code**, which is a more serious offence. They reported that police briefly confiscated their phones and the camera.[1827]

In April 2022, community reporter Eric Chiyuka, working for the privately owned online publication *CIC Press,* alleges that he was assaulted by police and then charged with assault himself in respect of the ensuing confrontation. The dispute arose after he ignored a direction from a town council official to stop taking photographs and video of a physical altercation between municipal police officers and members of the Evangelical Church of Zambia over a disputed piece of land in the town of Mufumbwe. As a result of an encounter with this official and police later that day, Chiyuka was charged with two counts of **assault with attempt to do grievous bodily harm under section 248 of the Penal Code** and detained for more than 48 hours.[1828]

In February 2022, television station manager Petty Chanda was questioned in connection with possible charges under **section 31(3) of the Cyber Security and Cyber Crimes Act, which makes it a crime to disclose or use intercepted communication**. This stemmed from the airing by the privately owned Kenmark Broadcasting Network (KBN TV) of a leaked audio conversation between two ruling party politicians about the possibility of preventing an opposition party from participating in a local by-election. Because Chanda could not produce the audio, she was later informed by police that a **charge of destroying evidence** was being investigated.[1829] Chanda was

[1825] "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
[1826] "Zambian police briefly detain 2 Millennium TV journalists covering protest", Committee to Protect Journalists, 14 March 2023.
[1827] "Muvi TV journalists arrested, fined after filming Zambian police raid on politician's home", Committee to Protect Journalists, 18 November 2022.
[1828] "Zambian journalist Eric Chiyuka charged with assault after covering land altercation", Committee to Protect Journalists, 6 April 2022.
[1829] "Police investigate journalist Petty Chanda over leaked audio of government officials", Committee to Protect Journalists, 3 February 2022.

apparently not ultimately arrested,[1830] but the intimidatory impact of the police action is obvious.

In April 2021, columnist Sishuwa Sishuwa was accused of **sedition** (which is a crime under the Penal Code) by Zambia's permanent representative to the African Union, Emmanuel Mwamba, after he wrote an article discussing the potential for unrest in Zambia after the August 2021 elections. In a Facebook post, Mwamba accused the columnist of "being a hired gun" and called the opinion piece an attempt to "scandalise Zambia, harm its reputation and impose a false and alarming international narrative".

After Sishuwa brought suit against Mwamba for defamation and malicious falsehood in respect of this post, Mwamba laid a charge of sedition with the police.[1831]

The government reportedly used the crime of **defamation of the President** and related offences to arrest at least 13 persons in separate incidents in 2022. For example, Andsen Zulu was convicted of defamation of the president and sentenced to one year's imprisonment for allegedly calling him "a member of the anti-Christ". Evangelist Benson Tembo was charged with defamation of the President for allegedly calling him a "satanist" and sentenced to 15 months' imprisonment. However, as noted above, this crime was repealed in December 2022.[1832]

There are a number of reports of intimidation of journalists by supporters of the ruling party:

- *In September 2022, a journalist received threatening phone calls from ruling party officials after a report on public complaints about a district commissioner, accusing him of disseminating falsehoods and threatening to send people to "sort him out".* [1833]
- In October 2022, a journalist from 3FM Radio Station was reportedly harassed, assaulted, and threatened by ruling party supporters on his way home from work, after he alleged that the minister of agriculture had misled parliament.[1834]
- In November 2022, ruling party supporters reportedly forced their way into the PASME radio studio during a live broadcast and assaulted the broadcaster.[1835]

[1830] "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
[1831] "Zambian columnist Sishuwa Sishuwa could face sedition charge for opinion piece on election", Committee to Protect Journalists, 12 May 2021; "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022.
[1832] "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A. Section 69 was repealed by the Penal Code (Amendment) Act 23 of 2022, section 11.
[1833] "Zambian officials threaten journalist Wellington Chanda over reporting", Committee to Protect Journalists, 30 September 2022.
[1834] "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
[1835] Id.

- In December 2021, ruling party supporters forced their way into the Mpika FM radio studio and forced the broadcaster to halt a program, featuring a discussion with an opposition member of Parliament. The radio station management reported the attack to local police, who arrested some persons in connection with the attack, but the radio station dropped the charges after the ruling party made a public apology that was broadcast on the station.[1836]

17.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) THE CYBER SECURITY AND CYBER CRIMES ACT 2 OF 2021

The Cyber Security and Cyber Crimes Act 2 of 2021 covers cyber security, the licensing of cyber security service providers, cybercrimes, interception of communications and electronic evidence.[1837] It deals with issues such as extradition, admissibility of electronic evidence, search and seizure, collection of traffic data, interception of content data and mutual assistance and cooperation relating to the investigation and prosecution of offences under the Act – as well as intelligence gathering, investigation, prosecution and judicial processes in respect of cybercrimes, cyber terrorism and cyber warfare. However, some civil society groups such as MISA-Zambia assert that aspects of this Act have the potential to infringe on internet freedoms.[1838] The Chapter One Foundation believes that the law restricts civic space by threatening "online assembly" and has forced journalists and others to engage in self-censorship for fear of arrest under the cybercrime law, or for related offences such as criminal defamation and sedition.[1839]

According to CIPESA (Collaboration on International ICT Policy for East and Southern Africa), the Act "was passed amidst criticism that it was primarily aimed at policing the cyber space and gagging freedom of expression and speech of government critics and opponents ahead of the general election slated for August 12, 2021". They quote a statement from then-President Lungu that the law was intended "to protect citizens from abuse by people who feel they can do or say whatever they want using the veil of cyberspace".[1840]

The Act is administered by the Zambia Information and Communication Technology Authority (ZICTA).[1841] It requires ZICTA to establish a "Zambia Computer Incidence Response Team" under its authority to deal with incidents such as hacking, computer

[1836] "Ruling party supporters raid Zambia's Mpika FM Radio, halt show featuring opposition", Committee to Protect Journalists, 5 January 2022.
[1837] The Cyber Security and Cyber Crimes Act, 2021. This Act replaces The Computer Misuse and Crimes Act 13 of 2004, which was repealed by section 114 of the Electronic Communications and Transactions Act 21 of 2009.
[1838] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 30; "2023 World Press Freedom: Zambia", Reporters Without Borders.
[1839] "2021 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
[1840] "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
[1841] The Cyber Security and Cyber Crimes Act, 2021, section 4 and definition of "authority" in section 2.

viruses and network attacks,[1842] and a National Cyber Security Advisory Coordinating Council to advise on cyber-security.[1843] The Authority must appoint a cyber inspector to ensure compliance with the Act.[1844]

The Act creates extensive new offences, both technical and content based. The non-content-based offences are listed in the table below.

THE CYBER SECURITY AND CYBER CRIMES ACT – TECHNICAL OFFENCES	
Section 49: Unauthorised access to, interception of or interference with computer system and data	It is an offence for a person to – • intentionally access or intercept any data without authority or permission to do so, or to exceed the authorised access; • intentionally and without authority to do so, interfere with or deviate data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective • without authority to do so, communicate, disclose or transmit any data, information, program, access code or command to any person not entitled or authorised to access them; • without authority to do so, introduce or spread a software code that damages a computer, computer system or network; • access or destroy any files, information, computer system or device without authorisation, or for purposes of concealing information necessary for an investigation into the commission of an offence; or • damage, delete, alter or suppress any communication or data without authorisation. It is also an offence to knowingly possess unauthorised data, subject to the Public Interest Disclosure (Protection of Whistleblowers) Act, 2010 or any other relevant law. o "Access" has the same meaning as in The Electronic Communications and Transactions Act 4 of 2021, which is "to use or open the whole or any part of the computer system or electronic communication system, or to see, open, use, get or enter information in a computer system".[1845] o None of these offences provides any justifications for situations where there was no intention to cause harm, such as tests of security vulnerabilities. This could be particularly problematic in respect of "exceeding authorised access" which could happen without malicious intention. o Two offences in this section are particularly worrying for freedom of expression: (1) communicating, disclosing or transmitting any *data or information* to any person not entitled to it or authorised to have it – oddly, with no reference to the use of any computer technology (subsection (4)(a)); and (2) knowingly possessing unauthorised *data* (subsection (5)). The term "data" is not defined. These offences could be applied to prevent journalists from possessing or reporting on information obtained from whistleblowers or caches of

[1842] Id, section 6.
[1843] Id, section 7.
[1844] Id, section 8.
[1845] The Electronic Communications and Transactions Act 4 of 2021, section 2

	documents such as Wikileaks – or even the old-school situation where information about wrongdoing arrives on a journalist's desk in an unmarked envelope. The reference to the Public Interest Disclosure (Protection of Whistleblowers) Act does not assist, since it appears to protect only the whistle-blowers themselves, and referrals from one public official to another public official; it does not cover others who may obtain data that the whistle-blowers uncovered.[1846] These offences would benefit from being tightened.
Section 50: Illegal devices and software	It is an offence to - • unlawfully produce, sell, procure for use, import, export, distribute or otherwise make available - o a device, including a computer program, that is designed or adapted for the purpose of committing a cybercrime; o a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; • knowingly possess one of these items with the intent that it be used by any person for the purpose of committing a cybercrime; • introduce or spread a software code that damages a computer or computer system with the intent that it be used by any person for the purpose of committing a cybercrime.
Section 51: Computer related misrepresentation	It is an offence to knowingly, without lawful excuse, input, alter, delete, or suppress computer data, resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic, whether or not the data is directly readable and intelligible. There is an enhanced penalty for committing this offence by sending out multiple electronic mail messages from or through computer systems, the penalty.
Section 53: Identity related crimes	It is an offence, knowingly and without lawful excuse, to use a computer system to transfer, possess, or use, a means of identification of another person, o Without clarity on what would be covered by "lawful excuse", this offence could inhibit some instances of investigative journalism.
Section 54: Publication of information	A person who, with intent to compromise the safety and security of any other person, publishes information or data presented in a picture, image, text, symbol, voice or any other form in a computer system commits an offence and is liable, on conviction, to a fine of not less than five hundred thousand penalty units or to imprisonment for a term exceeding five years or to both. o This offence is very broad. Would online publication of allegations of corruption or other wrongdoing compromises someone's "safety and security" by causing them to fear arrest and prosecution? Would hard-hitting criticism of a public official or a private person fall into this category? The formulation of this offence appears to inhibit freedom of expression unwarrantedly by its vagueness. o The offence applies regardless of whether or not the "information" published is true.

[1846] Public Interest Disclosure (Protection of Whistleblowers) Act 4 of 2010.

	○ A member of the digital rights organization Bloggers of Zambia has said that this "overly broad and vague" provision "can be used to stifle journalistic work".[1847]
Section 55: Aiding, abetting, counselling, etc.	It is an offence to aid, abet, counsel, procure, incite or solicit another person to commit, or to conspire to commit, any offence under the Act.
Section 60: Introduction of malicious software into computer system	It is an offence to intentionally introduce or spread malicious software into a computer system.
Section 61: Denial of service attacks	It is an offence to intentionally render a computer system incapable of providing normal services to its legitimate users.
Section 62: Unsolicited electronic messages [spam]	It is an offence "knowingly and without lawful excuse or justification" to - • initiate the transmission of multiple electronic communications from or through a computer system; • use a computer system to relay or retransmit multiple electronic communications, with the intent to deceive or mislead users, or any electronic mail of a licensee, as to the origin of such messages • materially falsify header information in multiple electronic communications and intentionally initiate the transmission of such messages. There are exceptions for - • the transmission of multiple electronic communications within customer, business or other relationships where this would be reasonably expected and where the recipient has not opted out of the relationship; and • the transmission of multiple electronic communications by public institutions for purposes of raising awareness or collecting information with regard to education, health, security, safety outages or emergencies. ○ Section 2 defines "multiple electronic mail message" as a mail message including email and instant messaging sent to *more than once to a recipient*. Provisions on spam in other cybercrime laws typically refer to messages sent *to more than one recipient*.
Section 63: Prohibition of use of computer system for offences	It is an offence to use a computer system for any activity which constitutes an offence under any written law other than the cybercrime law. The penalty is the same penalty specified for that offence in the applicable law. ○ This provision appears to be aimed at ensuring that the use of a computer system to commit an offence is covered even if this is not specified in the formulation of the offence in question.

[1847] Vaughan O'Grady, "Will Zambia review its cyber security law?", Developing Telecoms, 17 May 2022 (quoting Richard Mulonga).

Section 70: Cyber terrorism	It is an offence to use a computer system, or causes a computer system to be used, for the purposes of cyber terrorism. "Cyber terrorism" means "the unlawful use of computers and information technology to unlawfully attack or threaten to attack computers, networks and the information stored therein done to intimidate or coerce a government or its people in furtherance of political or social objectives and to cause severe disruption or widespread fear in society."
Section 71: Cyber attack	It is an offence to carry out a cyber attack. o "Cyber attack" is not defined, making it hard to know what precisely is covered by this offence.

The Act also creates the content-based offences listed in the table below.

The Cyber Security and Cyber Crimes Act – Content-based Offences	
Section 52: Cyberextortion	It is an offence to do any of the following through a computer system with intent to extort or gain anything from any person - • accuse or threaten to accuse a person of committing a crime or soliciting or threatening someone else to commit or permit the commission of a crime; • threatening that a person will be accused by another person of committing a crime; • causing any person to receive any writing containing such accusation or threat, with knowledge of the contents of the writing; • knowingly transmitting any communication containing a threat to cause damage to a computer system with the intent to extort from any person any money or other thing of value; • obtaining any advantage from another person; or • compelling another person to perform or to abstain from performing any act. o The reference to extortion by obtaining "any advantage from another person" is unclear. o Requiring the intention to extort helps to narrow this offence.
Section 56: Prohibition of pornography	It is an offence to produce or participate in the production of pornography using a computer system. The potential period of imprisonment for this offence is 5 years. It is also an offence to knowingly - • produce pornography for the purpose of its distribution for profit through a computer system (which could lead to imprisonment for 10 years) • offer, circulate or make available, pornography through a computer system (which could lead to imprisonment for 5 years). o "Pornography" is defined as "audio or visual material that depicts images of a person engaged in explicit sexual conduct". "Explicit sexual conduct" includes "sexual intercourse, or other sexual conduct whether between persons or between a person and an

	animal, masturbation, sexual sadistic or masochistic abuse, or the lascivious exhibition of the genitals or pubic area of any person" (section 2). o Note that these offences apply *without reference to the ages of the persons involved.* o The first offence listed here applies *without any requirement that the images be shared beyond the individual or individuals involved*. o Outlawing the production of pornography completely seems to be an unjustifiable restriction on freedom of expression, particularly when only a single individual or consenting adults are involved without any public element. The first offence could even apply to a person who produces a sexual image of themselves, without sharing the image with anyone at all. It seems unlikely that this prohibition would fall within the "public morality" exception in Article 20 of the Constitution if the images are not made public. o There is no exception for *bona fide* educational, artistic or similar endeavours. o Note that the *possession* of pornography is not included in the offence.
Section 57: Child pornography	It is an offence to knowingly - • produce child pornography for the purpose of its distribution through a computer system; • sell or make available any pornography to a child through a computer system; • compel, invite or allow a child to view pornography through a computer system with intent to corrupt a child's morals; • offer or makes available child pornography through a computer system; • distribute or transmit child pornography through a computer system; • procure and obtain child pornography through a computer system for oneself or another; • possess child pornography in a computer system or on a computer data storage medium; or • obtain access, through information and communication technologies, to child pornography. There are some exceptions for persons performing *bona fide* law enforcement functions. o Note that this offence would apply to consensual "sexting" between children of similar ages.
Section 58: Child solicitation	It is an offence to – • use a computer system to meet a child for the purpose of committing a sexual crime; • communicate with a child through a computer system for the purpose of making it easier to procure the child to engage in sexual activity; • attract a child for the purpose of making it easier to procure the child to engage in sexual activity; • attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with another person;

	• recruit a child to participate in pornographic performances intended to be produced or recorded, with or without the intent to distribute such material through a computer system or computer network. o The term "pornographic performances" is not defined. o Some of these offences do not require the use of a computer or a computer system, making these offences much broader than cybercrime.
Section 59: Obscene matters or things	It is an offence to - • make, produce or possess any obscene drawing, painting, picture, image, poster, emblem, photograph, video or any other object tending to corrupt morals; • import, convey, export any such matters or things; • put any such matters or things in circulation in any manner whatsoever; • carry on or take part in any business, whether public or private, concerned with any such matters or things; • deal in, distribute or publically exhibit such matters or things, or make a business of lending any of them; • advertise or make known any such matters or things, with a view to assisting the circulation of or traffic in them; • advertise or make known that a person is engaged in any of the acts referred to in this section; • advertise or make known how, or from whom, such matters or things can be procured, either directly or indirectly through a computer system; • publicly exhibit any indecent show or performance, or any show or performance tending to corrupt morals through a computer system. o This list of offences is broadly and confusingly drafted. There is no definition of what is "obscene" or "indecent" or "tending to corrupt morals", making it hard for persons to know what exactly is prohibited. o There is no exception for artistic or educational materials, which some might find as having a tendency to corrupt morals – particularly if they dealt with issues such as sexual orientation or gender identity. o Most of the actions which constitute offences under this section do not make any reference to the use of a computer or a computer system, making these offences much broader than cybercrime. o Some of the listed offences do not require any public element (such as simply making or possessing obscene matter), which would make it unlikely that they would fall within the "public morality" exception in Article 20 of the Constitution. o The potential period of imprisonment for these offences is very stiff, at 15 years. o CIPESA states: "The words 'any other object tending to corrupt morals,' in the provision make it ambiguous and so wide in scope that it has a chilling effect on freedom of expression and speech. The words 'corrupt morals' are not defined in the Act and thereby present uncertainties in implementation. Moreover, this potentially

	inhibits artistic, journalistic, research and education work on the basis of undefined obscenity, and corruption of morals. Indeed, authorities could use the section to levy charges of choice to prosecute critics of the government."[1848]
Section 65: Hate speech	It is an offence, using a computer system, to use "hate speech" knowingly and without lawful excuse. o Section 2 defines "hate speech and conduct" as "verbal or nonverbal communication, action, material whether video, audio, streaming or written, that involves hostility or segregation directed towards an individual or particular social groups on grounds of race, ethnicity, antisemitism, tribalism, sex, age, disability, colour, marital status, pregnancy, health status and economic status, culture, religion, belief, conscience, origin". o This is an admirably broad list of prohibited grounds, but "hostility" is not defined and could be over-broadly interpreted. "Segregation" might also be inappropriately applied in connection with sex; for example, it could technically apply to a discussion of single-sex prison cells, school hostels or toilet facilities. The same is true of segregation by "age", which could be justifiable in some contexts, or segregation by health status in an instance where quarantine for some infectious disease was promoted. It is not clear if all such instances would be covered by "lawful excuse. o CIPESA states: "Whereas fighting hate crime is a legitimate state responsibility the world over, this definition of hate speech is overly broad and vague and does not delineate legitimate expression which would not amount to hate crime. Accordingly, this provision could be abused to persecute critics through arbitrary arrests and detention. It could thus have a chilling effect on freedom of expression and information, promote self-censorship, and limit the exercise of the profession of journalism."[1849]
Section 66: Minimisation, etc., of genocide and crimes against humanity	It is an offence knowingly and without lawful excuse, through a computer system, to distribute or otherwise make available to the public or another person material which "denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity". o "Genocide" has the meaning assigned to the word in the United Nations Convention on the Prevention and Punishment of the Crime of Genocide (section 2). "Crimes against humanity" are not defined. o Note that this offence would capture even a private message from one individual to another if sent through a computer system, raising issues of privacy and freedom of expression. The Malabo Convention does not specify whether or not the communication must be public; it merely calls on States to make it a criminal offence to "deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system".

[1848] "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
[1849] Id.

Section 69: Harassment utilising means of electronic communication	This crime is concerningly broad.
	A person who[,] using a computer system intentionally[,] initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause emotional distress to a person commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.
	o The meaning of "harass" is not defined, nor is "emotional distress". o This offence is very broad and vague. For example, any criticism or allegation of wrongdoing, even if true, could "cause emotional distress". o According to CIPESA, "This provision can form the basis for silencing critical voices".[1850] o This offence needs to be re-drafted to avoid being an unreasonable restriction on freedom of expression.

In terms of investigation, law enforcement officers must apply for a warrant for **searches and seizures** of computer systems of computer data storage mediums under the Act, which requires approval by a magistrate.[1851] A cyber inspector has the power to "monitor and inspect a computer system or activity on an information system, where such activity or information is not in [the] public domain or is not accessible to the public", as well as search and seizure powers – but these investigative powers also require a warrant.[1852] However, in the case of a "cyber security threat" or a "cyber security incident" - which refers to a cyber act that "jeopardises or adversely impacts, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system" – a cyber investigator can issue a notice without judicial authority calling on a person to appear for questioning or to provide electronic records or other material.[1853]

The Act refers to **data retention notices** requiring an electronic communications service provider to retain internet connection records specified in the notice, but states that an electronic communication service provider shall not be required to retain "data" as part of an internet connection record.[1854] It does not specify the issuing authority or the procedure for such notices.

The Act establishes a **Central Monitoring and Co-ordination Centre** as the sole facility through which authorised interceptions are effected. The composition of this Centre is not specified, but it to be is managed, controlled and operated by the department responsible for Government communications in liaison with ZICTA.[1855] Law enforcement officers may apply to a judge for an "**interception of communications**

[1850] Id.
[1851] The Cyber Security and Cyber Crimes Act, 2021, section 75; Criminal Procedure Code [*Chapter 88*], section 118.
[1852] The Cyber Security and Cyber Crimes Act, 2021, sections 9 and 11.
[1853] Id, section 15.
[1854] Id. section 10.
[1855] Id, section 27.

order" if there are reasonable grounds to believe that an offence has been, or is likely to be, committed. The consent of the Attorney General is required for such an application. An initial order is valid for three months, but can be extended for any period determined by the judge.[1856] It has been noted that the failure to impose time limits on interception orders "could subject individuals, especially government critics and political opponents, to continued surveillance".[1857]

However, **where there is a risk of bodily harm, loss of life or property damage, a law enforcement officer may intercept communications without judicial authority**, and orally direct a service provider to route duplicate signals of indirect communications specified in that direction to the Central Monitoring and Coordination Centre; this includes situations where someone "has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries". An interception obtained via this route must be reported to a judge after the fact, along with a recording and a full or partial transcript of the communication intercepted in this manner. An electronic communications service provider who routes duplicate signals of indirect communications to the Central Monitoring and Coordination Centre via this route must also report the details to a judge after the fact. A judge has broad powers to fashion a remedy if interceptions undertaken without a warrant pursuant to this provision are abused.[1858] A similar procedure applies in cases where a law enforcement officer acts without judicial authority to obtain information pointing to a person's location in an emergency, which includes impending theft of finances from a bank or a financial institution.[1859]

Service providers are required to provide the technology necessary to enable the kinds of communications interception and monitoring that can be authorised under the Act. [1860]

The Act also requires electronic communication service providers to collect **identifying data from their customers** - including names, residential addresses and identity numbers. The law also authorises them to collect any other information that they consider necessary for the purpose of compliance with the Act's requirements.[1861] Such requirements undermine the possibility of anonymous communication.[1862]

In general, CIPESA notes that many provisions in the law "are vague and overly broad, in contravention of the principle of legality", while it also "extends the powers of state authorities to restrict and punish online expression, and gives law enforcement agents leverage to conduct unsupervised surveillance without the backing of a judicial

[1856] Id, section 28.
[1857] "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
[1858] The Cyber Security and Cyber Crimes Act, 2021, section 29.
[1859] Id, section 30.
[1860] Id, sections 38 and 40.
[1861] Id, section 39.
[1862] Freedom on the Net 2022: Zambia", Freedom House, section C4.

order".[1863]MISA-Zimbabwe (MISA's regional office) has expressed the view that the Act "falls far short of regional and international standards and instruments on human rights", noting its fears that governments in the region will rely on cybersecurity laws "to curtail freedom of expression and of the media".[1864] Other commentators have noted that the cybercrimes law was passed under former President Edgar Lungu at a time of closing civic space, with its vague definitions making it susceptible to "a politically selective application".[1865] Digital and media rights groups have continued to lobby the government to revise or repeal the law, on the grounds that interferes with a free and independent media. [1866]

In April 2021, several civil society groups[1867] approached the High Court in Lusaka alleging that the Cyber Security and Cyber Crimes Act should be declared unconstitutional on the basis that it threatens the right to freedom of expression, among other constitutional rights.[1868] At the time, these groups stated:

> *In a shrinking civic space, social media platforms and other online media present alternative platforms for members of the public to air their views on matters of public interest and gather virtually to share such views without the inhibitions of the much-abused Public Order Act. This platform has become even more important as the country and the world at large grapples with the Covid-19 pandemic and the regulations it necessitated. The Cyber Security and Cyber Crimes Act threatens this use of the cyber space.*[1869]

The legal challenge was unsuccessful, [1870] but no information on why it failed could be located.

President Hichilema has reportedly promised that the legislation would be reviewed with a view to protecting citizens from online abuse while also safeguarding media freedom.[1871] Indeed, the Ministry of Technology and Science issued a call for public comments and proposals for amendment to this law, with a deadline of 23 September 2022. This statement indicated that Cabinet had approved the amendment of the Act in principle, in order to "strengthen enforcement mechanisms and redefine concepts to align them to the Constitution".[1872]

[1863] "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
[1864] "Zambia's newly enacted cybercrime law challenged in court", MISA-Zimbabwe, 4 April 2021.
[1865] "Deluge of Digital Repression Threatens African Security", Nathaniel Allen and Catherine Lena Kelly African Center for Strategic Studies, 4 January 2022.
[1866] "Call for Comments on the Review of the Cyber Security and Cyber Crimes Act No. 2 of 2021", Ministry of Technology and Science, September 2022. The period between this call for input and the deadline for submission appears to have been less than one month.
[1867] Chapter One Foundation, Bloggers of Zambia, Gears Initiative, People's Action for Accountability and Good Governance in Zambia and the Alliance for Community Action.
[1868] "Zambia's newly enacted cybercrime law challenged in court", MISA-Zimbabwe, 4 April 2021; "New Cyber law goes to Court", *Lusaka Times*, 2 April 2021.
[1869] "Joint CSO Press Statement dated 1st April 2021 on the Cyber Security and Cyber Crimes Act No 2 of 2021", quoted in "New Cyber law goes to Court", *Lusaka Times*, 2 April 2021.
[1870] Susan Mwape, "Lungu law looms dangerously over Zambian digital rights", Association for Progressive Communications. 24 October 2022.
[1871] Vaughan O'Grady, "Will Zambia review its cyber security law?", Developing Telecoms, 17 May 2022
[1872] "Call for Comments on the Review of the Cyber Security and Cyber Crimes Act No. 2 of 2021", Ministry of Technology and Science, September 2022. The period between this call for input and the deadline for submission appears to have been less than one month.

However, Richard Mulonga, of Bloggers of Zambia, indicated for this report in July 2023 that, despite the undertaking by the Hichelema Cabinet in 2022 to amend the law, at the time the "process was not moving as fast as expected" and that there was "a lot of work that they need to do" instead of just going around making pronouncements about bringing the law in line with the constitution and best practice.

B) PENAL CODE

In addition to the broad content-based crimes in the Cyber Security and Cyber Crimes Act, there are also content-based provisions in the Penal Code that appear to unreasonably infringe freedom of expression – some of which have been applied in practice to inhibit free speech.[1873]

Zambia's Penal Code Act and Criminal Procedure Code Act were both recently reviewed,[1874] resulting in the **Penal Code (Amendment) Act 13 of 2022**,[1875] the **Criminal Procedure Code (Amendment) Act 22 of 2023**[1876] and the **Penal Code (Amendment) Act 23 of 2022.**[1877] Of relevance to this discussion, the Penal Code (Amendment) Act 23 of 2022 repealed section 69 on defamation of the President and section 71 on on "defamation of foreign princes".[1878]

Section 53 of the Penal Code deals with **prohibited publications**. If the President believes that a publication is contrary to the public interest (which is defined in section 62 as including the interest of defence, public safety and public order), he may, in his absolute discretion, issue an order declaring it to be a prohibited publication. Such an order can apply to a particular publication, a series of publications or *all* publications published by a particular person or association. Under section 54, it is an offence to print, import, publish, sell, distribute or reproduce a prohibited publication. It is an offence to even possess a prohibited publication "without lawful excuse". It has been remarked that a clear problem with the provisions on prohibited publications is that they are not objective: "In other words, the publication does not have to pose a genuine, realistic or objective threat to the public interest in defence, public safety or public order; the president just has to believe that this is the case before he makes an order prohibiting a publication. This does not comply with internationally accepted standards for prohibiting the publication of information."[1879] The Southern Africa Litigation Centre recommends that the power to declare a publication prohibited should lie with a body composed of members with specific expertise in media and related activities, and that there should also be an appeal process to different

[1873] Penal Code, 1930 [Chapter 87]. This version, as accessed on 29 June 2023, presents the law as it stood on 31 August 2000.
[1874] "What Prompted the Review of the Penal Code Act and the Criminal Procedure Code Act?", Zambia Law Development Commission, undated; "Call for Written Submissions: Review of the Penal Code Act, Chapter 87 of the Laws of Zambia, and the Criminal Procedure Code Act, Chapter 88 of the Laws of Zambia", Zambia Law Development Commissionm, undated (submission deadline: 20 February 2021).
[1875] Penal Code (Amendment) Act 13 of 2022.
[1876] Not located online.
[1877] Penal Code (Amendment) Act 23 of 2022.
[1878] Id, sections 11-12.
[1879] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 170.

decision makers. It also recommended that the offences related to possession and distribution of prohibited publications should include an intent element by requiring knowledge that a publication is prohibited.[1880]

Section 57 of the Penal Code, on **seditious practices**, makes it an offence to utter any seditions words, or to print, publish, sell, distribute, reproduce or even possess a seditious publication, which is a publication "containing any word, sign or visible presentation expressive of a seditious intention". Seditious intention has a detailed definition with a few exceptions in section 60 (reproduced in the box below), with the line between what is permitted and what is prohibited being very thin. The fact that prosecution for seditious actions requires the written consent of the Director of Public Prosecutions (section 58) is not an adequate safeguard against abuse of this offence. The Southern Africa Litigation Centre submits that the crime of sedition is contrary to modern principles of international human rights, noting that it has been found unconstitutional in Nigeria and Uganda, and unconstitutional in part in eSwatini.[1881]

Penal Code

57. OFFENCES IN RESPECT OF SEDITIOUS PRACTICES

(1) Any person who-

(a) does or attempts to do, or makes any preparation to do, or conspires with any person to do, any act with a seditious intention;

(b) utters any seditious words;

(c) prints, publishes, sells, offers for sale, distributes or reproduces any seditious publication;

(d) imports any seditious publication, unless he has no reason to believe that it is seditious;

is guilty of an offence and is liable for a first offence to imprisonment for seven years or to a fine not exceeding six thousand penalty units or to both; and any seditious publication shall be forfeited.

(2) Any person who, without lawful excuse, has in his possession any seditious publication is guilty of an offence and is liable for a first offence to imprisonment for two years or to a fine not exceeding three thousand penalty units or to both, and for a subsequent offence to imprisonment for five years; and such publication shall be forfeited.

60. SEDITIOUS INTENTION

(1) A seditious intention is an intention -

(a) to advocate the desirability of overthrowing by unlawful means the Government as by law established; or

(b) to bring into hatred or contempt or to excite disaffection against the Government as by law established; or

[1880] "Submission by the Southern Africa Litigation Centre on the Review of the Penal Code and Criminal Procedure Code", 20 February 2021.

[1881] Id.

(c) to excite the people of Zambia to attempt to procure the alteration, otherwise than by lawful means, of any other matter in Zambia as by law established; or
(d) to bring into hatred or contempt or to excite disaffection against the administration of justice in Zambia; or
(e) to raise discontent or disaffection among the people of Zambia; or
(f) to promote feelings of ill will or hostility between different communities or different parts of a community; or
(g) to promote feelings of ill will or hostility between different classes of the population of Zambia; or
(h) to advocate the desirability of any part of Zambia becoming an independent state or otherwise seceding from the Republic; or
(i) to incite violence or any offence prejudicial to public order or in disturbance of the public peace; or
(j) to incite resistance, either active or passive, or disobedience to any law or the administration thereof:
Provided that an intention, not being an intention manifested in such a manner as to effect or be likely to affect any of the purposes mentioned in the a foregoing provisions of this subsection, shall not be taken to be seditious if it is an intention-
(i) to show that the Government have been misled or mistaken in any of their measures; or
(ii) to point out errors or defects in the Government or Constitution as by law established or in legislation or in the administration of justice, with a view to the reformation of such errors or defects; or
(iii) to persuade the people of Zambia to attempt to procure by lawful means the alteration of any matter in Zambia as by law established; or
(iv) to point out, with a view to their removal, any matters which are producing or have a tendency to produce feelings of ill will or hostility between different classes of the population of Zambia.

(2) In determining whether the intention with which any act was done, any words were spoken, or any document was published, was or was not seditious, every person shall be deemed to intend the consequences which would naturally follow from his conduct at the time and under the circumstances in which he so conducted himself.

(3) For the purposes of paragraph (f) of subsection (1), "community" includes anybody or group of persons having a common tribal or racial origin.

Section 70 of the Penal Code criminalises **"expressing or showing hatred, ridicule or contempt for persons because of race, tribe, place of origin or colour".** The only problem here is understanding the parameters of "hatred, ridicule or contempt", none of which are elaborated.

Under section 177 of the Penal Code on **"obscene matters or things"**, it is an offence to make, produce or possess "obscene writings, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films or any other

object tending to corrupt morals", as well as to engage in various other actions involving such materials, or to publicly exhibit any indecent show or performance or any show or performance tending to corrupt morals. Section 59 of the cybercrime law appears to have simply translated this vague and broad provision to cyberspace. In both cases, material tending to "corrupt morals" is particularly subjective. One example of how this can be problematic is a 2010 case where a news editor circulated photographs of a woman giving birth outside a hospital during a nurses' strike to some politicians to highlight the effects of industrial action on public health. She was charged with distributing obscene material tending to corrupt morals but acquitted.[1882]

There is an entire chapter of the Penal Code on **criminal defamation ("libel")**, with the offence even being applicable in cases where the person defamed is already dead.[1883] The Southern Africa Litigation Centre takes the view that the provisions on criminal defamation "do not comply with international standards for freedom of expression and should be repealed", noting that defamation can be addressed through civil defamation or enforcement of media codes of ethics by self-regulatory bodies such as the Zambia Media Council.[1884]

As noted in section 17.2 above section 67 of the Penal Code on **alarming publications** which previously made it a crime to publish "any false statement, rumour or report that is likely to cause fear and alarm to the public or to disturb the public peace" has been declared unconstitutional – although it was surprisingly not formally repealed by the 2022 amendments.[1885] Section 69 of the Penal Code on **defamation of the President**, which previously made it a crime to publish any defamatory or insulting matter "with intent to bring the President into hatred, ridicule or contempt", was once frequently applied to silence critics but was ruled unconstitutional and repealed in 2022.[1886]

C) OTHER LAWS THAT MAY RESTRICT FREEDOM OF EXPRESSION

The **Prisons Act** makes it an offence to publish any part of a letter or document if there is reasonable cause to believe that it was written by or on behalf of a prisoner but was not endorsed by the officer in charge to authorise its removal from the prison).[1887] This could clearly make it difficult to expose problems in prison that government authorities would prefer to conceal.

[1882] Mandy Rossouw, "Zambian president challenged over violation of freedom of speech", *Mail & Guardian*, 1 June 2010.
[1883] Penal Code, 1930 [Chapter 87], Chapter XVIII, sections 191-198.
[1884] "Submission by the Southern Africa Litigation Centre on the Review of the Penal Code and Criminal Procedure Code", 20 February 2021.
[1885] Chipenzi v The People, HPR/03/2014, 4 December 2014; see the case analysis by Global Freedom of Expression here. The Court held as follows: "In conclusion, I find and hold that Section 67 does not fit under Article 20 (3) of the Constitution. It goes beyond what is permissible under that clause. I, therefore, find that Section 67 does not pass the test of being 'reasonably justifiable in a democratic society.' It contravenes Article 20 of the Constitution and is null and void, and therefore invalid for unconstitutionality. It follows also that the invalidity and the constitutional guarantee of freedom of expression preclude the prosecution of persons and the criminalization of alleged false statements under Section 67."
[1886] Penal Code (Amendment) Act 23 of 2022, section 11.
[1887] Prisons Act 56 of 1965, subsections 79(3) and (4).

The definition of espionage in the **State Security Act** includes amongst other things publishing or communicating any article or information which "might be" directly or indirectly useful to a foreign power or a "disaffected person" (a person carrying on a seditious activity), even if there was no intention to have this effect. The *minimum* penalty for this crime is imprisonment for 20 years.[1888] The group *Article 19* reports that the existence of this offence has "made civil servants reluctant to provide information about government operation to journalists".[1889]

The Anti-Terrorism and Non-Proliferation Act makes it an offence "for purposes of or in connection with terrorism and proliferation" to collect, make or transmit information "of a kind likely to be useful to a person committing or preparing an act of terrorism or proliferation", or to possess a document or record containing information "likely to be used for a terrorist act or proliferation". The penalty is life imprisonment.[1890] While the requisite purpose would appear to protect persons who obtain such information for the purpose of exposing or reporting on possible terrorism, it can be questioned if this offence with its severe consequences is sufficiently tightly drafted.[1891]

Zambia also has a statute that governs civil defamation, the **Defamation Act**, instead of relying on the common law on defamation as developed through court cases. This law provides for a defence of "fair comment" for publications consisting partly of allegations of fact and partly of expressions of opinion, which does not require that the truth of every allegation of fact be proved. The law also gives a qualified privilege to publications in newspapers and "wireless broadcasting" where no malice can be proved there is no similar privilege for online publications, probably due to the age of the law (which was enacted in 1953). Privilege in respect of otherwise defamatory publications is also inapplicable to statements in respect of a candidate for the National Assembly or any local authority or to the National Assembly.[1892]

D) STATE SURVEILLANCE AND INVESTIGATORY POWERS

The investigation tools that are included in **The Cyber Security and Cyber Crimes Act 2 of 2021** have already been summarised above.

It has been reported that the Zambian government uses an **international surveillance tool** to monitor the private communications of citizens, particularly protestors and opposition leaders. The surveillance platform in question allows access to telephone calls, text messages, and location services.[1893]

[1888] State Security Act, 1969 [*Chapter 111*], section 3.
[1889] "ARTICLE 19's Submission to the UN Universal Periodic Review of The Republic of Zambia, 14th Session of the Working Group of the Human Rights Council, October-November 2012", paragraph 4.
[1890] The Anti-Terrorism And Non-Proliferation Act 6 of 2018, section 26.
[1891] Article 19 expressed concern over a similar provision in a previous law. "ARTICLE 19's Submission to the UN Universal Periodic Review of The Republic of Zambia, 14th Session of the Working Group of the Human Rights Council, October-November 2012", paragraph 4.
[1892] Defamation Act 46 of 1953, sections 7, 9, 14 and 18 in particular. For an example of the limitations of the defence of fair comment see *Post Newspaper Ltd v Mulenga*, Supreme Court for Zambia, Appeal 22/2014, 13 May 2020.
[1893] "2021 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A, citing a report by the University of Toronto Citizen Lab entitled *Running in Circles:Uncovering the Clients of Cyberespionage Firm Circles*, released in December 2020

E) SIM CARD REGISTRATION

ZICTA has issued **Statutory Instrument Number 65 of 2011** on Registration of Electronic Communications Apparatus, which places obligations on service providers, sellers and buyers of SIM cards to ensure that all SIM cards are registered. Subscribers must provide their name and date of birth, gender, address and email address if available, along with (since 2019) an approved form of identification and a "live facial image". For citizens, this is a National Registration Card, a valid passport, a valid driver's license or a Voters Card. Pre-2019 registrations must be updated to include all the currently required information. Subscriber information is held by the respective mobile phone operators in a secure data base and can be disclosed only as authorised by law. Unregistered SIM cards are deactivated. It is also illegal for any one person to own more than 10 SIM cards without justification. [1894] ZICTA puts forward four reasons for requiring SIM card registration:

a) Help create a database to aid Law enforcement agencies identify the mobile phone SIM card owners.
b) Track criminals who use cell phones for illegal activities
c) Curb other negative incidents such as [loss] of phone through theft, nuisance/hate text messages, fraud, threats and inciting violence
d) Help service providers know their customers better. [1895]

F) TAKE-DOWN NOTIFICATIONS

Take-down notifications are governed by the **Electronic Communications and Transactions Act**. Any person can give a written notification to a service provider stating that certain data or activity is unlawful or infringes their rights or the rights of another with a motivation for this view. A service provider who receives such a notification must remove the materials as soon as possible. The provision says that a dispute regarding a takedown notification "may be referred" to ZICTA for determination, but the law contains no requirement to notify the person who has posted the material. The service provider avoids liability for the material in question if it was unaware of the infringement and if it removes, or disables access to, the offending material within a reasonable time after being informed that it infringes the rights of a person. A take-down notification submitted to a service provider must include a statement certifying that it is made in good faith, and it is a crime to submit a false notification, punishable by a fine or imprisonment for a maximum of two years.[1896] Nevertheless, the legal scheme is clearly weighted in favour of the removal of material alleged to be unlawful, with the initial decision-making lying entirely with the service provider.

[1894] "Mandatory SIM Card Live Facial Capture Directive", ZICTA, 6 January 2023; ZICTA webpage, "Sim registration (FAQ)", undated (accessed 4 August 2023); Lucky Phiri, "ZICTA to Deregister Half a Million SIM Cards", ZNBC, 8 February 2022.
[1895] ZICTA webpage, "Sim registration (FAQ)", undated (accessed 4 August 2023)
[1896] Electronic Communications and Transactions Act 4 of 2021, sections 81-82.

CHAPTER 18

ZIMBABWE

CHAPTER 18: ZIMBABWE

ZIMBABWE KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **126th globally; 39th out of 48 African countries** "The media situation in Zimbabwe has improved slightly since the dictator Robert Mugabe's ouster in 2017. Access to information has increased and self-censorship has declined."
MALABO CONVENTION: NOT signatory or party
BUDAPEST CONVENTION: NOT signatory or party

CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION:
Zimbabwe's 2013 Constitution, as amended through 2017
The Constitution of Zimbabwe Amendment Act No. 2 of 2021 does not affect the quoted provisions.

61. FREEDOM OF EXPRESSION AND FREEDOM OF THE MEDIA

1. Every person has the right to freedom of expression, which includes -
a. freedom to seek, receive and communicate ideas and other information;
b. freedom of artistic expression and scientific research and creativity; and
c. academic freedom.

2. Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information.

3. Broadcasting and other electronic media of communication have freedom of establishment, subject only to State licensing procedures that –
a. are necessary to regulate the airwaves and other forms of signal distribution; and
b. are independent of control by government or by political or commercial interests.

4. *All State-owned media of communication must –*
a. be free to determine independently the editorial content of their broadcasts or other communications;
b. be impartial; and
c. afford fair opportunity for the presentation of divergent views and dissenting opinions.

5. *Freedom of expression and freedom of the media exclude –*
a. incitement to violence;
b. advocacy of hatred or hate speech;
c. malicious injury to a person's reputation or dignity; or
d. malicious or unwarranted breach of a person's right to privacy.

86. LIMITATION OF RIGHTS AND FREEDOMS

1. **The fundamental rights and freedoms set out in this Chapter must be exercised reasonably and with due regard for the rights and freedoms of other persons.**

2. **The fundamental rights and freedoms set out in this Chapter may be limited only in terms of a law of general application and to the extent that the limitation is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom, taking into account all relevant factors, including-**

a. the nature of the right or freedom concerned;
b. the purpose of the limitation, in particular whether it is necessary in the interests of defence, public safety, public order, public morality, public health, regional or town planning or the general public interest;
c. the nature and extent of the limitation;
d. the need to ensure that the enjoyment of rights and freedoms by any person does not prejudice the rights and freedoms of others;
e. the relationship between the limitation and its purpose, in particular whether it imposes greater restrictions on the right or freedom concerned than are necessary to achieve its purpose; and
f. whether there are any less restrictive means of achieving the purpose of the limitation.

KEY LAWS:

- Criminal Law (Codification and Reform) Act [*Chapter 9:23*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Criminal Procedure and Evidence Act [*Chapter 9:07*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Interception of Communications Act, 2007 [*Chapter 11:20*]
  as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]
- Criminal Law Codification and Reform Amendment Act, 2023 ("Patriots Act")

CRIMINAL DEFAMATION: No[1897]

DATA PROTECTION: Zimbabwe has a combined cybercrimes and data protection law.[1898]

ACCESS TO INFORMATION: Zimbabwe has a right of access to information in its Constitution[1899]
as well as an access to information law.[1900]

[1897] Madanhire & Another v AG (CCZ 2/14 Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.
[1898] Data Protection Act, 2021 [Chapter 11:22] originally, now part of the Cyber and Data Protection Act, 2021 [Chapter 12:07].
[1899] Zimbabwe's 2013 Constitution, as amended through 2017, section 62.
[1900] Freedom of Information Act, 2020 [Chapter 10:33], which replaced the Access to Information and Protection of Privacy Act of 2003. See also Freedom of Information (General) Regulations, 2021 [Statutory Instrument 229 of 2021, CAP. 10:33].

18.1 CONTEXT

Journalists, news agencies and media services were previously required to be accredited or registered under the **Access to Information and Protection of Privacy Act, 2003**. In 2005, the African Commission on Human and People's Rights found that the onerous regime for the accreditation of journalists in terms of this law was inconsistent with the African Charter on Human and People's Rights. The Commission found that, while compulsory registration procedures are not in themselves a violation of the right to freedom of expression if they are merely administrative in nature, the Zimbabwean law - which contained an offence for "abusing journalistic privilege" which included the publication of false news - created considerable scope for politically motivated action by the authorities" and was aimed at control rather than regulation. It recommended specific changes to remove the offending sections of this law.[1901] The entire law was repealed by the Freedom of Information Act, 2020 – although, confusingly, fees for accreditation are still being issued under the authority of the repealed Act.[1902]

The key regulatory body for the media is **the Zimbabwe Media Commission established by section 248 of the Zimbabwe Constitution** and comprising a Chairperson appointed by the President and eight members appointed by the President from a list of not fewer than twelve nominees proposed by the Parliamentary Committee on Standing Rules and Orders.[1903] Its core functions are set out in section 249 of the Zimbabwe Constitution as follows:

a) to uphold, promote and develop freedom of the media;
b) to promote and enforce good practices and ethics in the media;
c) to monitor broadcasting in the public interest and, in particular, to ensure fairness and diversity of views broadly representing Zimbabwean society;
d) to encourage the formulation of codes of conduct for persons employed in the media and, where no such code exists, to formulate and enforce one;
e) to receive and consider complaints from the public and, where appropriate, to take action against journalists and other persons employed in the media or broadcasting who are found to have breached any law or any code of conduct applicable to them;
f) to ensure that the people of Zimbabwe have fair and wide access to information;
g) to encourage the use and development of all the officially recognised languages of Zimbabwe;

[1901] Scanlen & Holderness v Zimbabwe, Case No. 297/2005, decided 3 April 2009; the case is analysed by Global Freedom of Expression here.
[1902] Section 41 of the Freedom of Information Act preserved regulations made under the repealed law the extent that they could have been made under the appropriate provisions of the new law – but the Freedom of Information Act makes no provision for accrediting journalists or registering media services and news agencies. "AIPPA Resurrected : New Media Accreditation & Registration Fees Gazetted", Commissions Watch: Zimbabwe Media Commission. 1 February 2021; "Zimbabwe: 2022 Media Accreditation Fees Gazetted", *The Herald*, 2 April 2022
[1903] [1903] Zimbabwe's 2013 Constitution, as amended through 2017, section 248.

h) to encourage the adoption of new technology in the media and in the dissemination of information;
i) to promote fair competition and diversity in the media; and
j) to conduct research into issues relating to freedom of the press and of expression, and in that regard to promote reforms in the law.[1904]

The **Zimbabwe Media Commission Act, 2020 [*Chapter 10:35*]** gives the Commission these additional powers:

(a) to monitor and secure compliance with any –
(i) law which regulates media practitioners and media services including broadcasting, print and electronic media, in order to ensure respect for the rights protected by section 61 of the Constitution [on freedom of expression and freedom of the media];
(ii) international treaty to which Zimbabwe is a party with respect to the protection, promotion or advancing of people's rights in relation to the media in Zimbabwe;

(b) to collaborate and co-operate with other independent constitutional Commissions in supporting and entrenching human rights and democracy.[1905]

The Commission is also empowered to consider complaints from any person alleging a violation of the right to freedom of expression, and "on its own motion, investigate or inquire into any action on the part of any person that constitutes, or is likely to result in, a violation of any of the rights protected under section 61 of the Constitution".[1906] Where the Commission finds a violation of section 61 rights, it is empowered to order various forms of redress – including compensation to aggrieved persons, orders that decisions or practices resulting in the violation must be stopped, reversed or altered, and recommendations that any law on which the offending action was based should be reconsidered. It can also pursue an action in court to redress such a violation.[1907]

Broadcasting in Zimbabwe is regulated by the **Broadcasting Services Act, 2001 [*Chapter 12:06*]**, which creates a Broadcasting Authority of Zimbabwe (BAZ) appointed by the relevant minister after consultation with the President,[1908] and the minister has the power to give policy directions to the Board.[1909] BAZ issues licences for radio and television broadcasting[1910] and is tasked with developing broadcasting codes of conduct.[1911] All licensees have a duty to "provide sufficient coverage of national events" - which means any "event or occasion which is declared to a national event by the minister by notice in the Government Gazette – and a duty,

[1904] Id, section 249.
[1905] Zimbabwe Media Commission Act, 2020 [*Chapter 10:35*], section 4.
[1906] Id, section 8.
[1907] Id, sections 12 and 15.
[1908] Broadcasting Services Act, 2001 [*Chapter 12:06*], section 4.
[1909] Id, section 4B.
[1910] Id, Part III.
[1911] Id, section 24.

when providing an information service, to "provide a fair, balanced, accurate and complete service".[1912] No broadcaster may broadcast any matter that contains "false or misleading news";[1913] it appears that violation of this condition could be a basis for suspension or cancellation of the broadcasting licence.[1914]

The Zimbabwean Broadcasting Corporation (ZBC), which operates as a state broadcaster, is governed by a board appointed by a Minister, under the **Zimbabwe Broadcasting Corporation Act, 2001 [*Chapter 12:01*]**, which is set to be replaced by the **Zimbabwe Broadcasting Corporation (Commercialisation) Act, 2001**.[1915]

The **Postal and Telecommunications Act, 2000 [*Chapter 12:05*]** establishes the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) which licenses and regulates postal and telecommunication services, including internet service licences.[1916] The Board of POTRAZ is appointed by the relevant minister after consultation with the President,[1917] and the minister has the power to give policy directions to the Board.[1918] The minister is also empowered, after consultation with the President, to direct the Board to reverse, suspend or rescind its decisions or actions if the minister considers on reasonable grounds that a decision or action "is not in the national or public interest or the interests of consumers or licensees as a whole".[1919]

According to Freedom House, "POTRAZ is expected to operate independently, but in practice its independence has been questioned over the years, as it has become increasingly subordinated to state security agencies". Freedom House also states that POTRAZ was largely seen as having supported and enabled the infamous Government directive to suspend Internet services in 2019 (discussed below).[1920]

The Postal and Telecommunications Act has a few content-based offences. It is a criminal office to send by post any "indecent or obscene article", or any postal article containing any word or other content "of an indecent, obscene, seditious, scurrilous, threatening or grossly offensive character".[1921] It is also an offence to use a telephone for any message that is "grossly offensive or is of an indecent, obscene or threatening character", or any message that the sender knows to be false "for the purpose of causing annoyance, inconvenience or needless anxiety to any other person". In addition, it is an offence to make any telephone call "without reasonable cause for the purpose of causing annoyance, inconvenience or needless anxiety".[1922]

[1912] Id, section 39.
[1913] Id, Fifth Schedule (section 11(1)(b)), Standard Conditions of Licences, item 7. This provision is contained in a section on political matters and medicines. but it is worded generally.
[1914] Id, sections 11(1) and 16(1)(b).
[1915] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 16: Zimbabwe", Konrad Adenauer Stiftung, 2021, pages 229-ff.
[1916] Postal and Telecommunications Act, 2000 [*Chapter 12:05*].
[1917] Id, section 5.
[1918] Id, section 25.
[1919] Id, section 26.
[1920] "Freedom on the Net 2022: Zimbabwe", Freedom House, section A5.
[1921] Postal and Telecommunications Act, 2000 [*Chapter 12:05*] section 84.
[1922] Id, section 88.

Zimbabwe's constitutional provisions are strong, with a sound basis for limited restrictions on the right to freedom of expression that incorporates necessity and proportionality.[1923] The constitutional protections have been applied in practice to invalidate specific legislative provisions.

In 2014, the Constitutional Court of Zimbabwe relied on the constitutional protection for freedom of expression (under Zimbabwe's previous constitution) to declare the offence of criminal defamation unconstitutional in the *Madanhire* case. The case concerned charges of criminal defamation against a journalist and an editor after the publication of an article critical of a medical aid company. The relevant statute was section 96 of the Criminal Law Code, which made dissemination of false information with intent to cause harm to the reputation of another person punishable by a fine or a maximum of two years imprisonment. Although the Court found the law to be rationally related to the important objective of protecting the reputation, rights and freedoms of others, it found that the criminalization of defamatory statements lacked proportionality and was not a necessary means to protect reputation. The Court also noted that criminal sanctions for the publication of inaccurate or erroneous statements had the inherent effect of silencing the free flow of information on public matters. It viewed the monetary damages for of civil defamation as a more appropriate way to protect reputation.[1924] In 2016, the Constitutional Court affirmed that section 96 of the Criminal Law Code is equally void under Zimbabwe's current Constitution, in the case of *MISA-Zimbabwe v Minister of Justice*.[1925]

Section 50(2)(a) of the Law and Order (Maintenance) Act, 1960 (which is no longer in force) previously made it an offence to make, publish or reproduce any "false statement, rumour or report which (a) is likely to cause fear, alarm or despondency among the public or any section of the public or (b) is likely to disturb the public peace". In 2000, in the *Chavunfuka* case, the Supreme Court of Zimbabwe declared the provision unconstitutional (under the previous Zimbabwe Constitution). The case followed on the arrest of the author of a 1999 article describing a failed *coup d'etat* and the subsequent arrest of twenty-three soldiers. The article claimed that the insurrection was inspired by dissatisfaction with the mismanagement of the economy and Zimbabwe's involvement in war in the Democratic Republic of the Congo. The editor of the publication where the article appeared was also arrested. The Supreme Court found that the provision in questions did not constitute a justifiable limitation of the freedom of expression because it was too vague and arbitrary to be qualify as a restriction imposed under the authority of law. The following were relevant factors:

- the provision not only criminalised statements that *actually* caused fear, alarm or despondency, but also statements that were *likely* to do so; the law required no proof of any damage to the state or impact on the public;
- given that the relevant provision was concerned with *likelihood* rather than *reality,* it was too vague to give clear guidance and could thus discourage

[1923] Zimbabwe's 2013 Constitution, as amended through 2017, sections 61 and 86 (quoted in the table at the beginning of this chapter).
[1924] Madanhire & Another v AG (Judgment No CCZ 2/14, Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); see the summary of case by Global Freedom of Expression here.
[1925] MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.

expression by persons wary of prosecution;
- the expression "fear, alarm or despondency" was overbroad since anything that is newsworthy is likely to cause some of these emotions in some members of the public;

- the use of the word "false'" was too wide, because it covered inaccurate statements, rumours or reports as well as intentional lies, and the law does not require actual knowledge of the statement 's falsity to impose liability; thus, the law criminalises negligence.

The entire law was later replaced by the **Public Order and Security Act, 2002**, which includes no comparable provision.[1926]

In 2021, the Constitutional Court ruled in the *Chimakure* case that **section 31(a)(iii) of the Criminal Law (Codification and Reform) Act** was invalid in terms of the previous Constitution. Two journalists were charged with violating this provision, which made the **reporting of false news that would undermine public confidence in the uniformed forces** punishable with a significant fine and a prison sentence of up to twenty years. Their publication had accused intelligence and police officials of involvement in the abduction of opposition and human rights activists in 2008. The Court issued an initial order stating that the provision restricted freedom of expression as protected under the previous Constitution, and the State failed to put forward reasons to show that the restriction was justifiable – with the effect being that the provision in question was declared void.[1927] (The other prohibitions on false news in section 31 of this Act remain in force and are discussed below.)

In 2019, on the second day of a stay-away called by the Zimbabwe Congress of Trade Unions, the Minister of State in the President's Office for National Security issued **a directive under section 6 of the Interception of Communications Act ordering the suspension of all** *internet services – which effectively also shut down* email services and social media platforms. The directive was challenged by three individual journalists and MISA Zimbabwe, who asserted (amongst other things) that the Act did not give authority to the Minister of State to issue directives (since the President had reserved administration of the Act to himself under a statutory instrument issued in terms of the Act), that section 6 of the Act did not authorise a blanket suspension of Internet services and that section 6 violated the constitutional protection for freedom of expression, producing disproportionate disruption of services and loss of income to ordinary citizens and businesses. The government defended its actions on the basis of national security, asserting that the Internet shutdown was aimed at preventing violence and illegal activity. The Court invalidated the directive to suspend Internet services on the narrow basis that it had not been issued by the President, without reaching the broader constitutional issues.[1928]

[1926] Chavunfuka v Minister of Home Affairs 2000 JOL 6540 (ZS); see the summary of the case by Global Freedom of Expression here.
[1927] Chimakure v Attorney-General of Zimbabwe (Judgment No. CCZ 6/201411, Const. Application No. CCZ 247/09), 22 July 2014; see the analysis of the case by Global Freedom of Expression here.
[1928] Zimbabwe Lawyers for Human Rights v. Minister of State, National Security, HC 261/19, 21 January 2021. See Veritas, "Court Watch: Internet Shutdown Case – High Court's Ruling", as published in The Zimbabwean, 1 February 2019; "High Court sets aside internet shut down directives", MISA-Zimbabwe. 21 January 2019; "Freedom on the Net 2022: Zimbabwe", Freedom House, section B3; and case analysis by Global Freedom of Expression here.

It appears noteworthy that the Constitution specifically protects "the confidentiality of journalists' sources of information",[1929] but Reporters Without Borders reports that the confidentiality of sources is not actually respected in practice.[1930]

18.3 CASE STUDIES

The 2022 Bertelsmann Transformation Index provides this overview of shrinking civic space and violence and harassment against journalists in recent years:

> *In the past two years, the hope for positive change in Zimbabwe after the departure of former President Robert Mugabe has been effectively dashed. Under President Emmerson Mnangagwa's "new dispensation" many of the country's challenges remained unaddressed or even intensified. Zimbabwe's multi-faceted crisis was further exacerbated by this and the impact of COVID-19. Its continued economic decline was characterized by high prices, cash shortages and a huge debt overhang. The phased reintroduction of the Zimbabwe dollar led to record inflation, which peaked at over 700% in July 2020 and nearly eradicated the income of many Zimbabweans. The economic decline resulted in a severe humanitarian crisis, with over seven million Zimbabweans in need of food aid at the end of 2020, according to the U.N.*
>
> *Of particular concern in the past two years have been the further shrinking of democratic space and the failure to uphold constitutionalism. The January 2019 crackdown by the state security apparatus, which responded with disproportionate force to protests over poor living conditions, was followed by two years of increased repression against opposition members, activists, journalists and other actors. The most notable cases were the abduction, torture, sexual abuse and subsequent arrest of three female opposition leaders in 2020 and the repeated arrest and detention of prominent journalist Hopewell Chin'ono after he had exposed government corruption. The government's systematic repression made use of an increasingly partisan judiciary, which led to lengthy pretrial detentions of opposition members, activists and journalists. These arrests have led to further polarization of the political domain and to a continued stalemate between the ZANU-PF (Zimbabwe African National Union-Patriotic Front) and the MDC Alliance, which also negatively affected the prospects for a much-needed national dialogue process.*[1931]

According to Reporters without Borders, "levels of violence against journalists have declined significantly under the Mnangagwa administration" but still remain alarmingly high, meaning that self-censorship is routinely practiced to avoid reprisals. It is also reported that police often use disproportionate force against journalists and confiscate their equipment. Intimidation, verbal attacks and threats (especially on social media) are also common practices. Cases of journalists being imprisoned and

[1929] Id, section 61(2).
[1930] "2023 World Press Freedom: Zimbabwe", Reporters Without Borders, "Legal Framework".
[1931] "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".

prosecuted are more rare than in the past, but journalists' phone communications are often subject to surveillance.[1932]

In 2022, Freedom House reported that "[b]oth journalists and ordinary users continued to face arrest and harassment for their online activities, particularly those that criticize President Emmerson Mnangagwa's government."[1933]

Amnesty International reports that three journalists were the first persons to be arrested under the **Criminal Law Codification and Reform Act , as amended by the Cyber and Data Protection Act,** in 2022. The first two to be arrested were editor Wisdom Mdzungairi and senior reporter Desmond Chingarande. After publishing a news story on a private business enterprise allegedly operated by individuals with government connections, they were charged with **transmitting "false data intending to cause harm"**. Freelance sports journalist Hope Chizuzu was arrested on the same charge after board members of the Dynamos Football Club filed a complaint against him. Police reportedly confiscated his mobile phone and iPad for the purpose of further investigations.[1934]

Other arrests have been based on **cyberbullying**. In May 2022, Raymond Chari was reportedly charged with cyberbullying in violation of **section 164B of the Criminal Law Codification and Reform Act, as amended in the Cyber and Data Protection Act** for allegedly using foul language to describe the Zimbabwean ambassador to Tanzania and his wife in a WhatsApp group. Also in May 2022, television actor David Kanduna was reportedly fined for cyberbullying after he posted a video to WhatsApp and Tik Tok which showed an incident at a local university where a police officer was heckled.[1935]

The **Criminal Law (Codification and Reform) Act** has been the basis of numerous arrests for offences related to expression:

- In August 2022, editor Wisdom Mdzungairi and senior reporter Desmond Chingarande were charged with **publishing false data messages intending to cause harm in contravention of section 164C of the Criminal Law (Codification and Reform) Act, as amended by the Cyber and Data Protection Act**. The charge stemmed from a news story alleging that a local cemetery was being run without government approval.[1936]
- In January 2021, Vongai Chiminya and Devine Panashe Maregere were charged with **communicating false statements prejudicial to the State in violation of section 31(a)(i) of the Criminal Law (Codification and Reform) Act** for sending an audio message to a WhatsApp group claiming that President Mnangagwa had died from COVID-19. Neither Chiminya nor Maregere were

[1932] "2023 World Press Freedom: Zimbabwe", Reporters Without Borders. "Safety".
[1933] "Freedom on the Net 2022: Zimbabwe", Freedom House, "Overview".
[1934] Amnesty International Report 2022/23, "Zimbabwe 2022"; "Zimbabwean journalist Hopewell Chin'ono denied bail", Reporters Without Borders, 12 November 2020.
[1935] Freedom on the Net 2022: Zimbabwe", Freedom House, section C3; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.
[1936] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023; "Journalists charged with publishing false data messages", African Freedom of Expression Exchange, 6 August 2022.

the original creators of the audio message, and there was reportedly no evidence that sharing the message cause any public harm.[1937]

- In April 2020, an opposition politician, Chrispen Rambu, was charged under section 33 of the **Criminal Law (Codification and Reform) Act** for calling President Mnangagwa a fool in a WhatsApp message. Two other persons, Robert Zakeyo and Admire Mupemhi, were charged the **undermining the authority of the President in violation of section 33(2)(b) of the Criminal Law (Codification and Reform) Act** for sharing a video clip on which criticised President Mnangagwa's economic policies and referred to him as a frog. Another man, Goodman Musariri, was also arrested in April 2020 for **undermining the authority of the President in violation of this provision**, for a WhatsApp message saying that President Mnangagwa had nothing to offer the country and so should resign.[1938]
- In April 2020, Lovemore Zvokusekwa was arrested and charged for **publishing or communicating false statements prejudicial to the state under section 31 of the Criminal Law (Codification and Reform) Act**. on the basis that he had instigated a rumour about a planned extension of the COVID-19 lockdown by 13 days, which the president later denied. State authorities claimed that the rumour was causing public distress and unrest, and that it posed a threat to public health. However, the rumour later proved to be true when the lockdown was in fact extended.[1939]
- Prominent journalist Hopewell Chin'ono (winner of CNN's African Journalist of the Year award in 2008) was arrested in January 2021, for **publishing false information** for a statement on Twitter that a police officer had beaten a child to death while enforcing COVID-19 restrictions. He was granted bail, once again subject to limits on his Twitter usage. These charges were thrown out in April 2021, when **section 31(a)(iii) of the Criminal Law (Codification and Reform) Act was ruled unconstitutional.**[1940]

There have been internet shutdowns in Zimbabwe in recent years. In January 2019, a total **internet shutdown** was ordered by a warrant issued pursuant to the Interception of Communications Act – which (as discussed in more detail below) provides for the interception of telecommunications to fight crime and protect national security. It defines interception as "to listen to, record, or copy" a communication. The law makes no reference to blocking or disrupting communication services. In 2016, the government disrupted Internet-based communications without referring to the Interception of Communications Act. On that occasion, there was a partial shutdown for about four hours that targeted social media websites.[1941]

[1937] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[1938] Freedom on the Net 2022: Zimbabwe", Freedom House, section C3.
[1939] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[1940] Id. Chin'ono has been repeatedly arrested under various laws for his online reporting activities. for instance, in July 2020, he was charged with **incitement to violence** in connection with photos and videos anti-government protests posted on Twitter, with some speculating that his arrest could have been a consequence of series of Facebook posts alleging that the president's son was involved in corrupt business dealings related to government contracts for medical supplies. Chin'ono was released on bail in September 2020, but banned from using social media for his activism as part of his bail conditions. In November 2020, Chin'ono was arrested for violating his bail conditions with a Twitter post about the initial denial of bail in his case. He was granted bail again in November 2020, on the condition that he would not anything on Twitter that would "obstruct justice."
[1941] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 8.

Problematic government attitudes are illustrated by some of the statements that have been reported in recent years. A presidential spokesperson stated that the 2017 creation of a new Ministry of Cyber Security, Threat Detection and Mitigation was aimed at catching mischievous elements using social media.[1942] Freedom House reports that President Mnangagwa has referred to online campaigns against human rights abuses and corruption as "a cyber-war on our country in pursuit of a regime change agenda."[1943] In November 2021, the Minister of Information, Publicity, and Broadcasting Services announced that the government had set up a "cyber-team" for the purpose of monitoring social media.[1944] It is reported that, in April 2022, the Permanent Secretary for the Ministry of Information suggested enactment of a law that criminalizes "campaigning against one's own country," following an address by journalist Hopewell Chin'ono on the state of human rights in Zimbabwe at a summit in Geneva.[1945] It all points to concerns that criticisms of government will not be tolerated.

18.4 CYBERCRIME LEGISLATION AND OTHER LEGAL PROVISIONS RELEVANT TO FREEDOM OF EXPRESSION

A) CRIMINAL LAW (CODIFICATION AND REFORM) ACT [CHAPTER 9:23] AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 [CHAPTER 12:07]

The Cyber and Data Protection Act was previously called the Data Protection Act. Its title was changed when the law was amended in February 2022.[1946] One analysis notes that this law "borrows extensively from the SADC Model Law; and "also leans heavily towards the Tanzanian Cybercrime Act".[1947]

The wisdom of combining cybersecurity and data protection in one law, under one consolidated regulatory authority has been questioned.[1948] However, in fact, the substantive provisions on cybercrimes are all actually contained in the **Criminal Law (Codification and Reform) Act *as amended by* the Cyber and Data Protection Act,**[1949] with the Cyber and Data Protection Act itself being exclusively a data protection law.

[1942] Malvern Mkudu, "Policy Brief: Zimbabwe's Cyber Crime and Cyber Security Bill 2017", 2018.
[1943] Id, section B8, citing "Zimbabweans unfazed by cyber attacks", *The Herald*, 28 August 2020.
[1944] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.
[1945] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4.
[1946] This law replaced sections 163-166 of the Criminal Law (Codification and Reform) Act [Chapter 9:23] with new provisions, added new provisions to the Criminal Procedure and Evidence Act [Chapter 9:07] and amended the Interception of Communications Act [Chapter 11:20].
[1947] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 32.
[1948] "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 35; "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 33.
[1949] Criminal Law (Codification and Reform) Act [*Chapter 9:23*] as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]. section 35.

(The Criminal Law (Codification and Reform) Act is the current version of Zimbabwe's general penal code.)

The procedural issues relating to cybercrime are all contained in the **Criminal Procedure and Evidence Act *as amended by* the Cyber and Data Protection Act**[1950] and in the **Interception of Communications Act *as amended by* the Cyber and Data Protection Act.**[1951] Some of these laws also have provisions pre-dating the Cyber and Data Protection Act that could compromise freedom of expression.

The computer-dependent offences are listed in the following table. One shortcoming with almost all of these offences (with the exception of section 165E) is that they fail to make provision for lawful justification, such as acting in good faith in the public interest or testing for security vulnerabilities.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 - TECHNICAL OFFENCES	
Section 163: Hacking	It is an offence for a person who knows or suspects that he or she must obtain prior authority to access data, a computer programme, a computer data storage medium, or the whole or any part of a computer system, to secure such access intentionally, unlawfully and without such authority. o To "secure access" "includes - (a) to obtain, to make use of, gain entry into, view, display, instruct or communicate with, or store data in or retrieve data from; (b) to copy, move, add, change or remove data, critical data or a critical database, or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network, a critical information infrastructure, whether in whole or in part, including their logical, arithmetical, memory, access codes, transmission, data storage, processor or memory function, whether physical, virtual, by direct or indirect means or by electronic, magnetic, audio, optical or any other means." (section 163(2)) o This description helpfully narrows the offence beyond just logging onto a computer or computer system without authorisation.
Section 163A: Unlawful acquisition of data	It is an offence to unlawfully and intentionally - • intercept by technical or any other means any private transmission of computer data to, from or within a computer network, computer device, database or information system or electromagnetic emissions from a computer or information system carrying such computer data; • overcome or circumvent any protective security measure intended to prevent access to data;

[1950] Criminal Procedure and Evidence Act [*Chapter 9:07*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 36.
[1951] Interception of Communications Act, 2007 [*Chapter 11:20*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 37.

	• acquire data within a computer system or data which is transmitted to or from a computer system. o For the purposes of this offence, "acquire" includes "to use, examine, capture, copy, move to a different location or divert data to a destination other than its intended location". o The offence does *not* appear to apply to the use of data unlawfully acquired from a computer system by another person (as in the case of journalistic use of Wikileaks material).
Section 163B: Unlawful interference with data or data storage medium	It is an offence to unlawfully and intentionally interfere with computer data or a data storage medium by - • damaging, corrupting, impairing or deteriorating computer data; • deleting computer data; • altering computer data; • rendering computer data meaningless, useless or ineffective; • obstructing, interrupting or interfering with the lawful use of computer data; • obstructing, interrupting or interfering with any person in the lawful use of computer data; • denying, hindering, blocking access to computer data to any person authorised to access it; or • maliciously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer.
Section 163C: Unlawful interference with computer system	It is an offence to unlawfully and intentionally interfere with the use of a computer or information system, a computer device, an electronic communications system or critical information infrastructure by blocking, hindering, impeding, interrupting, altering or impairing access to it, or its functioning or integrity.
Section 163D: Unlawful disclosure of data code	It is an offence to unlawfully and intentionally - • communicate, disclose or transmit any computer data, programme, access code or command or any other means of gaining access to any programme or data held in a computer or information system to any person not authorised to access the computer data, programme, code or command for any purpose; • activate, install or download a programme that is designed to create, destroy, mutilate, remove or modify any data, programme or other form of information existing within or outside a computer or computer system; • creates alter or destroy a password, personal identification number, code or any method used to access a computer or computer network. The offence applies regardless of whether the intended effect of the illegal interference is permanent or temporary. There is provision for an enhanced penalty where this offence is committed in relation to data that forms part of a database, or involves national security or the provision of an essential service. There is an exception for actions "authorised under the law" or "pursuant to measures that can be taken in terms of section 39".

	○ It is unclear what is covered by the exception that references "section 39". Section 39 of the Criminal Law Code concerns dealing in or possession of prohibited knives, and there is no section 39 in the Cyber and Data Protection Act. Thus, the import of this exception cannot be assessed.
Section 163E: Unlawful use of data or devices	It is an offence to unlawfully and intentionally acquire, possess, produce, sell, procure for use, import, distribute, supply, use or make available an access code, password, a computer programme designed or adapted for the purpose of committing an offence, or any similar data or device by which the whole or any part of a computer or information system is capable of being accessed, for purposes of the commission or attempted commission of an offence in terms of this Act. It is also an offence to unlawfully and intentionally assemble, obtain, sell, purchase, possess, make available, advertise or use malicious software, programmes or devices for purposes of causing damage to data, computer or information systems and networks, electronic communications networks, critical information infrastructure or computer devices. ○ The title of this offence is somewhat misleading since it does not cover data in the simplest sense of the term, but only applies to access codes, passwords, computer programmes and malicious software. ○ The criteria that the items covered must be for the purpose of committing an offence, or for causing damage, keeps the offence appropriately narrow.
Section 163F: Aggravating circumstances	The aggravating circumstance listed in this section warrant enhanced penalties for all of the offences listed here except for section 163D which lists its own basis for enhanced penalties. It is an aggravating circumstance where the offence - • was committed in connection with a crime against the State specified in Part III of the Criminal Law (Codification and Reform) Act; • was intended for or results in damaging, destroying or prejudicing the safe operation of an aircraft; • was intended to conceal or disguise the proceeds of unlawful dealing in or partaking of dangerous drugs • results in defeating or obstructing the course of justice; • seriously prejudices the enforcement of the law by any law enforcement agencies; • involved any computer, computer network, information communications network data, programme or system owned by the State, a law enforcement agency, the Defence Forces, the Prison Service, a statutory corporation or a local authority; • results in considerable material prejudice or economic loss to the owner of the computer, computer network, data, programme or system; • seriously interferes with or disrupts an essential service; • was committed in furtherance of organised crime or the perpetrator was part of an organised criminal gang. ○ The enhancement of penalties where cybercrimes are committed in connection with crimes against the State listed in Part III of the Criminal

	Law (Codification and Reform) Act covers a number of offences that unreasonably compromise freedom of expression (sections 30, 31 and 33, all discussed below).

As in other SADC countries, it is the content-based offences which are the most problematic for freedom of expression. The offences described in the table below were introduced into the law by the Cyber and Data Protection Act.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT AS AMENDED BY THE CYBER AND DATA PROTECTION ACT, 2021 - CONTENT-BASED OFFENCES	
Section 164: Transmission of data message inciting violence or damage to property	It is an offence to unlawfully by means of a computer or information system make available, transmit, broadcast or distribute a data message to any person, group of persons or the public with intent to incite such persons to commit acts of violence against any person or persons or to cause damage to any property. o According to MISA-Zimbabwe: "Provisions such as these are at risk of being relied on to inhibit constructive criticism which is important for promoting transparency and accountability especially from the government. There is therefore a danger that such provisions will be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. This will potentially stifle citizen engagement and open debate, both of which are necessary elements to promote democracy."[1952] o Another assessment states that this provision "can easily be used to inhibit constructive criticism, which is important for promoting transparency and accountability especially from the government. In a context of polarized politics and retribution, such provisions can be used as political tools and mechanisms by the state to prevent the expression of dissenting opinions. In the end, such a provision can contribute immensely towards stifling citizen engagement and open debate, which are essential building blocks for electoral and constitutional democracy."[1953]
Section 164A: Sending threatening data message	It is an offence to unlawfully and intentionally by means of a computer or information system send any data message to another person threatening "harm" to the person or the person's family or friends or damage to the property of such persons. This section includes an additional offence that appears to be misplaced. It is an offence for any person to "up skirt" and record nude images or videos of a citizen, or a foreigner who is resident in Zimbabwe, without consent.

[1952] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)
[1953] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.

	○ Note that the formulation of the first offence covers messages sent via social media. ○ The first offence should be limited to threats of "physical harm", so as not to be confused with reputational harm. It otherwise amounts to a reintroduction of criminal defamation, which has been declared unconstitutional.[1954] ○ Although not the subject of this paper, it is curious that the second offence provides no protection for the invasion of the privacy of non-residents.
Section 164B: Cyber-bullying and harassment	This offence has been used to inhibit freedom of expression in practice and so is quoted in full. Any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment. ○ MISA Zimbabwe notes that this offence criminalises not only the generation but also the communication of such offensive messages through any electronic medium, which includes social media. [1955] ○ The intentionality required for this offence is low and vague, with key terms such as "harass", "bully" and "substantial emotional distress" left undefined. ○ The potential term of imprisonment is extremely disproportionate, given that any imprisonment for an offence based entirely on expression is widely considered to be inappropriate.
Section 164C: Transmission of false data message intending to cause harm	This is another overbroad offence that has been used to inhibit freedom of expression in practice, quoted here in full. Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend [sic] to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment. ○ The fact that this offence is committed if there is an intent to cause either "psychological or economic harm" makes it very likely to inhibit reports of wrongdoing, since allegations of corruption or abuse of government power may not be known to be fully "true" until adjudicated.

[1954] See section 13.2 above.
[1955] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023).

	○ It appears that this offence might be committed even if a report is substantially true, and there is no exception for fair comment in the public interest. ○ This offence also appears to reintroduce of criminal defamation, which has been declared unconstitutional.[1956] ○ As in the case of offence above, the potential term of imprisonment is extremely disproportionate, given that any imprisonment for an offence based entirely on expression is widely considered to be inappropriate. ○ According to one analysis: "It is not clear how it would be determined whether a message was "false" or the scope of "psychological or economic harm". Additional guidance is also needed on whether this provision applies to legal or natural persons. Section 164C therefore fails to provide clear guidance for individuals and provides an overly wide degree of discretion to those charged with the enforcement of this law.[1957] ○ Another analysis also highlights the complexities of distinguishing truth from falsehood in this context: "This clause ignores the fact that there are multiple truths and various regimes of truth and non-truth. Even more important it ignores the fact that on the internet and social media platforms it difficult to determine the origin and authenticity of a message. In such an environment, individuals are exposed to communication messages voluntarily or involuntarily. In a context, where a culture of citizen journalism and blogging has taken route, this provision can be abused to implicate thousands of ordinary citizens who would have 'received' and communicated such messages."[1958]
Section 164D: Spam	It is an offence to "intentionally and without lawful excuse" – • to use a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead recipients or any electronic mail or internet service provider as to the origin of such messages; • to materially falsifies header information in multiple electronic mail messages and initiate the transmission of such messages.
Section 164E: Transmission of intimate images without consent	It is an offence to unlawfully and intentionally by means of a computer or information system make available, broadcast or distribute a data message containing any intimate image or video of an identifiable person without the consent of the person concerned or with recklessness as to the lack of consent of the person concerned, with the aim of causing the humiliation or embarrassment of such person. An 'intimate image" for this purpose is a "visual depiction of a person made by any means in which the person is nude, the genitalia or naked female breasts are exposed or sexual acts are displayed". ○ The fact that the offence requires an aim of causing humiliation or embarrassment should protect persons who send such images for legitimate purposes, such as in genuine artistic material.

[1956] See section 13.2 above.
[1957] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
[1958] "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.

Section 164F: Production and dissemination of racist and xenophobic material	It is an offence "unlawfully and intentionally through a computer or information system - • to produce racist or xenophobic material for the purpose of its distribution (or to cause this to happen); • to offer, make available or broadcast racist or xenophobic material (or to cause this to happen); • to distribute or transmit racist or xenophobic material (or to cause this to happen); • to use language that tends to lower the reputation or feelings of persons for the reason that they belong to a group of persons distinguished on the grounds set out in section 56(3) of the Constitution or any other grounds whatsoever, if used as a pretext for any of these factors. o Racist or xenophobic material" is not defined. The final point appears very broad and vague, since it appears to cover hurt feelings. However, it appears consistent with the provisions on hate speech in the Malabo Convention and the SDC Model Law on cybercrime which both cover "insult". Some laws criminalise hate speech only where it incites hatred, discrimination or violence on the prohibited grounds.
Section 164G: Identity-related offence	There seems to be an error in the law as this offence is almost identical to section 164B on cyberbullying and cyber harassment. (Several online versions were accessed, and all had the same version of section 164G.) The only substantive difference is that this provision states that special consideration must be given to a child who is found guilty of this offence, who must not be sentenced to imprisonment or acquire a criminal record as a result.
The amendments to the Criminal Law (Codification and Reform) Act also contain offences relating to - • the non-consensual recording of the genitalia and buttocks beneath clothing, or the sharing of such images by means of a data message (section 165) • child sexual abuse material [i.e., child pornography] and grooming of a child (section 165A) • exposing children to pornography for the purpose of grooming (section 165B). These offences do not appear to pose any problems, as they appear to limit freedom of expression in justifiable ways.	

Amnesty International has warned that the new offences have been used to intimidate and harass journalists for doing their work and threaten to further curtail media freedom in Zimbabwe.[1959]

According to Dr. Allen Munoriyarwa, a senior media studies lecturer at the University of Botswana, the insertion of some of the content-based 'new offences' was "deliberate to try and balance public demands with the political survival" of the ruling party.[1960] Munoriyarwa stated that on the one hand the politicians realise that they have to legislate on issues in the public interest, such as dealing with online harms, but on the other they then also exploit these law making processes to create laws that can be used for

[1959] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
[1960] Dr Allen Munoriyarwa was interviewed via Zoom on 25 July 2023.

repressive purposes because such laws "give them ways of deploying surveillance capabilities".

Some worrying content-based offences in Part III of the Criminal Law (Codification and Reform) Act ("Crimes against the State") pre-date the Cyber and Data Protection Act and remain in force. One small safeguard is that prosecution for any of the offences listed in the table below requires authorisation from the Attorney General,[1961] but this is not sufficient to overcome the freedom-of-expression concerns and does nothing to prevent the existence of the crimes from inhibiting robust political discussion and debate.

CRIMINAL LAW (CODIFICATION AND REFORM) ACT - CONTENT-BASED OFFENCES	
Section 30: Causing disaffection among Police Force or Defence Forces	If any person who, whether inside Zimbabwe induces, or attempts to induce, or does any act with the intention or realising that there is a real risk or possibility of inducing or causing any member of the Police Force or Defence Forces to withhold his or her services, loyalty or allegiance or to commit breaches of discipline, he or she shall be guilty of causing disaffection among the Police Force or Defence Forces and liable to a fine not exceeding level seven or imprisonment for a period not exceeding two years or both. o Due to the reference to "real risk or possibility" in connection with intent, it is conceivable that this offence could capture the publication of allegations of corruption or mismanagement in the armed forces, even if (and perhaps particularly if) the allegations were true.
Section 31: Publishing or communicating false statements prejudicial to the State	Any person or outside Zimbabwe - (a) publishes or communicates to any other person a statement which is wholly or materially false with the intention or realising that there is a real risk or possibility of- (i) inciting or promoting public disorder or public violence or endangering public safety; or (ii)adversely affecting the defence or economic interests of Zimbabwe; or (iv) interfering with, disrupting or interrupting any essential service; shall, whether or not the publication or communication results in a consequence referred to in subparagraph (i), (ii), (iii) or (iv); or (b)with or without the intention or realisation referred to in paragraph (a), publishes or communicates to any other person a statement which is wholly or materially false and which - (i) he or she knows to be false; or (ii) he or she does not have reasonable grounds for believing to be true; shall, if the publication or communication of the statement- A. promotes public disorder or public violence or endangers public safety; or

[1961] Criminal Law (Codification and Reform) Act [*Chapter 9:23*], section 34.

	B. adversely affects the defence or economic interests of Zimbabwe; or C. undermines public confidence in a law enforcement agency, the Prison Service or the Defence Forces of Zimbabwe; or D. interferes with, disrupts or interrupts any essential service; be guilty of publishing or communicating a false statement prejudicial to the State and liable to a fine up to or exceeding level fourteen or imprisonment for a period not exceeding twenty years or both. ○ This provision has been frequently applied in practice to restrict freedom of speech, including online speech. ○ Paragraph (a)(iii) was found to be an unconstitutional restriction on freedom of expression, with the reasoning in the case suggesting that other aspects of the law which have not yet been challenged might also raise constitutional problems. ○ The intention in subsection (a) is very broad since it covers "realising that there is a real risk or possibility" of the indicated harms and does not require that any of the listed consequences actually resulted. Subsection (b) is conversely based on a result without requiring intention (or even recklessness) to produce that result. ○ One analysis state: "It is not clear how a statement would be determined 'wholly or materially false' or what the threshold is for deciding whether there is a 'real risk' of 'adversely affecting the defence or economic interests of Zimbabwe. Section 31 thus fails to provide clear guidance for individuals to conform their behaviour and provides an overly wide degree of discretion to those charged with the enforcement of this law."[1962]
Section 33: Undermining authority of or insulting President	(1) In this section - "publicly", in relation to making a statement, means - (a) making the statement in a public place or any place to which the public or any section of the public have access; (b) publishing it in any printed or electronic medium for reception by the public; "statement" includes any act or gesture. (2) Any person who publicly, unlawfully and intentionally - (a) makes any statement about or concerning the President or an acting President with the knowledge or realising that there is a real risk or possibility that the statement is false and that it may - (i) engender feelings of hostility towards; or (ii) cause hatred, contempt or ridicule of; the President or an acting President, whether in person or in respect of the President's office; or (b) makes any abusive, indecent or obscene statement about or concerning the President or an acting President, whether in respect of the President personally or the President's office; shall be guilty of undermining the authority of or insulting the President and liable to a fine not exceeding level six or imprisonment for a period not exceeding one year or both.

[1962] "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.

	○ MISA Zimbabwe notes that this offence criminalises not only the generation but also the communication of such offensive messages through any electronic medium, which includes social media. [1963] ○ The intentionality required for this offence is low and vague, with key terms such as "harass", "bully" and "substantial emotional distress" left undefined. The potential term of imprisonment is extremely disproportionate, given that any imprisonment for an offence based entirely on expression is widely considered to be inappropriate.
Another problematically broad content-related provision, contained in another chapter of the Criminal Law (Codification and Reform) Act, makes it an offence **to use threatening, abusive or insulting words at a public gathering** (amongst other acts) with the intention of preventing the transaction of the business for which the gathering was called, or realising that there is a real risk or possibility of this result (section 44). We have not found any examples of this provision being used in practice purely against speech. Section 95 of the Criminal Law (Codification and Reform) Act contains the offence of **criminal insult** which applies to words or conduct that seriously impairs the dignity or invades the privacy of another person, punishable by a fine not exceeding level six or imprisonment for a period not exceeding one year or both. Many of the same problems that apply to criminal defamation - which has been ruled unconstitutional – would also be relevant to criminal insult. Section 88 of the Postal and Telecommunications Act criminalises **offensive and annoying telephone calls and messages**.[1964]	

In July 2023, a new offence of **wilfully injuring the sovereignty and national interest of Zimbabwe** was added to the Criminal Law (Codification and Reform) Act, by the Criminal Law Codification and Reform Amendment Act – referred to by the Government during its discussion as the "Patriots Bill" or the "Patriotic Bill". This new offence prohibits actively taking part in a meeting, inside or outside Zimbabwe, that considers armed intervention in Zimbabwe by a foreign government, "subverting, upsetting, overthrowing or overturning the constitutional government in Zimbabwe", sanctions or a trade boycott. The penalty for some manifestations of this offence is the same as for treason, which can be punished by life imprisonment.[1965] This would constitute a wildly disproportionate sentence. The bill was widely criticised, domestically and internationally. For instance, the Southern Africa Litigation Centre comments: "The criminalisation of any communication constitutes an immediate threat to the constitutional right to freedom of expression. The vague and broad wording of the suggested provision is further appalling as it constitutes a high potential

[1963] "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)

[1964] Postal and Telecommunications Act, 2000 [*Chapter 12:05*], section 88. This provision, making it an offence to send by telephone any message that is grossly offensive, indecent, obscene or threatening, or to send a message known to be false by telephone "for the purpose of causing annoyance, inconvenience or needless anxiety to any other person". It is also an offence to make any telephone call without reasonable cause for the purpose of causing annoyance, inconvenience or needless anxiety.

[1965] Criminal Law Codification and Reform Amendment Bill [H.B. 15, 2022], clause 2 which would insert a new section 22A into the Criminal Law (Codification and Reform) Act [*Chapter 9:23*]. See section 20 of this law for the penalty for treason. Section 20 refers to the death penalty, but section 48 of the 2013 Constitution states that the death penalty may be imposed only for murder committed in aggravating circumstances. The Act was published as a bill 23 December 2022. The Bill was passed by the lower house of the National Assembly on 31 May 2023 and by the Senate on 7 May 2023. It was signed by the President on 14 July 2023. "Zimbabwe: President's signing of 'Patriotic Bill' a brutal assault on civic space", Amnesty International, 15 July 2023.

of abuse and misuse by state authorities to silence any dissent or criticism of state authorities."[1966]

Echoing these sentiments, Dr Munoriyarwa stated that the "Patriotic Bill" was "basically tailored against the people who speak up against the ruling party, it is basically an attempt to stifle opposition" and that it was also "tailored against activists, tailored against the journalists. You don't know what to write and you don't know what not to write" as "anything can be damaging of the national interest". Munoriyarwa was of the opinion that the "Patriotic Bill" was timed to be in place for deployment ahead of the August 2023 elections.

As can be seen, Zimbabwean law provides a host of broad, vague and overlapping offences that criminalise freedom of expression. It is highly doubtful that all of these provisions satisfy the international criteria for legitimate restrictions on freedom of expression.

B) INVESTIGATION TOOLS AND STATE SURVEILLANCE

The **Cyber and Data Protection Act** introduces new procedural provisions in the form of amendments to the Criminal Procedure and Evidence Act.[1967]

Search and seizure of computer-related items require judicial authority (from a magistrate) and must involve the investigation of a specific offence. A police officer who has a warrant can direct a service provider to **preserve relevant data** [1968] There is also provision for a **preservation** order in respect of traffic data, on judicial authority (from a magistrate).[1969]

There are also new **take-down provisions**. In terms of section 379C(3), a service provider is not criminally liable for information stored at the request of a user of the service if the hosting provider promptly removes or disables access to the information *after receiving an order from any court of law* to this effect, Alternatively, if the service provider becomes aware of any illegal information in any other manner, that service provider can avoid criminal liability *by promptly informing "the appropriate authority" which can evaluate the nature of the information and if necessary, issue an order for its removal*.[1970] This provision is a positive one in that it does not place the decision-making power in the hands of the service provider. Presumably no final order would be issued by a court or any other authority without providing the person who posted the data a chance to state his or her case. Section 379C(9), relating to internet service providers who enable access to information provided by a third person by providing an electronic hyperlink, takes a similar approach.[1971] There are criminal penalties for

[1966] "'Patriotic Bill' is a threat to democracy and the future of Zimbabwe", Southern Africa Litigation Centre, 8 June 2023. See also, for example, Columbus Mavhunga, "Amnesty International to Zimbabwe Leader: Don't Sign 'Patriotic Act' Into Law", *VOA News*, 9 June 2023; Columbus Mavhunga, "Zimbabwe Opposition, Rights Groups Bemoan Passing of 'Patriotic Bill'", *VOA News*, 9 June 2023.
[1967] Criminal Procedure and Evidence Act [*Chapter 9:07*].
[1968] Id, section 379A, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[1969] Id, section 379B, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[1970] Id, subsection 379C(3), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[1971] Id, subsection 379C(9), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].

service providers who fail to comply with orders issued under these two subsections.

However, these provisions appear to be undermined by section 379C(11), which places an even heavier penalty on any service provider who "knowingly enables access to, stores, transmits or provides an electronic hyperlink to, any information with knowledge of the unlawfulness of the content of any such information";[1972] it is not clear whether the service provider is expected to make its own assessment on unlawfulness for the purpose of this section or if this relates to material determined to be unlawful by a court or another appropriate authority.[1973]

In terms of evidence-gathering and policy on cybercrime, the Cyber and Data Protection Act amends the **Interception of Communications Act *[Chapter 11:20]*** to create a **Cyber Security and Monitoring of Interception of Communications Centre** located in the Office of the President. This is described as a "monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorised person". In addition to being the channel for effecting "authorised interceptions", its functions include advising Government on cybercrime and cyber security, operating a "protection-assured whistle-blower system", and promoting cyber security in the public and private sectors; (amongst other things). The Centre is advised by a Cyber Security Committee appointed by the relevant minister.

Disturbingly, in terms of the amended Interception of Communications Act, a warrant for the **interception of communications** (by post, telecommunications or radio communications) can be issued by the Minister on the advice of the Cyber Security Committee – with no judicial involvement. Applications for such interceptions can be made by or on behalf of the Chief of Defence Intelligence, the Director-General of the President's department responsible for national security, the Commissioner of the Zimbabwe Republic Police or the Commissioner General of the Zimbabwe Revenue Authority.[1974] The criteria for the issue of such warrants include reasonable suspicion of a serious offence by an organised criminal group, one of a list of serious criminal offences (which do not at this stage include cybercrime offences),[1975] an "actual threat to national security" or any "compelling national economic interest", or "a potential threat to public safety or national security"[1976] - which are for the most part broad, general and subjective standards. Similarly, the same officials who can apply for a warrant under hits law can demand a decryption key, in the interests of national security, to prevent or detect a serious criminal offence, or to ensure the country's economic well-being.[1977]

[1972] Id, subsection 397C(11) as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[1973] "Freedom on the Net 2022: Zimbabwe", Freedom House, section B2 assume that these provisions impose penalties providers that fail to remove illegal content when ordered by a court or other public authority or *upon discovery by the service provider*.
[1974] Interception of Communications Act, 2007 [*Chapter 11:20*], section 5, as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
[1975] The offences are listed in the Third Schedule and in paragraphs 1-8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*].
[1976] Interception of Communications Act, 2007 [*Chapter 11:20*], section 6.
[1977] Id, section 11.

C) SIM CARD REGISTRATION

Another part of the surveillance picture is **SIM card registration**. In terms of the regulations issued under the Postal and Telecommunications Act, mobile phone subscribers are required to provide identification details to service providers, including full name, permanent residential address, nationality, gender, subscriber identification number, and national identification or passport number. Service providers are required to retain this information for five years after the subscription has been discontinued. They are also obliged to transmit all of this data to POTRAZ on a monthly basis. POTRAZ is to maintain a Central Subscriber Information Database, where all subscriber information will be stored. Access to the database will be available for several purposes including for assisting law enforcement agencies, for "safeguarding national security", and for "undertaking approved educational and research purposes."

Access to this data for law enforcement purposes initially required a written request from an official of a senior rank, with no requirement for any judicial authority. This was altered when 2014 regulations replaced the 2013 set, with the updated regulations requiring a warrant or a court order for access to subscribed data by law enforcement agencies.[1978] However, Zimbabwe's Parliamentary Legal Committee noted that the amended regulations are still inadequate to ensure independent judicial oversight since a warrant can be issued by police officers who have been designated as justices of the peace.[1979]

It has been noted that this scheme "clearly shows a disregard for the rights to privacy and free expression protected by the new Zimbabwean constitution" as well as eradicating the potential for anonymous communications, enabling location-tracking, and simplifying communications surveillance and interception.[1980]

It has been reported that the privacy of mobile subscribers was violated during the July 2018 elections, when subscribers received unsolicited campaign messages from ZANU-PF (the ruling party). These campaign messages reportedly referred to the recipients by name, even though many were not party members, raising suspicions on this score.[1981]

In 2020, an official from the Criminal Investigation Department Asset Forfeiture Unit obtained a warrant from a magistrate for a list of *all* the customers of the country's leading mobile network service provider during a specified six-month period, along with a summary of e-money or airtime credit services on the platform during the same period, for a money laundering investigation. However, the High Court cancelled the warrant on the found that it was excessively wide, speculative and liable to abuse. Observers noted that this search warrant, if allowed to stand, "would have gravely

[1978] Postal and Telecommunications (Subscriber Registration) Regulations, 2013 (Statutory Instrument 142 of 2013), replaced by Postal and Telecommunications (Subscriber Registration) Regulations, 2014 (Statutory Instrument 95 of 2014).
[1979] Freedom on the Net 2022: Zimbabwe", Freedom House, section C6.
[1980] "Zimbabwe: New SIM registration database law represses twin rights to privacy and expression", Association for Progressive Communications, 3 October 2012; "Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.
[1981] Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.

compromised the privacy of over 11 million people, who did not break the law", constituting an acute breach of the right to privacy. [1982]

18.5 ELECTION LAW AND FREEDOM OF EXPRESSION

Elections for the President, Members of Parliament and local councillors will be held in Zimbabwe in August 2023, with current President Emmerson Mnangagwa seeking a second term.[1983]

Elections are administered by the **Zimbabwe Electoral Commission (ZEC)**, which is covered in detail in the Constitution, and conducted in accordance with the **Electoral Act**.[1984]

ZIMBABWE CONSTITUTION

ZIMBABWE ELECTORAL COMMISSION

238. ESTABLISHMENT AND COMPOSITION OF ZIMBABWE ELECTORAL COMMISSION

1. There is a commission to be known as Zimbabwe Electoral Commission consisting of –

a. a chairperson appointed by the President after consultation with the Judicial Service Commission and the Committee on Standing Rules and Orders; and

b. eight other members appointed by the President from a list of not fewer than twelve nominees submitted by the Committee on Standing Rules and Orders.

2. The chairperson of the Zimbabwe Electoral Commission must be a judge or former judge, or a person qualified for appointment as a judge.

3. If the appointment of a chairperson to the Zimbabwe Electoral Commission is not consistent with a recommendation of the Judicial Service Commission, the President must cause the Committee on Standing Rules and Orders to be informed as soon as practicable.

4. Members of the Zimbabwe Electoral Commission must be Zimbabwean citizens and chosen for their integrity and experience and for their competence in the conduct of affairs in the public or private sector.

5. Members of the Zimbabwe Electoral Commission are appointed for a six-year term and may be re-appointed for one such further term, but no person may be appointed to or serve on the Commission after he or she has been a

[1982] "Econet judgement guarantees privacy", *The Standard*, 13 September 2020.
[1983] "Zimbabwe holds harmonized elections (presidential, parliamentary and local government elections) every five years." "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
[1984] Electoral Act [*Chapter 2:13*].

member for one or more periods, whether continuous or not, that amount to twelve years.

239. FUNCTIONS OF ZIMBABWE ELECTORAL COMMISSION

The Zimbabwe Electoral Commission has the following functions –

a. to prepare for, conduct and supervise –
   i. elections to the office of President and to Parliament;
   ii. elections to provincial and metropolitan councils and the governing bodies of local authorities;
   iii. elections of members of the National Council of Chiefs established by section 285; and
   iv. referendums;
   and to ensure that those elections and referendums are conducted efficiently, freely, fairly, transparently and in accordance with the law;
b. to supervise elections of the President of the Senate and the Speaker and to ensure that those elections are conducted efficiently and in accordance with the law;
c. to register voters;
d. to compile voters' rolls and registers;
e. to ensure the proper custody and maintenance of voters' rolls and registers;
f. to delimit constituencies, wards and other electoral boundaries;
g. to design, print and distribute ballot papers, approve the form of and procure ballot boxes, and establish and operate polling centres;
h. to conduct and supervise voter education;
i. to accredit observers of elections and referendums;
j. to give instructions to persons in the employment of the State or of a local authority for the purpose of ensuring the efficient, free, fair, proper and transparent conduct of any election or referendum; and
k. to receive and consider complaints from the public and to take such action in regard to the complaints as it considers appropriate.

240. DISQUALIFICATIONS FOR APPOINTMENT TO ZIMBABWE ELECTORAL COMMISSION

In addition to the persons mentioned in section 320(3) [Members of Parliament and members of provincial or metropolitan councils, local authorities and Government-controlled entities], the following persons are ineligible for appointment to the Zimbabwe Electoral Commission –

a. public officers, other than judges;
b. employees of provincial and metropolitan councils and local authorities; and
c. members and employees of statutory bodies and government-controlled entities.

241. ZIMBABWE ELECTORAL COMMISSION TO REPORT ON ELECTIONS AND REFERENDUMS

In addition to the report it is required to submit in terms of section 323 [which requires every Commission to submit to Parliament, through the responsible Minister, an annual report describing fully its operations and activities], the Zimbabwe Electoral Commission must without delay, and through the

appropriate Minister, submit a report to Parliament on the conduct of every election and every referendum.

The forthcoming elections should be viewed in historical context:

When Zimbabwe gained Independence in 1980, the abolition of the Rhodesian system of apartheid awakened hopes for political transformation. However, in the years afterward, Zimbabwe effectively transformed into a one-party state led by President Robert Mugabe and his Zimbabwe African National Union – Patriotic Front (ZANU-PF). One of the first, and most severe, glimpses of the violent nature of the new regime were the Gukurahundi massacres in Matabeleland, which resulted in around 20,000, mostly from the Ndebele minority, dead. However, Zimbabwe's economy continued to perform well in the first decade after independence, and Zimbabwe remained the "breadbasket" of southern Africa.

The formation of the Movement for Democratic Change (MDC) in 1999, by a wide range of civic movements, led to the first opposition party that posed a serious threat to ZANU-PF rule. Not only did the MDC win a significant number of parliament seats in 2000, but it also managed to successfully mobilize a "no" vote during a referendum around proposed constitutional amendments earlier that year.
The fast-track land reform program, which ZANU-PF initiated shortly after its defeat in the constitutional referendum in 2000, exacerbated an economic crisis that had started in the 1990s and was aggravated by Zimbabwe's adoption of the Economic Structural Adjustment Programs (ESAP). Combined with economic mismanagement and other factors, this led to a 40% decline in GDP between 1998 and 2009, and the notorious hyperinflation and shortages of almost all commodities in 2008.

After the 2008 elections, the Zimbabwe Electoral Commission (ZEC) took five weeks to announce the results, which many believed was an indication Morgan Tsvangirai's MDC-T had won. ZEC did indeed announce an MDC-T win but stated that Tsvangirai had received only 47.9% of the vote (against Mugabe's 43.2%), not enough to secure an outright, first-round victory. The resulting run-off was marred by violence, as opposition leaders and supporters were beaten, tortured, kidnapped and killed. To avoid further violence, Tsvangirai decided to withdraw from the run-off.

Following the international community's refusal to accept ZANU-PF's blocking of an apparent MDC-T victory, a Government of National Unity (GNU) was formed with South Africa acting as mediator. This forced political parties to jointly govern the country and form the first coalition government since independence. The GNU managed to ensure political and economic stability, halting inflation and ensuring economic growth. One of the other major gains in this period was the formulation of a new constitution, which was overwhelmingly approved in a referendum after years of negotiations.

The GNU ended with the 2013 elections, which resulted in a contested ZANU-PF win. It was the scale of their victory that shocked most observers, as Mugabe won 61% of the vote, while Tsvangirai only managed to secure 33%. Moreover, the ZANU-PF went from being a parliamentary minority to a holding resounding majority (from 99 to 160 out of 210 seats). In the years that followed, the political landscape was dominated by intense factionalism within ZANU-PF, continued political and economic paralysis and a lack of substantial reforms. The factionalism ultimately culminated in the coup

presented as a military intervention, called Operation Restore Legacy, in November 2017, which led to the forced departure of President Mugabe.

The 2018 elections were historic, as they were the first ones in which Mugabe did not participate. ZANU-PF's Mnangagwa, who took over from Mugabe in 2017, beat the young MDC-A leader, Nelson Chamisa, who became the leader of the opposition after Tsvangirai's death earlier that year.[1985]

As noted by local and international election observers, the run-up to the 2018 elections was characterized by a largely peaceful environment. They further indicated the opening of democratic space and the ability of the opposition to campaign freely, including in areas it previously could not access. The fact that the EU was invited to send an Election Observation Mission (EOM) for the first time in 16 years further testified to this change. However, despite some positive developments, most international EOMs concluded the elections were not in accordance with international standards. They indicated there was no level playing field and highlighted the partisan role of the Zimbabwe Electoral Commission (ZEC), the biased state media, the use of state resources by ZANU-PF and subtle forms of intimidation.[1986]

The departure of Mugabe after his 37-year rule led to renewed hope for political and economic transformation, which was further fueled by Mnangagwa's public remarks that his "new dispensation" was "open for business" and willing to implement democratic reforms. However, Mnangagwa's initial years were marked by increasing repression, a lack of reform, severe corruption and a worsening economic crisis.[1987]

According to the Africa Centre for Strategic Studies, the Zimbabwean elections "are shaping up to be the bloodiest on the continent" in 2023, as the ruling Zimbabwe African National Union-Patriotic Front (ZANU-PF) ramps up its use of violence and intimidation in the attempt to retain its 43-year grip on power":[1988]

The latest cycle of violence against opposition candidates has, in fact, already begun. In June 2022, opposition activist Moreblessing Ali was abducted on the outskirts of Harare. Her dismembered body was later found in a well nearby. Witnesses identified a ZANU-PF activist as the assailant. Over a dozen opposition politicians who attended her funeral were arrested for "inciting violence." Many remain incarcerated even though they have yet to be charged.

This is but one illustration of the pattern of intimidation and suppression of political opposition, including arrests and extrajudicial killings, that Zimbabwe faces as it heads toward elections. […]
What is noteworthy in the 2023 cycle is how early the violence against the opposition has started. The faction now in control of the ZANU-PF is also increasingly dropping any pretence that violence is not part and parcel of the party campaign playbook.

[1985] "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
[1986] Id, "Political Participation".
[1987] Id, "Executive Summary"
[1988] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).

[…]

With this climate of violence and intimidation, it is a given that the elections will not be free and fair.
This perspective is reinforced by widely held perceptions that the Zimbabwe Electoral Commission (ZEC) is biased, with leading ZANU-PF family members serving as commissioners. ZEC's reputation also suffers from the outsized role of the military, where 15 percent of ZEC staff are former service personnel, including the chief elections officer, who is a retired army major. Contrary to electoral best practice, ZEC has refused to publish an electronic copy of the electoral register to foster transparency. This pattern of institutional bias builds on a long history of election engineering in Zimbabwe including: limiting the number of polling stations in opposition strongholds, challenging the credentials of opposition candidates, and filing criminal charges against others—all with the aim of preventing them from standing for office.

An illustration of the latter is the imprisonment of Fadzayi Mahere, a 36-year-old lawyer and opposition member of Parliament with half a million Twitter followers. She was charged with "communicating false statements prejudicial to the state".[1989]

Looking more specifically at freedom of expression, Zimbabwe's **Electoral Act** contains some specific provisions relating to media and media coverage.

Public broadcasters are required to afford all political parties and independent candidates such free access to their broadcasting services as may be prescribed by regulations which are aimed at providing at a fair and balanced allocation of time between each political party and independent candidate, by regulating the total time to be allocated to each political party and candidate, the duration of each broadcast by or on behalf of a party or candidate, and the times and areas in which these broadcasts are to be transmitted.[1990]

Broadcaster or print media which publish any advertisement by or on behalf of a political party or candidate contesting an election must offer the same terms and conditions of publication to all the political parties and candidates contesting the election, without discrimination. All political advertisements must be clearly identified as such.[1991]

The Zimbabwe Electoral Commission can require broadcasters and print publishers to publish statements issued by the Commission for the purpose of informing voters about the electoral process, upon payment by the Commission of a reasonable amount for such publication.[1992]

During the election period (which will be identified by the Commission), broadcasters and print publishers must follow certain principles:

- All political parties and candidates must be treated equitably in their news

[1989] Id.
[1990] Electoral Act [*Chapter 2:13*], as amended through 2018, section 160G.
[1991] Id, section 160H.
[1992] Id, section 160I.

media, in regard to the extent, timing and prominence of the coverage accorded to them.
- News reports on the election must be factually accurate, complete and fair,
- There must be a clear distinction between factual reporting and editorial comment.
- Inaccuracies in reports on the election must be rectified without delay and with due prominence.
- Political parties and candidates must be afforded a reasonable right of reply to allegations by others.
- News media must not promote political parties or candidates that encourage violence or hatred against any class of persons in Zimbabwe.
- News media must avoid language that encourages racial, ethnic or religious prejudice or hatred, incites violence, or is likely to lead to "undue public contempt" towards any political party, candidate or class of person in Zimbabwe.[1993]

The general rules appear to be fair and reasonable for the most part - although the duty to avoid producing "contempt" in news reporting about a candidate could inhibit justified criticism or reports of wrongdoing on the part of a candidate.

The media requirements in the Electoral Act overlap with those in the **Broadcasting Services Act**, which require broadcasters to give "reasonable and equal opportunities for the broadcasting of election matter to all political parties contesting the election" during an election period and forbids the broadcasting of election advertisements by broadcast licensees during the period from four days before the first polling day until the closing of the polls on the last polling day.[1994]

The **Electoral Act** imposes certain restrictions on speech on **polling day**. It is an offence to do any of the following within three hundred metres of a polling station on a polling day:

- convoke or take part in any gathering of more than twelve persons: or
- canvass for votes; or
- utter slogans; or
- distribute leaflets or pamphlets for or on behalf of any candidate or political party; or
- organise or engage in public singing or dancing; or
- use bands or music or loudspeaker vans or apparatus.[1995]

These seem to be reasonable restrictions to avoid voter intimidation.

[1993] Id, section 160J.
[1994] Broadcasting Services Act, 2001 [*Chapter 12:06*], sections 2-3 read with the definitions in section 1.
[1995] Electoral Act [*Chapter 2:13*], as amended through 2018, section 147.

The **Zimbabwe Electoral Commission, assisted by the Zimbabwe Media Commission**, will monitor the Zimbabwean news media during the election period to ensure that the rules in the Electoral Act are followed. although it is not clear what remedies or sanction will be applied in the case of violations.[1996]

In the run-up to the August 2023 elections, there has already been a **collision between the Electoral Act and the Cyber and Data Protection Act**. The Zimbabwe Electoral Commission has indicated that the electronic version of the voters' roll cannot be released on the grounds that this would compromise the security of the personal data in the database and possibly lead to identity theft. Civil society groups counter-argue that section 11(5)(h) of the Cyber and Data Protection Act allows processing of sensitive personal data where this is authorised by a law or regulation for any reason constituting substantial public interest, with some alleging that the reluctance to release the digital voters' roll is intended to provide leeway to manipulate it with a view to swaying the electoral outcome. In March 2023, the High Court refused to order the Commission to release an electronic copy of the voters' roll, on the grounds that this could compromise the security of the database. The case is on appeal to the Supreme Court.[1997]

As noted above, **concerns about voters' data privacy** were raised after mobile phone users received personalised messages from the ruling party soliciting their votes. Following on a complaint about this by MISA-Zimbabwe, POTRAZ in its role as the Data Protection Authority undertook to investigate the matter.[1998]

Another election issue that has already arisen concerns **media coverage of the voter registration process**. The Zimbabwe Electoral Commission denied journalists access to voter registration statistics and voter registration centres on the basis that they had not been accredited by the Zimbabwe Electoral Commission ZEC, even though they are already accredited as journalists by the Zimbabwe Media Commission.[1999]

Disputes may well heat up even further as the 2023 election grows closer.

[1996] Id, section 160K. Penalties can be provided n statutory instruments issued by the Commission in terms of the Act. See section 192.
[1997] "Zimbabwe's uneven electoral field: Data protection laws used to deny digital voter roll inspection", Advox, 13 June 2023; "ZEC wins voters' roll case… Releasing electronic format compromises security, court rules", *The Herald*, 8 March 2023.
[1998] Wallace Mawire, "MISA-Zimbabwe pleased by POTRAZ bid to investigate violations of the Cyber and Data Protection Act", April 2023.
[1999] "ZEC denies journalists access to voter registration stats", *The Zimbabwean*, 12 March 2023.

REFERENCES

REFERENCES

1. "Elections Calendar for SADC-2022-to-2026", SADC Parliamentary Forum website; "SADC Elections Calendar", GENDER & Development in SADC and Southern African Research and Documentation Centre (SARDC)
2. "**East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom**", Amnesty International, 3 May 2023.
3. Karen Allen, "Journalism on trial in Africa: fortitude and fake news", Institute for Security Studies, 26 June 2023.
4. Interviewed via Zoom on 25 July 2023.
5. African Union Convention on Cyber Security and Personal Data Protection, African Union, 27 June 2014.
6. The Declaration of Principles of Freedom of Expression and Access to Information in Africa, African Commission on Human and Peoples' Rights, 10 November 2019.
7. Guidelines on Access to Information and Elections in Africa, African Commission on Human and Peoples' Rights, 15 November 2017.
8. See, for example, Assessing Cybercrime Laws from a Human Rights Perspective, Global Partners Digital, [2022], page 9; Kirsty Phillips et al, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies", 2(2) Forensic Science 2022, pages 379-398; Prof. Dr. Marco Gercke, "Understanding cybercrime: phenomena, challenges and legal response", International Telecommunications Union, 2012, Chapter 2; "Cybercrime", United Nations Office on Drugs and Crime (UNODC), undated (accessed 23 June 2023).
9. "Southern African Development Community Cybersecurity Maturity Report 2021", Cybersecurity Capacity Centre for Southern Africa (C3SA), 2022, page 48 (footnote omitted).
10. John General, "Analysis: For Journalists, Using Hacked and Surveillance Data Creates Tough Ethical Decisions", *The Click*, 13 October 2021.
11. See, for some examples, Caroline O'Donovan, "Hacking in the newsroom? What journalists should know about the Computer Fraud and Abuse Act", Nieman Lab, 3 March 2014 (discussing a US cybercrime statute); Katitza Rodriguez et al, "Protecting Security Researchers' Rights in the Americas", Electronic Frontier Foundation, 16 October 2018; Deborah Brown, "When Digital Rights and Cybercrime Collide: A Trial to Watch in Ecuador", *Opinio Juris*. 10 November 2021.
12. "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021; Katitza Rodriguez et al, "Protecting Security Researchers' Rights in the Americas", Electronic Frontier Foundation, 16 October 2018. According to this article, one US court found that scraping information from a public website "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions".
13. Rainey Reitman, "When Computer Crimes Are Used To Silence Journalists: Why EFF [Electronic Frontier Foundation] Stands Against the Prosecution of Glenn Greenwald", Electronic Frontier Foundation, 24 January 2020 (suggesting that references to malicious intent in cybercrime laws can help avoid misuse of cybercrime laws against journalists and researchers).
14. "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.
15. See, for example, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights", A/HRC/39/29. paragraph 34: "Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted."
16. "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.
17. SADC Model Law on Electronic Transactions and Electronic Commerce, section 35.
18. See, for example, Juan Londoño, "Content Moderation Using Notice and Takedown Systems: A Paradigm Shift in Internet Governance", *Insight* column, American Action Forum, 8 November 2021.
19. "Elections Calendar for SADC-2022-to-2026", SADC Parliamentary Forum website; "SADC Elections Calendar", GENDER & Development in SADC and Southern African Research and Documentation Centre (SARDC); Dr Tabani Moyo, "States in Southern Africa cracking down on free expression online", Media Institute of Southern Africa (MISA), 22 February 2023; "IFES Election Guide: Madagascar", International Foundation for Electoral Systems. Elections for the National Assembly were set to take place in Malawi in 2024, but the Parliamentary and Presidential Elections Act (PPEA) Amendment Act, 2020 extended the term of office for Members of Parliament and ward councillors by one year so that harmonised presidential, parliamentary and local elections can take place in 2025. Enelless Nyali, "Elections May 19", *The Nation*. 25 February 2020.
20. *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. Despite its designation as a draft, this appears to be the most recent version of the document. See "Open-ended intergovernmental expert group meeting on cybercrime", UNODC website, undated, (accessed 23 June 2023), which links to the 2013 draft as well as various country comments on that draft.
21. *Universal Declaration of Human Rights*, Article 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
22. *International Covenant on Civil and Political Rights*, Article 19: "1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or

through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

23. *African Charter on Human and Peoples' Rights*, Article 9: "1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law."
24. *International Covenant on Civil and Political Rights*, Article 19(3) (quoted above).
25. "Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022. paragraphs 19-20 (footnote omitted).
26. The text of the *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information* can be found here.
27. Quotation from the Windhoek+30 Declaration, paragraph 12. The Windhoek Declaration and the Windhoek+30 Declaration are described further below.
28. *Council of Europe Convention on Cybercrime, 2001* ("Budapest Convention").
29. See "Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Status as of 28/07/2019". The text refers to the status as of 7 June 2023.
30. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003*. See the "Chart of signatures and ratifications of Treaty 189". The text refers to the status as of 7 June 2023.
31. The text of the *Second Additional Protocol* is available here, and the status list can be found here. The *Second Additional Protocol* requires five ratifications to enter into force.
32. "Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence", CETS-224, 12 May 2022, paragraph 22.
33. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, January-June 2018.
34. "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.
35. "Abuse of Cybercrime Measures Taints UN Talks", Human Rights Watch, 5 May 2021.
36. "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.
37. Id.
38. *Council of Europe Convention on Cybercrime, 2001* ("Budapest Convention"), Article 15.
39. *Second Additional Protocol*, Article 13.
40. Id, Article 14.
41. "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.
42. See, for example, "ARTICLE 19's briefing: The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol", May 2022.
43. "AU Convention on Cyber Security and Personal Data Protection: Malabo Convention", Michaelson's, 24 April 2023. The treaty came into force on 8 June 2023. June 15, 2023. Yohannes Eneyew Ayalew, "The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?", *EJIL: Talk!*, Blog of the European Journal of International Law, 15 June 2023.
44. *African Union Convention on Cyber Security and Data Protection, 2014*, Article 36: Entry into Force; Status List (dated 11 April 2023). The status list as accessed on 15 July 2023 was not up-to-date.
45. "The state of cybercrime legislation in Africa – an overview", Council of Europe, Version 11, May 2015.
46. *African Union Convention on Cyber Security and Data Protection, 2014*, Article 29.1(b).
47. Id, Article 29.2(b).
48. See, for example, "Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'". CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence), undated, text and footnote 1; Lukman Adebisi Abdulrauf & Charles Manga Fombad. "The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?", paper presented at the 7th International Conference on Information Law and Ethics (ICIL) at the University of Pretoria, South Africa, 22-23 February 2016.
49. The text of the 2012 *SADC Computer Crime and Cybercrime Model Law* can be found here.
50. SADC, "Consultancy for the Review and Modernisation of the SADC Cyber Crime Model Law", 22 September 2022.
51. "How SADC Government Cybersecurity Laws Impact Human Rights", ICT Works, 17 November 2021.
52. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 20.
53. Zahid Jamil, "Cybercrime Model Laws: Discussion paper prepared for the Cybercrime Convention Committee", Council of Europe, 9 December 2014.
54. Id.
55. See "Commonwealth model law promises co-ordinated cybercrime response", The Commonwealth, 22 April 2016. The text of the 2002 *Commonwealth Computer and Computer-Related Crime Model Law* is available here.
56. See, for example, Zahid Jamil, "Cybercrime Model Laws", discussion paper prepared for the Cybercrime Convention Committee, 9 December 2014.
57. *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, "Introduction".

58. Article 19(3) of the *International Covenant on Civil and Political Rights* requires restrictions on the freedom of expression only if they are "provided by law and are necessary:
    (a) For respect of the rights or reputations of others;
    (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."
    See also, for example, the Special Rapporteurs' Joint Declaration on Media Freedom and Democracy, 2023 and Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, 2017. The Joint Declarations are discussed further below.
59. The complete set of Joint Declarations can be accessed here.
60. See "30th Anniversary of the Windhoek Declaration", UNESCO website. The text of the 1991 Windhoek Declaration is available here.
61. *Windhoek Declaration, 1991*, paragraph 6.
62. *Windhoek+30 Declaration*, paragraphs 9, 11, and 13; quote from paragraph 13.
63. Id, paragraph 13.
64. Id, paragraph 16.
65. African Commission on Human and Peoples Rights, "Resolution 169 on Repealing Criminal Defamation Laws in Africa", 2010.
66. *Konaté v Burkina Faso*, African Court on Human and People's Rights, Application No. 004/2013, 5 December 2014.
67. Id, "Separate Opinion".
68. *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 22.
69. **Lesotho:** *Peta v Minister of Law, Constitutional Affairs and Human Rights* (CC 11/2016) [2018] LSHC 3 (18 May 2018); **Kenya:** *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR. An appeal is reportedly pending. Carmel Rickard, "Pen Report: Criminal Defamation is Used to Stifle Dissent in Africa", *AfricanLII,* 20 April 2018. **Zimbabwe:** *Madanhire & Another v AG (*CCZ 2/14 Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); "Concourt outlaws Criminal Defamation", *The Herald*, 4 February 2016; *MISA-Zimbabwe v Minister of Justice* (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.
70. *Hoho v The State* 2009 (1) SACR 276 (SCA) at paras 27-36, citing a similar conclusion in Granada: *Worme and another v Commissioner of Police of Grenada* [2004] UKPC 8 at 455E-F para 42 and *R v Lucas* [1998] SCR 439 at para 55. The Supreme Court of India also upheld the constitutionality of criminal defamation in 2016, finding that this law constitutes a reasonable restriction on the right to freedom of expression *Subramanian Swamy v Union of India* (2016) 7 SCC 221.
71. Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022, paragraph 57 (footnotes omitted).
72. Id, paragraph 58.
73. "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, paragraph 20.
74. Id, paragraph 21, citing General Comment No. 16 of the Human Rights Committee that monitors compliance with the International Covenant on Civil and Political Rights.
75. "Report on encryption, anonymity, and the human rights framework", Special Rapporteur on freedom of opinion and expression, A/HRC/29/32**,** 22 May 2015, paragraph 16.
76. Id, paragraph 51.
77. Id, paragraphs 31-35.
78. Id, paragraph 60.
79. "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/39/29, 3 August 2018, paragraph 20.
80. *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 40.
81. "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, paragraph 26. On this point, the report references the Addendum to General Comment No. 27, Human Rights Committee, CCPR/C/21/Rev.1/Add.9, 1 November 1999, paras 11-16, https://undocs.org/CCPR/C/21/Rev.1/Add.9.
82. Id, paragraph 25.
83. Id, paragraph 27.
84. *ACHPR Declaration on the Principles of Freedom of Expression and Access to Information*, Principle 41.
85. A link to the text of the Guidelines is available here; the Guidelines can also be found here. The background to their adoption is set out in the introduction.
86. The text of the Revised 2015 Guidelines can be found here (the text could not be accessed on the SADC website at the time of writing). The background to their adoption is set out in the introduction. (The text of the previous 2008 Guidelines can be found here, as a point of comparison.)
87. *Revised SADC Principles and Guidelines Governing Democratic Elections, 2015*, Definitions of Concepts and Acronyms.
88. Id, paragraph 4.1.2.
89. Id, paragraph 4.1.6.
90. Id, paragraph 5.1.10
91. "SADC Model Law on Elections adopted", SADC Parliamentary Forum website, undated. The text of the model law is available here. The introduction to the model law gives more background information on its adoption.

92. *SADC Model Law on Elections, 2018*, section 76.
93. Id, section 81.
94. **Lei n.º 22/11 de 17 de Junho**: Data Protection Law. A short overview is available in English here. In addition, **Lei n.º 23/11 de 20 de Junho**: Electronic Communications and Information Society Services Law contains specific data protection rules for personal data generated from electronic communications. See also **Decreto Presidencial n.º 214/2016 de 10 de Outubro**: Organic Statute of the Angolan Data Protection Agency. João Robles, "Doing Business in Angola: Overview", section 14, Thompson Reuters Practical Law, discussing law in force as of 1 October 2021.
95. **Lei n.º 11/02 de 16 de Agosto**: Access to Documents held by Public Authorities, available in English here.
96. "Africa Freedom of Information Centre Submission to the UN Universal Periodic Review", undated.
97. "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022; **Lei n.º 17/22 de 6 de Julho** – Alteração da Lei de Imprensa (amends the Press Law (Law no. 1/17) and adds articles 2.ºA and 25.ºA); **Lei n.º 16/22 de 6 de Julho** – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão (amends the Law on the Exercise of Broadcasting Activity (**Law no. 4/17**), and adds Chapter IV-A with Articles 46A-46F).
98. "Angola: Events of 2022", Human Rights Watch World Report 2023.
99. Rui Verde, "The Death Knell for Freedom of the Press in Angola", Maka Angola, 8 February 2017.
100. Id.
101. D Quaresma Dos Santos, "Angola passes laws to crack down on press and social media", *The Guardian* via *Maka Angola,* part of the Guardian Africa Network, 19 August 2016.
102. The text of all five laws in Portuguese can be found here. See also "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 24 and footnote 99.
103. Lei n.º 1/17 de **23 de Janeiro**: Lei de Imprensa, que estabelece os Princípios Gerais Orientadores da Comunicação Social e regula as Formas do Exercício da Liberdade de Imprensa. (Press Law, which establishes the General Guiding Principles of Social Communication and regulates the Forms of Exercise of Freedom of Press). This law repeals the 2006 Press Law (**Lei n.º 7/06**: Lei de Imprensa).
104. Lei n.º 2/17 de **23 de Janeiro:** Lei Orgânica da Entidade Reguladora da Comunicação Social Angolana, que estabelece as Atribuições, as Competências, a Composição, a Organização e o Funcionamento da Entidade Reguladora da Comunicação Social Angolana.
105. Lei n.º 3/17 de **23 de Janeiro:** Lei sobre o Exercício da Actividade de Televisão, que regula o Acesso e o Exercício da Actividade de Televisão, a Gestão e Exploração de Redes de Transporte e Difusão do Sinal Televisivo e a Prestação de Serviços de Comunicação Social Audiovisual em todo o Território Nacional.
106. Lei n.º 4/17 de **23 de Janeiro:** Lei sobre o Exercício da Actividade de Radiodifusão, que regula o Exercício da Actividade de Radiodifusão no Território.
107. Lei n.º 5/17 de **23 de Janeiro:** Lei sobre o Estatuto do Jornalista. This law revokes Decree no. 56/97.
108. See "Data Protection and Cybersecurity Laws in Angola", CMS law firm, undated; An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-24.
109. Lei n.º 23/11 de 20 de Junho: Das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (Electronic Communications and Information Society Services Law), described in "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-23.
110. An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, pages 22-23/
111. Ferreira Manuel, "Angola precisa reforçar a aplicação das leis sobre cibersegurança nas instituições públicas", 14 de Abril, 2023: "De acordo com Alcides Miguel, que falava em representação do Banco Millennium Atlântico, há já em Angola leis importantes que regulam as principais preocupações relactivas à cibersegurança, entre as quais a Lei 7/17, relactiva à protecção e segurança das redes e a Lei 23/11, relactiva às infra-estruturas críticas. Entretanto, o observa, a aplicabilidade destas normas nos organismos públicos e a sua supervisão não é visível."
Translation: "According to Alcides Miguel, who was speaking on behalf of Banco Millennium Atlântico, there are already important laws in Angola that regulate the main concerns relating to cybersecurity, including Law 7/17, relating to the protection and security of networks, and Law 23 /11, concerning critical infrastructures. However, he observes, the applicability of these norms in public bodies and their supervision is not visible."
112. Decreto Presidencial n.º 202/11 de 22 de Julho: Aprova o Regulamento das Tecnologias e dos Serviços da Sociedade da Informação.
113. "Freedom on the Net 2022: Angola ", Freedom House, section A5 (footnotes omitted).
114. Decreto Presidencial nº 108/16 de 2 de Maio: Regulamento Geral das Comunicações Electrónicas (General Electronic Communications Regulation).
115. Lei nº 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
116. An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 23, which refers to this law as the "Computer Networks and Systems Protection Act, 2016";

"Freedom on the Net 2022: Angola ", Freedom House, section C6, which refers to the law as the "2017 Law on Protection of Information Networks and Systems".
117. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 23.
118. "Freedom on the Net 2022: Angola ", Freedom House, section A4.
119. "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022. The three laws are:
Lei n.º 17/22 de 6 de Julho – Alteração da Lei de Imprensa (amends the Press Law (**Law no. 1/17**) and adds articles 2A and 25A);
Lei n.º 16/22 de 6 de Julho – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão (amends the Law on the Exercise of Broadcasting Activity (**Law no. 4/17**), and adds Chapter IV-A with Articles 46A-46F);
Lei n.º 15/22 de 6 de Julho – Aprovação da Lei das Sondagens e Inquéritos de Opinião (Opinion Polls and Surveys).
"Newsletter Julho-Agosto 2022", LegisPalop+TL. The texts of these laws are available on LEXLINK, which is a subscription service.
120. Law no. 1/17, which establishes the General Guiding Principles of Social Communication and regulates the Forms of Exercise of Freedom of Press. It has been amended by **Lei n.º 17/22 de 6 de Julho.** "Angola: National Assembly Approves Amendments to Press Law", Angola Press Agency, 8 May 2022; "Newsletter Julho-Agosto 2022", LegisPalop+TL.
121. Id, Article 5.
122. Id, Article 6.
123. Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017.
124. Translation of this provision as in Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017. "Social communication" includes printed materials and telecommunications disseminated to the public (Article 2: definitions).
125. Rui Verde, "The Death Knell for Freedom of the Press in Angola", Maka Angola, 8 February 2017.
126. "Freedom on the Net 2022: Angola ", Freedom House, section B3 (footnote omitted)
127. Law no. 1/17, Article 21.
128. Id, Article 22.
129. Id, Article 16.
130. Id**,** Article 8(1).
131. Law no. 2/17**,** Article 2(2).
132. Id, Article 7
133. Id, Article 3.
134. Id, Article 13.
135. Id, Article 45.
136. Id, Articles 48-50.
137. Id, Article 51.
138. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
139. "Media regulation is 'undemocratic' and should be shared", *Lusa/Verangola*, 1 October 2021.
140. Rui Verde, "The Death Knell for Freedom of the Press in Angola", *Maka Angola*, 8 February 2017.
141. Law no. 3/17**,** Article 1.
142. Id, Article 2(i).
143. Id, Article 34. See also Article 35.
144. Id, Article 36.
145. Id, Article 82.
146. Law no. 4/17, as amended by **Lei n.º 16/22 de 6 de Julho** – Alteração da Lei sobre o Exercício da Actividade de Radiodifusão.
147. Id, Article 36.
148. Law no. 5/17.
149. Id, Article 2. Persons who carry out these activities without falling under the definition of journalists are termed "specialised collaborators". (The term translated as "specialised collaborator" in Portuguese is "colaborador especializado".)
150. Id, Article 4. Specialised collaborators who work for media outlets are not subject to licensing, but must have an identification card issued by the media outlet. Id, Article 25.
151. Id, Article 20.
152. Id, Chapter III read with Article 30. This body has also been referred to in English as the "Ethics and Credentialing Commission". "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A. In Portuguese, it is the "Comissão da Carteira e Ética".
153. Id, Article 31.
154. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
155. Id, Article 10(2)(a).
156. Id, Article 11(1).
157. This is, in Portuguese, "menores que tenham sido objecto de medidas tutelares sancionatórias".
158. Law no. 5/17, Article 16.
159. Id, Articles 42-43.

160. Id, Article 39.
161. Coque Mukuta, "Angola: Organizações de classe criticam propostas de alteração ao estatuto dos jornalistas e da ERCA", VOA, junho 15, 2023.
162. Personal communication with Rui Verde, July 2023.
163. "Angola: Judicial harassment of the award-winning investigative journalist, Mr. Rafael Marques de Morais", International Federation for Human Rights 12 July 2017. The charges were (1) "**outrage towards a sovereign body**" ("*ultraje ao órgão de soberania*" under Article 25(1) of the Law on Crimes against State Security and Article 105(1) of the Angola Constitution); (2) "**insult towards public authority** ("*injúrias contra autoridade pública*"), Article 181 of the previous Penal Code); (3) "**abuse of press freedom**" (Article 74(2) of the Press Law, Law No. 7/06); (5) **slander** (Article 7 of the previous Penal Code) and (6) **defamation** (Article 410 of the previous Penal Code). The Penal Code was revised in 2020, and Law No. 7/06 has been repealed.
164. Processo n.592/17-B, Repûblica de Angola, Tribunal Provincial de Luanda, 6ª Seccão da Sala dos Crimes Comuns.
165. The crime of abuse of the press is defined in article 43 of the Press Law as "any act or behaviour that injures the juridical values and interests protected by the criminal code, effected by publication of texts or images through the press, radio broadcasts or television".
166. Article 407 of the Penal Code describes the crime of defamation as publicly imputing to another person "something offensive to his honour and dignity".
167. *Rafael Marques de Morais v Angola*, Communication No. 1128/2002, U.N. Doc. CCPR/C/83/D/1128/2002 (2005). This case is also summarised in the Malawi case of *Mbele v R*, Misc. Criminal Case No. 04 of 2022, High Court of Malawi, 20 June 2022.
168. This account is based on the case summary of the Provincial court case, *Public Prosecutor v. Beirão, et al.* (15+2), by Global Freedom of Expression *here*; Ricardo Miguel Vieira, "Angolan Awakening: Ikonoklasta Doubles Down in his Fight for Change", *okayafrica*, [2017]; "'In Angola nobody is free,' activist Luaty Beirao tells DW", *Deutsche Welle,* 13 September 2016; "Opinion No. 21/2016 concerning Henrique Luaty da Silva Beirão, Manuel Chivonde, Nuno Álvaro Dala, Nelson Dibango Mendes dos Santos, Hitler Jessy Chivonde, Albano Evaristo Bingobingo, Sedrick Domingos de Carvalho, Fernando António Tomás, Arante Kivuvu Italiano Lopes, Benedito Jeremias, Inocêncio Antônio de Brito, José Gomes Hata, Osvaldo Sérgio Correia Caholo, and Domingos da Cruz (Angola)", Opinions adopted by the Working Group on Arbitrary Detention at its seventy-fifth session, 18-27 April 2016, UN Human Rights Council Working Group on Arbitrary Detention, A/HRC/WGAD/2016, 31 May 2016; "UN expert urges Angola to release fourteen rights activists detained for criticizing the Government", Press Release, UN Office of the High Commissioner on Human Rights, 23 October 2015.
169. "2023 World Press Freedom Index: Angola", Freedom House, "Safety".
170. "2022 Country Reports on Human Rights Practices: Angola", US State Department, Executive Summary.
171. Id, section 1F.
172. Id, section 2A.
173. "Freedom on the Net 2021: Angola", Freedom House, "Overview".
174. "Freedom on the Net 2021: Angola", Freedom House, excerpt from section B8 (footnotes omitted),
175. In addition to the examples summarised below, see "Angola charges 2 more journalists with criminal defamation over corruption reporting", Committee to Protect Journalists, 1 July 2021 and "Angolan editors questioned in separate criminal defamation investigations", Committee to Protect Journalists, 4 June 2021.
176. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
177. "Angolan journalists continue to face criminal insult and defamation proceedings", Committee to Protect Journalists, 30 June 2022.
178. "Angolan journalists questioned in criminal defamation complaint over gun trafficking report", Committee to Protect Journalists, 16 March 2022.
179. "Angolan outlet Camunda News suspends operations indefinitely after police harassment", Committee to Protect Journalists", 17 March 2023.
180. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A.
181. "Angola: Events of 2022", Human Rights Watch World Report 2023.
182. "Angolan editor Carlos Alberto sentenced to fine, 2 years in prison over coverage of land deal", Committee to Protect Journalists, 17 September 2021. "2023 World Press Freedom Index: Angola", Freedom House, "Safety".
183. "Freedom on the Net 2021: Angola", Freedom House, section B4.
184. "DW correspondent Borralho Ndomba harassed, briefly detained while covering student protest in Angola", Committee to Protect Journalists, 17 October 2022.
185. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A; "VOA correspondent briefly detained covering attempted election protest in Angola", Committee to Protect Journalists, 17 August 2022; "Angola: Events of 2022", Human Rights Watch World Report 2023.
186. Angola: Events of 2022", Human Rights Watch World Report 2023.
187. "Angola: Events of 2022", Human Rights Watch World Report 2023.
188. "2022 Country Reports on Human Rights Practices: Angola", US State Department, section 2A; "Angolan security forces attack journalists covering evictions in Luanda", Committee to Protect Journalists, 3 May 2022.
189. "Angola: Events of 2022", Human Rights Watch World Report 2023.
190. "Angolan public media journalists assaulted, branded 'sellouts' while covering nationwide strike", Committee to Protect Journalists, 18 January 2022; Angola: Events of 2022", Human Rights Watch World Report 2023.
191. "Angolan police unleash dog on reporter covering protest", Reporters Without Borders, 17 February 2021.

192. "Crackdown on reporters covering Luanda demonstration", Reporters Without Borders, 28 October 2020; "Angolan police detain, harass, and beat journalists covering protests", Committee to Protect Journalists, 27 October 2020.
193. "Cyber-attacks against Angolan news site and reporter", Reporters Without Borders, 9 October 2020.
194. "Angolan police unleash dog on reporter covering protest", Reporters Without Borders, 17 February 2021. No further details about this incident were reported.
195. "Angola: Judicial harassment of the award-winning investigative journalist, Mr. Rafael Marques de Morais", International Federation for Human Rights 12 July 2017; Kerry A Dolan, "Journalist Rafael Marques Given Two Year Suspended Sentence In Angolan Defamation Trial", *Forbes*, 28 May 2015; "The Case of Rafael Marques de Morais", Global Freedom of Expression, Columbia University, reporting on court decision of 28 May 2015.
196. "Cyber-attacks against Angolan news site and reporter", Reporters Without Borders, 9 October 2020; "Newspaper editor freed provisionally pending outcome of appeal", Reporters Without Borders, 13 November 2007; "Angola: Prominent journalist sent to jail in libel case", Committee to Protect Journalists, 5 October 2007.
197. Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
198. Lei n.º 38/20 de 11 de Novembro: Código Penal Angolano (Angolan Penal Code).
199. Lei n.º 39/20 de 11 de Novembro: Código do Processo Penal Angolano (Code of Criminal Procedure).
200. "Angola: Cybercrime policies/strategies", Council of Europe, undated.
201. "Data Protection and Cybersecurity Laws in Angola", CMS law firm, undated, section 4.
202. See id, sections 3 and 6.
203. Id.
204. Article 47 of the Penal Code.
205. "Angola Marks Technology Advancements With Cybersecurity Academy Plans", *Dark Reading*, 15 June 2023.
206. "Angola now has an IT Networks and Systems Protection Law", Gabinete Legal Angola, *News Lextter*, March 2017.
207. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12; Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
208. Preliminary Draft of the Penal Code, undated.
209. "Angola: Provisions of the 'Draft Criminal Code' are Incompatible with Angola's Human Rights Obligations", Amnesty International, 2012.
210. "LEXOTA Country Analysis: Angola", last updated July 2022.
211. Id.
212. "Article of the new Penal Code threatens freedom of expression, lawyers consider", *Lusa/Verangola*, 17 November 2020.
213. "Freedom on the Net 2022: Angola ", Freedom House, section C5 (footnotes omitted).
214. Id.
215. Lei n.º 2/20 de 22 de Janeiro: Da Videovigilância (Videosurveillance).
216. "Freedom on the Net 2022: Angola ", Freedom House, section C5 (footnotes omitted); see also "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12; "Angola: Regulation of the Video-Surveillance Law", PLMJ, 4 January 2022.
217. Lei n.º 7/17 de 16 de Favereiro: Protecção das Redes e Sistemas Informáticos (Protection of Networks and Information Systems).
218. "Freedom on the Net 2022: Angola ", Freedom House, section C6.
219. Id, section C4.
220. Lei n.º 11/20 de 23 de Abril: Da Identificação ou Localização Celular e da Vigilância Electrónica (Cellular Identification or Location and Electronic Surveillance), Article 3; "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 12.
221. "Freedom on the Net 2022: Angola ", Freedom House, section B2.
222. Data Protection Act 32 of 2018.
223. Sarah Buerger, "Botswana's Data Protection Act grace period extended", Michaelson's, 30 October 2022. Amendments are being considered. Andrew Maramwidze, "Back to the drawing board … glaring gaps in Botswana's Data Protection Act", IT web, 24 June 2022.
224. Printed Publications Act 15 of 1968. This is the original law; there may have been amendments since 1968 that are not reflected here. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 121-123.
225. See, for example, Thapelo Ndlovu and Jacqueline Kabeta, "Media Sustainability Index 2008: Botswana", IREX, page 16.
226. Cedric Swanka, "Botswana Reviews Cinematography Act to Boost Creative Economy", *Sunday Standard*, 2 September 2019; Esther Mmolai, "Collaborations Boost Film Production", *Daily News*, 13 June 2023.
227. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 123-124. The text of the law is available here, but only to subscribers.
228. Broadcasting Act [*Chapter 72:04*], section 5.
229. Id, section 10(1).
230. Broadcasting Regulations, 2004
231. Broadcasters' Code of Practice.

232. Communications Regulatory Authority Act 19 of 2012.
233. Id, sections 4 and 94. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 138-139.
234. The Act defines the "regulated sector" as "any sphere of activity within the telecommunications, broadcasting and postal service sectors which includes the installation of telecommunications networks; the installation and operation of radiocommunication equipment; the provision of postal services; the converging of electronic technologies and *the provision of internet services*" (emphasis added). "Regulated supplier" is accordingly defined as any supplier of goods or services in the regulated sectors whose activities fall within the scope to be regulated by the Authority". Communications Regulatory Authority Act 19 of 2012, section 2.
235. Media Practitioners Association Act, 2022, on file with authors.
236. Media Practitioners Act 29 of 2008.
237. "Press Freedom in Botswana 2022", International Press Institute, February 2023 (based on information gathered during a mission to Botswana in August 2022), page 8; "US State Department Human Rights Reports, Custom Report Excerpts: Botswana", section 2A, 2020.
238. "Statement for Second Reading Media Practitioners' Association Bill, 2002, Bill No 8 of 2022 before Parliament by Honourable Minister for State President Kabo N.S. Morwaeng", paragraph 3.
239. Media Practitioners Association Act, 2022, sections 6-7.
240. Id, Parts III and IV.
241. Id, Part IX.
242. Id, section 37(1).
243. Id, section 38.
244. Id, section 44.
245. Memorandum to the Media Practitioners' Association Bill, Bill No. 8 of 2022 (on file with the authors).
246. "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 8.
247. "Analysis of the Botswana Media Practitioners' Association Bill, 2022", MISA, page 3.
248. Id.
249. Id, pages 3-4; "Press Freedom in Botswana 2022", International Press Institute, February 2023, pages 8-9; Anton Harber, "Botswana Media Practitioner Act is a threat to freedom of the media", *Daily Maverick*, 28 September 2022.
250. Professor Tachilisa Balule was interviewed via Zoom on 13 July 2023.
251. "Reinforcing media freedom and the safety of journalists in the digital age", Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/HRC/50/29, 20 April 2022, paragraph 15.
252. Anton Harber, "Botswana Media Practitioner Act is a threat to freedom of the media", *Daily Maverick*, 28 September 2022
253. "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 7.
254. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 4: Botswana", Konrad Adenauer Stiftung, 2021, pages 109-110.
255. *Media Publishing (Pty) Ltd v The Attorney-General and Another* 2001 (2) BLR 485 (HC), summarised and analysed by Global Freedom of Expression here.
256. *Odong Ocaya v Francistowner (Pty) Ltd t/a The Voice Newspaper and Others* (2464 OF 2004) [2008] BWHC 268 (21 August 2008), paragraph 89.
257. *Good v Republic of Botswana* (2010) AHRLR 43 (ACHPR 2010), summarised and analysed by Global Freedom of Expression here.
258. Id, paragraphs 59, 118, 120 and 146.
259. Id, paragraph 199.
260. Id, paragraph 200.
261. Id, paragraph 198.
262. "2023 World Press Freedom: Botswana", Reporters Without Borders.
263. "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 6.
264. "'I am a warrant myself': State security agents detain journalists in Botswana", *news24*, 21 July 2023.
265. "Botswana journalist Tshepo Sethibe criminally charged over 'alarming publications'", Committee to Protect Journalists, 19 July 2022; "2022 Country Reports on Human Rights Practices: Botswana", US State Department, section 2A.
266. Melusi Simelane, "False news or free speech: Protecting freedom of expression in Botswana", Southern Africa Litigation Centre, 3 May 2023; "Challenging Criminal Code on Alarming Publications in Botswana", Southern Africa Litigation Centre, 22 March 2023.
267. Southern Africa Litigation Centre, Facebook message, 19 May 2023.
268. "Botswana police charge Moeladilotlhoko News Boiler staff with criminal trespass", Committee to Protect Journalists, 2 June 2021.
269. "News editor in Botswana faces jail time over Facebook posts, alleges suffocation by police", Committee to Protect Journalists, 5 May 2021; Jonathan Rozen, "Equipped by US, Israeli firms, police in Botswana search phones for sources", Committee to Protect Journalists, 5 May 2021; "Coronavirus: Censorship is not the cure", Ink Centre for Investigative Journalism, 23 April 2020.
270. "Journalists arrested, charged with 'nuisance' in Botswana", Committee to Protect Journalists, 29 June 2020; "President Masisi and the illusion of change", Ink Centre for Investigative Journalism, 19 June 2020
271. "A Zimbabwean Man Arrested in Botswana for Publishing False Information On Social Media", *Afrinews 247*, 4 July 2020.

272. "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 11. The appellate case could not be located online.
273. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 24.
274. Seth Sarefo, Banyatsang Mphago & Maurice Dawson, "An analysis of Botswana's cybercrime legislation", *Procedia Computer Science*, Volume 219, 2023, pages 1023-1033, Section 1, Introduction.
275. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 14.
276. *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
277. SADC Model Law on Computer Crime and Cybercrime, section 4.
278. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], pages 14 and 30.
279. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 23.
280. Id.
281. Id, page 17.
282. Id, page 16.
283. Id, page 23.
284. Id, page 21.
285. For a brief overview, see "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], pages 21-23.
286. "Misa Botswana Press Release on Mr Daniel Kenosi", *The Patriot on Sunday*, 5 April 2015; "Daniel Kenosi sued for 25000", *Razi 24*, 26 February 2019; "Kenosi to swallow P250K bitter pill", *Mmegi online*, 27 February 2019.
287. In a case involving a report of an extramarital affair, a newspaper published a photo of a partially unclothed woman, alleging that the public has a right to be informed of current news and events. The person pictured won damages against the newspaper for invasion of privacy. The High Court pointed out that the story could have been told without the photograph. *Esterhuizen v Francistowner (Pty) Ltd T/A Voice Newspaper* (CVHFT-000621-11) [2012] BWHC 61 (12 October 2012).
288. "Cyber bullying must be dealt with thoroughly", *Weekend Post,* 10 October 2017.
289. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 25. A similar point is made in "LEXOTA Country Analysis: Botswana", last updated July 2022.
290. Penal Code [*Chapter 08:01*], section 92.
291. Id, section 140.
292. Cybercrime and Computer Related Crimes Act, 2018, section 24.
293. Id, section 25.
294. Id, section 26.
295. Id, sections 27-28.
296. Id, section 30.
297. Id, section 29.
298. Botswana Cybercrime and Computer Related Crimes Act, 2018, section 31(1).
299. Penal Code [*Chapter 08:01*], section 59.
300. "LEXOTA Country Analysis: Botswana", last updated July 2022.
301. Penal Code [*Chapter 08:01*], section 176, as amended by the Penal Code (Amendment) Act 21 of 2018.
302. Id, sections 192-199.
303. Id, section 33 (which applies when no penalty is otherwise specified in the law).
304. Id, sections 50-51.
305. Id, section 51(1)-(2).
306. Id, section 51(4).
307. Id, section 51(5).
308. "Press Freedom in Botswana 2022", International Press Institute, February 2023, page 11.
309. Penal Code [Chapter 08:01], section 134.
310. Id, section 60.
311. Id, section 93.
312. Id, section 47. There is a separate provision of the Penal Code on "traffic in obscene publications" (section 178).
313. Id, section 2: "'publication' includes all written and printed matter, and any gramophone or other record, perforated roll, recording tape or wire, cinematograph film or other contrivance by means of which any words or ideas may be mechanically produced, represented or conveyed, and everything, whether of a nature similar to the foregoing or not, containing any visible representation or by its form, shape or other characteristics, or in any manner capable of producing, representing or conveying words or ideas, and every copy or reproduction or any publication".
314. Id, section 48.

315. Id, section 49.
316. Id, section 92.
317. Id, section 140.
318. Communications Regulatory Authority Act 19 of 2012, section 2.
319. Id, section 8(1).
320. Id, section 50(3)-(5).
321. Id, section 54(2).
322. Id, section 53.
323. Id, section 55.
324. "LEXOTA Country Analysis: Botswana", last updated July 2022.
325. Jonathan Rozen, "Botswana journalists remain 'vigilant' under new surveillance law", Committee to Protect Journalists, 4 May 2022.
326. Id, section 23.
327. Id, section 24(1).
328. Id, section 24(2)-(3).
329. Id, section 25.
330. Id, section 28.
331. Id, Schedule: paragraph 1.
332. Id, section 14 and Schedule.
333. Counter-Terrorism Act 24 of 2014, section 20. This link is to the original version of the Act, which has been amended several times. See Tachilisa Badala Balule, "Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework", Media Policy and Democracy Project, November 2021, pages 10, 14.
334. Intelligence and Security Services Act 16 of 2007, sections 22, 5(1)(h) and 2 (definition of "threats to natinal security"). See Tachilisa Badala Balule, "Surveillance of Digital Communications in Botswana: An Assessment of the Regulatory Legal Framework", Media Policy and Democracy Project, November 2021, pages 11-15.
335. Broadcasting Regulations, 2004, regulation 11.
336. Broadcasters' Code of Practice, item 1
337. Id, section 50(3)-(5).
338. Electronic Communications and Transactions Act 14 of 2014, section 44 read with sections 41-43.
339. Botswana's 1966 Constitution with amendments through 2016, Article 32.
340. Id, Articles 65A and 66.
341. "Botswana Country Report 2022", Bertelsmann Transformation Index (BTI), Bertelsmann Stiftung, "Executive Summary".
342. A clear and searchable copy of this law can be found here, but it is amended only up to 2008. A less clear copy that is not searchable, but contains amendments up to 2012, can be found here on the website of Botswana's Independent Electoral Commission. Press reports discuss an *Electoral (Amendment) Bill No. 6 of 2023*. A copy of the Bill appears to be available here, but only to subscribers. See "Morwaeng Tables Electoral Act Amendment Bill 2023", *Daily News*, 30 March 2023; "Electoral Act Amendment Imminent", *Africa Press*, 24 February 2023.
343. Broadcasters' Code of Practice, item 1.
344. A draft data protection law dated 2014 does not appear to have been enacted: Loi n°14-029/AU Portant protection des données à caractère personne, which can be downloaded here.
345. A more detailed overview of the laws, policies and institutions relating to Information and Communications Technology in Comoros can be found here (last updated 23 May 2023).
346. "Conseil National de la Presse et de l'Audiovisuel website", home page and "Nos Principes".
347. "Comoros: National Regulation Authority of Information and Communications Technology (ANRTIC)", Global Edge, undated. ANRTIC is established by "Le Décret N°09-065/PR du 20 mai 2009, portent creation, organisation et fonctionnement de l'Autorité Nationale de Régulation des Technologies de l'Information et de la Communication".
348. ANRTIC website, "Missions". The key law enforced by ANRTIC is Le Décret n°14-197/PR portant promulgation de la loi n°14-031/AU du 17 mars 2014 relative aux communications électroniques (Decree No. 14-197/PR promulgating Law No. 14-031/AU of March 17, 2014 relating to electronic communications).
349. Loi N°14-031, Article 6. The organization and functioning of ANRTIC are set by decree. Id, Article 7.
350. Le décret n°22-002/PR portant promulgation de la loi n°21-011/AU du 08 juin 2021 portant "Code de l'Information et de la Communication en Union des Comores".
351. "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A. Because the text of the law could not be sourced online, the discussion here is based on the summary of the law in Chamsoudine Said Mhadji, "Code de l'information et de la communication I Les qualités, les devoirs et les droits d'un journaliste, selon la loi", *Al-watwan,* 21 January 2022.
352. Loi n°21-011/AU du 08 juin 2021, Article 153
353. Id, Articles 154-155.
354. Id, Article 158: "in the exercise of his profession, the professional journalist has free access to sources of information".
355. Id, Article 159: "the journalist is not required to disclose his sources and cannot, in this case, be troubled by the public authority".
356. Id, Articles 161, 163.
357. Id, Article 166.

358. The 2018 Constitution abolished the Constitutional Court, which was previously the country's highest judicial authority. Its duties have been transferred to a new Supreme Court chamber. "Comoros: Country Strategy Paper 2021-2025, Revised Version", African Development Bank Group, paragraph 2.1.1; "Freedom in the World 2022: Comoros", Freedom House, section A3.
359. See the ICCPR status list maintained by the UN Treaty Body Database here.
360. Comoros' 2018 Constitution, Article 8.
361. Id, Article 91.
362. See, for example, "Towards A More United & Prosperous Union of Comoros: Systematic Country Diagnostic", World Bank Group, [2019].
363. "Freedom in the World 2022: Comoros", Freedom House, section F1.
364. "2023 World Press Freedom: Comoros", Reporters Without Borders.
365. "2022 Country Reports on Human Rights Practices: Comoros", US State Department, Executive Summary.
366. "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.
367. "2023 World Press Freedom: Comoros", Reporters Without Borders, "Legal Framework".
368. "Comoros: RSF denounces the abusive judicial proceedings against four journalists?", Reporters Without Borders, 21 June 2023; "2023 World Press Freedom: Comoros", Reporters Without Borders, "Safety".
369. "Comorian journalists detained, accused of participating in protests", Committee to Protect Journalists, 21 January 2021. Two dates appear on this article: 21 January 2021 and 21 January 2020; it is not clear which date is correct.
370. At that time, the relevant law was the Penal Code, "Loi N°- 082 P/A.F - Loi 95-012/AF portant Code pénal (Crimes et délits)" , Article 254. A new Penal Code is now in force.
371. "Comoros journalist Oubeidillah Mchangama held for 3 days over Facebook posts", Committee to Protect Journalists, 22 December 2020; "Heavy penalty for Comorian journalist for Facebook post if convicted", Committee to Protect Journalists, 5 January 2021.
372. "Two senior state broadcast journalists suspended in Comoros", Reporters Without Borders, 4 February 2020.
373. "Comoros: Journalist threatened for exposing flaws in handling of coronavirus crisis", Reporters Without Borders, 7 April 2020.
374. "Two journalists held in pretrial detention since February in Comoros", Committee to Protect Journalists, 26 March 2019.
375. "Comoros authorities detain journalist, censor newspapers amid political crisis", Committee to Protect Journalists, 10 April 2019.
376. Id.
377. "Freedom in the World 2022: Comoros", Freedom House, section D4.
378. Decret n° 21-018/PR portant promulgation de la loi n°20-038/AU du 29 décembre 2020, portant Code Pénal. The Penal Code contains Chapter IV (Articles 449-505) on cybercriminality ("*la cybercriminalité*").
379. Decret n° 22-003/PR portant promulgation de la loi N°21-012/AU du 25 juin 2021 relative à la Cyber Sécurité et à la Lutte contre la Cybercriminalité en Union des Comores.
380. Loi N°21-012/AU, Article 150.
381. Id, Article 1.
382. Penal Code, Article 449.
383. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
384. Id, Article 474.
385. Id, Article 505.
386. Penal Code, Article 461.
387. Id, Article 472.
388. Id, Article 504.
389. Id, Article 479-481.
390. Id, Article 482.
391. Id, Article 486.
392. Id, Article 488.
393. Id, Article 489.
394. Id, Article 490.
395. Id, Articles 483-485.
396. Id, Article 287.
397. Loi N°21-012/AU, Article 2.
398. Id, Articles 6-7.
399. Id, Article 18.
400. Id, Articles 53-63.
401. Loi N°21-012/AU, Articles 133 and 89.
402. Id, Articles 87 and 134.
403. Id, Articles 105-106.
404. Id, Articles 107-108.
405. Id, Articles 116 and 136.
406. Id, Articles 137-138.
407. Id, Articles 139-140 and 143.
408. Id, Article 144.

409. Id, Articles 141 and 145.
410. Id, Articles 109-114.
411. Id, Article 115.
412. Article 300 of the Penal Code prohibits any "act of a sexual nature contrary to mores or against nature".
413. "LEXOTA Country Analysis: Comoros", last updated July 2022.
414. Id.
415. "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.
416. "Comoros: Full Country Dossier", Open Doors International/World Watch Research, January 2023, pages 20 and 23 (writing from a Christian perspective).
417. "2022 Report on International Religious Freedom: Comoros", US State Department, Office of International Religious Freedom, "Executive Summary".
418. Loi N°14-031, Article 69.
419. Id, Article 70.
420. Loi N°21-012/AU, Article 67.
421. "2022 Country Reports on Human Rights Practices: Comoros", US State Department, section 2A.
422. "Which governments impose SIM-card registration laws to collect data on their citizens?", *comparitech*, 20 March 2023.
423. "Democratic Republic of Congo: Council of Ministers authorises ratification of Malabo Convention", alt.advisory, 27 January 2023.
424. Loi n° 11/002 of 20 janvier 2011, amending Articles 71, 110, 126, 149, 197, 198, 218 and 226.
425. Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, Article 74.
426. Hogan Lovells, "DRC Overview: Guidance Note", Data Guidance, September 2022; "Recent developments in African data protection laws - Outlook for 2023", Lexology, [2022]; Jean-François Henrotte, "Protection des données en RDC", Lexing, [2023]. Other relevant laws on this topic are Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies") and L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Law no. 23/010 of 13 March 2023, the "Digital Code").
427. Proposed Law on Access to Information (Proposition de Loi Relative a l'Access a l'Information). This law was passed by the Senate (the upper chamber of Parliament) in 2015, but not ratified by the National Assembly. See "Democratic Republic of Congo", PPLAAF, 2021; "Democratic Republic of Congo: High Commissioner update", UN High Commissioner for Human Rights, 30 March 2023.
428. Loi organique n° 11/001 du 10 janvier 2011 portant composition, attribution et fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication ("Organic Law No. 11/001 of January 10, 2011 on the composition, attribution and functioning of the High Council for Broadcasting and Communication"). Note that Article 160 of the 2005 Constitution requires that all Organic Laws must be submitted to the Constitutional Court for a ruling on their conformity with the Constitution before they are promulgated. Internal regulations of the CSAC must also be submitted to the Court for a ruling on their constitutionality before they are applied.
429. Loi organique n° 11/001, Articles 8-10, as translated and summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 206 (hereinafter "Limpitlaw").
430. Loi organique n° 11/001, Articles 24 and 26.
431. Id, Article 4.
432. Id, Article 57.
433. Id, Articles 58-59; Limpitlaw, pages 206-207.
434. Id, Articles 68 and 74.
435. See id, Article 62.
436. id, Article 6.
437. Oscar Bisimwa, "Urgent : le CSAC suspend le journaliste Louis-France Kuzikesa et sa chaîne CML13 TV", *Congo Reformes*, 22 mai 2023.
438. This body was first created by Loi n°014/2002 du 16 octobre 2002, which was later replaced by Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies"). A table comparing the key points in these two laws can be found on the ARPTIC website here.
439. Limpitlaw, page 209. Note that Limpitlaw's analysis does not cover the modifications made by the 2017 Telecommunications Law. Note also that the "Press Freedom Law" referred to in Limpitlaw is the 1996 version and not the one enacted in 2023.
440. Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies").
441. Id, Article 52.
442. Limpitlaw, page 208: "The DRC has more than one regulatory authority for broadcasting and signal distribution. While regulators are established in terms of a number of different statutes, it is clear that real power in respect of broadcasting resides in the executive branch of government and, in particular, with the Ministry of Press and Information. Despite being

a constitutionally mandated body, the [CSAC] operates alongside a Regulatory Authority [ARPTIC], which deals with technical matters, and is overshadowed by the very real powers exercised by the executive".
443. Ministerial Decree 04/MIP/020/96, dated 26 November 1996.
444. Ministerial Decree 04/MCP/011/2002, dated 20 August 2002.
445. Ministerial Decree 04/MIP/006/97 dated 28 February 1997.
446. Limpitlaw, pages 226-229.
447. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
448. **L'Ordonnance-Loi n°23/009 du 13 mars 2023** fixant les modalites d'exercice de la liberté de presse, la liberté d'information et d'emission par la radio et la télévision, la presse écrite ou tout autre moyen de communication en République Démocratique du Congo ("Ordinance-Law N°23/009 of March 13, 2023 fixing the procedures for the exercise of freedom of the press, freedom of information and emission by radio and television, the written press or any other means of communication in Democratic Republic of Congo") ("Press Freedom Law"). This law could not be located online as of mid-2023, but a copy is on file with the authors. It replaces Law no. 96/002 of 22 June 1996.
449. L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
450. **L'Ordonnance-Loi n°23/009**, Articles 1 and 82.
451. Id, Article 15.
452. Id, Article 2.
453. Id, Article 140.
454. "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders, "Legal Framework".
455. Prince Mayiro, "RDC - Ass. Nat: Porté par Muyaya, le projet de loi de ratification de l'ordonnance-loi sur la liberté de la presse et la liberté d'information adopté",*7sur7.cd*, 5 avril 2023: "*Cette loi permet de résoudre un nombre important de problèmes qui dérangent ce secteur au quotidien, entre autres, les dérapages et la non-conformité de certains médias, surtout les médias d'informations en ligne qui, avec l'évolution technologique, avancent avec une rapidité remarquable.*" See also "Ordonnance loi fixant modalités de l'exercice de la liberté de la presse en RDC, Assemblée nationale : Patrick Muyaya explose et passe!", *Publié par La Prospérité*, 5 avril 2023.
456. Compare Articles 23 and 24 of the Democratic Republic of the Congo 2005 Constitution quoted on the first page of this chapter.
457. Id; "DRC enacts press law and digital code that criminalize journalism", Committee to Protect Journalists, 23 May 2023.
458. "La RDC se dote d'une nouvelle Loi sur la Presse, moins répressive, mais plus contraignante, à quelques mois des élections à hauts risques", statement by Journaliste en Danger (JED), *deskeco.*, 7 avril 2023.
459. Id, Article 3 (item 11).
460. Id (item 20).
461. Id, Articles 8-12, 93
462. Id, Article 94.
463. Id, Article 59.
464. Id, Article 6.
465. Id, Article 84.
466. Id, Articles 64-66.
467. Id, Articles 67-70.
468. Id, Article 77.
469. Id, Article 3 (item 14).
470. Id, Article 80.
471. Id, Articles 87- 88.
472. Id, Article 92.
473. "Les attributions du Conseil Supérieur de l'Audiovisuel et de la Communication, CSAC en sigle", Edmond Mbokolo Eilima, *LegaVox*, 11 mai 2023.
474. **L'Ordonnance-Loi n°23/009**, Article 91.
475. Id, Articles 95-97.
476. Id, Article 104.
477. Id, Articles 105-111.
478. Id, Article 112.
479. "The Democratic Republic of Congo takes a significant step in digital with the ratification of the Digital Code", *fatshimetrie*, 23 August 2023.
480. L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code"), Article 7
481. L'Ordonnance n° 81/050 du 2 avril 1981 (not found online). See also Décret n°09/62 du 03 décembre 2009 fixant les statuts d'un établissement public dénommé Radio-Télévision Nationale Congolaise, en sigle « RTNC », which changed its name from "*L'Office Zaïrois de Radio diffusion et de television*" (OZRT) to "*Radio Télévision Nationale Congolaise"* (RTNC).
482. Limpitlaw, page 216.
483. It is currently regulated in terms of L'Ordonnance n° 81/052 du 2 avril 1981 (not found online).
484. Tresor Musole Maheshe was interviewed via Zoom on 25 July 2023.
485. Limpitlaw, page 187.
486. Id, page 183 (footnotes omitted).
487. "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders.

488. "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
489. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
490. "Congolese soldiers arrest, beat 3 journalists covering land dispute", Committee to Protect Journalists, 30 June 2023.
491. "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
492. Id
493. Id.
494. "Congolese journalist John Ngongo Lomango arrested over conflict reporting", Committee to Protect Journalists, 28 March 2023; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
495. "DRC defence minister files, withdraws false news complaint against reporter Stanis Bujekera", Committee to Protect Journalists, 14 March 2023.
496. "DRC broadcaster Radio Tokomi Wapi suspended, police shutter station", Committee to Protect Journalists, 18 January 2023.
497. "DRC authorities detain 2 journalists for 48 hours over reporting on alleged secret jails", Committee to Protect Journalists, 12 January 2023.
498. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 1E. The report views these persons as political prisoners and detainees.
499. "Patrick Lola Imprisoned", Committee to Protect Journalists, 10 January 2022; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
500. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
501. Id, section 1E
502. Id, section 2A.
503. Joel Simon, Carlos Lauría and Ona Flores,"Weaponizing the Law: Attacks on Media Freedom", Thompson Reuters Foundation and Tow Centre for Digital Journalism, April 2023, page 18.
504. "Governor of DRC's Equateur province defies court order allowing Radio Télévision Sarah to reopen", Committee to Protect Journalists, 13 June 2023; "In DRC, provincial governor blocks radio station's bid to resume broadcasting", Reporters Without Borders, 20 June 2023.
505. "DRC: Drop Defamation Charges Against Human Rights Defender", Amnesty International Public Statement, AFR 62/3924/2021, 30 March 2021.
506. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
507. Limpitlaw, page 221.
508. Such moves could also have been implemented by ARPTIC under Article 3(i) of Loi n° 014-2002 du 16 octobre 2002 portant création de l'Autorité de régularisation de la poste et des télécommunications which empowers it to protect the public interest. Limpitlaw, page 221. (Limpitlaw also mentions the Telecommunications Act 13-2002 of 16 October 2002 as possible authority, but this law was repealed by Article 202 of Law 20/17.)
509. "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019**,** page 9 (footnote omitted).
510. Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication (Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies). This law is administered by ARPTIC, under the supervision of the relevant minister. Id, Articles 12-13.
511. L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
512. Id, Article 389.
513. Loi n° 20/17, Article 154.
514. "Est punie de un à trois ans de servitude pénale principale et/ou d'une amende de 1.000.000 à 10.000.000 de francs congolais, toute interception, écoute, enregistrement, transcription au moyen d'un quelconque dispositif pour divulgation d'une communication ou correspondance privée."
515. "Est puni d'une peine de servitude pénale principale d'un mois à un an et/ou d'une amende de 50.000.000 à 100.000.000 de Francs congolais, toute personne qui perturbe, en utilisant, sans titre, une fréquence ou une installation radioélectrique, les émissions hertziennes d'un service autorisé."
516. "*Quiconque accède ou se maintient frauduleusement dans tout ou partie d'un système de communication électronique est puni d'une servitude pénale de six mois à trois ans et d'une amende 1.000.000 à 10.000.000 de francs congolais ou de l'une de ces peines seulement*".
517. "*Est également puni des mêmes peines, celui qui se procure poir soi-même ou pour autrui, un avantage quelconque, en s'introduisant ou se maintenant frauduleusement dans tout ou partie d'un système de communication électronique.*"
518. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
519. Code pénal congolais, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006. Article 174 applies to "any representation by any means whatsoever, of a child engaging in sexual activities explicit, real or simulated, or any representation of the sexual organs of a child, for primarily sexual purposes".
520. Code pénal congolais, Articles 184-185. The Penal Code provides separate offences for Congolese citizens (treason) and for foreigners (espionage). The cybercrime offence applies to "any person".
521. Loi n° 20/17, Article 192.
522. Id, Articles 92-95.
523. Id, Articles 156-157 and 172-173.

524. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 26. The ministerial order referenced in this source could not be located online.
525. See id, page 25 for more details.
526. L'Ordonnance-Loi n°23/010, Article 331: "*Les infractions de droit commun commises au moyen d'un ou sur un reseau de communication electronlque ou un svsterne informatique sont reprirnees conforrnernent au Code penal congolais et aux dispositions penales particulleres en vigueur*."
527. Id, Article 332: "*Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un svsteme informatique, avec une intention frauduleuse est puni dune peine de servitude penale de trois a cinq ans et d'une amende de clnquante millions a cent rnllllons de francs Congolais ou de l'une de ces peines seulement."*
528. Id: "*Quiconque, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'acces legal a un svsterne informatique, est puni d'une peine de servitude penale de deux a cinq ans et d'une amende de cinquante millions a cent millions de francs congolais ou de l'une de ces peines seulement*."
529. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
530. L'Ordonnance-Loi n°23/010, Article 332: "*Est puni d'une servitude penale de six moi à trois ans et d'une amende de cinq millions a cent millions de francs conqolals, celui qui transfère, sans autorisation de la personne concernée, des données à caractère personnel de cette dernière d'un systerne informatlque ou d'un moyen de stockage de données vers un autre."*
531. Id, Article 339: "*Quiconque commet un faux en introduisant, intentionnellement et sans droit, dans un système informatique ou un réseau de communication électronique, en modifiant, en altérant ou en effaçant des données qui sont stockées, traitées ou transmises par un système informatique ou un réseau de communication électronique ou en modifiant par tout autre moyen technologique, l'utilisation possible des données dans un système informatique ou un réseau de communication électronique, et par la modifie là portée juridique de telles données, est puni d'une servitude penale de trois a cinq ans et d'une amende de·vingt millions a cinquante millions de francs congolais, ou l;une de ces peines seulement*."
532. Id, Articles 341-347.
533. Id, Article 356: "*Quiconque aura, intentionnellement, créé, téléchargé, diffusé ou mis à la disposition du public par le biais d'un systems informatique des écrlts, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idees ou de théories, de idées raciste, tribaliste ou xénophobe ou sous quelque-forme que ce soit […]*":
534. Id, Article 372: "*Le présent article n'est pas applicable lorsque l'enregistrement soit la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public soit lorsqu'il est réalisé afin de servir de preuve en justice*."
535. Id, Article 364.
536. Id, Article 282: "*Le fournisseur des services en ligne est tenu détenir et de conserver les données de nature à permettre l'identification de quiconque aura contrlbué à la création du contenu ou de l'un des·contenus des services dont ils sont prestataires.*
Il est également tenu de fournir aux personnes qui éditent un service de communication au public en ligne des garanties permettant à celles-ci de satisfaire aux conditions d'identification prévues à la présente ordonnance-loi.
L'Officier du Ministère Public ou l'Autorité protection des données peut requerir aupres des fournlsseurs de services en ligne, conformément à la loi en la rnatiere, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées à alinéa 1 du présent article."
537. Id, Article 288.
538. Id..Similar rules apply to caching and linking to illegal information. Id, Articles 290-291.
539. Id, Article 287.
540. Id, Article 285. The statute refers to notification of *one* of the listed elements ("*La connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il·lui est notifié l'un des elements suivants…*"), but it appears to be intended to refer to a notification containing the listed elements.
541. Id, Article 365.
542. Id, Article 286.
543. Id, Article 287.
544. Id, Article 287: *Ils sont éqalement tenus, d;une part,d'informer et prompternent les autorités compétentes de toutes activités illicites mentionnées qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part suspendre tout contenu sussceptible de porter atteinte à la moralité*".
545. Id.
546. Id, Articles 366-368.
547. Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006 modifiant et complétant le Décret du 30 janvier 1940 portant Code pénal congolais.
548. "LEXOTA Country Analysis: Democratic Republic of Congo", last updated July 2022.
549. Code pénal congolais, Article 150h-150i.
550. **L'ordonnance-loi n°23/009**, Article 113.
551. Id, Article 120
552. Id, Article 124.
553. Id, Article 123.
554. Id.
555. Id, Article 124.

556. Id, Articles 125-126.
557. Id, Article 126.
558. Id, Article 136.
559. Id, Articles 127-128.
560. Trésor Maheshe Musole and Jean-Paul Mushagalusa Rwabashi, "Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection", Media Policy and Democracy Project, December 2021, page 20.
561. Id, page 21.
562. Id, page 20.
563. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 24.
564. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
565. Democratic Republic of the Congo 2005 Constitution, Article 211. CENI is governed by the Loi organique n° 10/013 du 28 juillet 2010 portant organisation et fonctionnement de la Commission Électorale Nationale Indépendante telle que modifiée et complétée par la Loi organique n° 13/012 du 19 avril 2013 et la Loi organique n° 21/012 du 03 juillet 2021 (Textes coordonnés et mis à jour) ("Organic Law No. 10/013 of 28 July 2010 on the organization and functioning of the Independent National Electoral Commission as amended and supplemented by Organic Law No. 13/012 of 19 April 2013 and Organic Law No. 21/012 of 03 July 2021 (Coordinated and updated texts)"). The CENI website can be found here.
566. "Freedom in the World 2022: Democratic Republic of the Congo", Freedom House, section A3; Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
567. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 182 (footnotes omitted).
568. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 3.
569. "Democratic Republic of the Congo 2018 Harmonized Presidential, Parliamentary and Provincial Elections: Expert Mission Report", The Carter Center, undated.
570. Id.
571. "UN expert urges DRC to restore internet services", UN Office of the High Commissioner on Human Rights, 7 January 2019.
572. "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, "Executive Summary".
573. Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
574. Christel Insiwe "Élections: Le CSAC adopte la directive de réglementation de la campagne électorale dans les medias", *7sur7.cd*, 22 juin 2023; Emille Kayomba, "Processus électoral : le CSAC et la CENI en concertation pour des bonnes élections", *b-onetv*, 14 juillet 2023.
575. As a point of comparison, the previous "Directive du Conseil Supérieur de l'Audiovisuel et de la Communication n°CSAC/AP/001/2015 du 05 mars 2015 relative à la campagne électorale à travers les medias" is available here.
576. Data Protection Act 5 of 2022.
577. Books and Newspapers Act 20 of 1963, section 4. A "newspaper" is defined in section 2 to include "any printed matter containing news, or intelligence, or reports of occurrences of interest to the public or any section thereof, or any views, comments or observations thereon printed for sale or distribution and published periodically or in parts or numbers at intervals not exceeding one month but does not include a visiting or business card, billhead, letter-head, price list, annual report, trade circular, trade advertisement or other legal or trade or business document".
578. The Swaziland Communications Commission Act 10 of 2013, read with section 6 of The Public Enterprises (Control And Monitoring) Act 8 of 1989.
579. The Swaziland Communications Commission Act 10 of 2013, section 6.
580. Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
581. The Swaziland Television Authority Act, 1983, sections 9-10 in particular.
582. Personal communication with local expert, July 2023.
583. Sifiso Nhlabatsi, "Parliament Passes Broadcasting Bill", *Eswatini Observer*, 16 October 2020; "Eswatini Broadcasting Bill heralds new hope", *Inhlase*, 31 October 2020; "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), section 3.
584. "Eswatini: Misa Applauds Registration of Media Complaints Commission", Media Institute of Southern Africa (Windhoek) press release, 15 June 2011.
585. "Freedom of the Press 2016 – Swaziland", Freedom House, "Legal Environment".
586. "African Media Barometer: Eswatini 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 47.
587. Journalist quoted anonymously in Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
588. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 246.

589. *Swaziland Independent Publishers v The King* [2014] SZSC 25, 30 May 2014; see the case summary by Global Freedom of Expression here.
590. *Maseko v R* [2015] SZSC 03, 29 July 2015; see the case summary by Global Freedom of Expression here.
591. *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016; see the case summary by Global Freedom of Expression here. See also Angelo Dube and Sibusiso Nhlabatsi, "The (Mis)application of the Limitation Analysis in *Maseko and others v Prime Minister of Swaziland and others*" [referring to the dissenting judgment], *Law, Democracy and Development*, Vol 22, 2018.
592. Peter Fabricius, "Historic Swazi court judgment striking down parts of sedition and terrorism laws is under threat", *Daily Maverick*, 29 September 2022,
593. "eSwatini: Experts condemn killing of human rights defender Thulani Maseko, demand accountability", UN Office of the High Commissioner on Human Rights, 26 January 2023; Pavan Kulkarni, "Assassination of Thulani Maseko has killed prospects of peaceful struggle in Swaziland", *People's Dispatch*, 27 January 2-23.
594. "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Legal framework".
595. Id, "Safety".
596. "2022 Country Reports on Human Rights Practices: eSwatini", US State Department, section 2A.
597. Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021, quoting Nqaba Matshazi, MISA's fundraising and regional campaigns coordinator.
598. Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 3.
599. "eSwatini prison officers assault, threaten to shoot reporter covering pro-democracy protest", Committee to Protect Journalists, 16 February 2022.
600. "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.
601. "More delays as Eswatini MPs languish in jail", Southern Africa Litigation Centre, 22 September 2021.
602. "Swazi editor flees to South Africa, wanted in false news investigation", Committee to Protect Journalists, 15 May 2020. Dlamini had previously received death threats from a local businessman, in 2017, in connection with an article about the King's involvement in a corruption case. He fled to South Africa at that stage, and his newspaper, ,*Swaziland Shopping,* was shut down by the government. He returned to Swaziland in 2018 after the businessman who had threatened him passed away. "2023 World Press Freedom: eSwatini", Reporters Without Borders, "Safety.
603. "eSwatini editor receives death threats over pro-government article", Committee to Protect Journalists, 13 July 2020. The opposition party in question denied that the person who sent the threats was their member.
604. "Swaziland journalists harassed, threatened with treason charges over reporting on king", Committee to Protect Journalists, 30 April 2020. Police apparently searched for Mthobisi Ntjangase, the reporter who wrote the other article, but could not find him.
605. "Id. The *Independent News report referred to appears to be no longer available online.*
606. Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020.
607. Joint submission by the Women and Law in Southern Africa Research and Educational Trust Eswatini (WLSA) and the Advancing Rights in Southern Africa (ARISA) Program on Eswatini to the 39th Session of the Working Group on the Universal Periodic Review (undated), page 10.
608. Vuyisile Hlatshwayo, "'Climate of fear' in eSwatini media", *Mail & Guardian*, 11 November 2020,
609. "eSwatini police detain, abuse 2 reporters from South African outlet New Frame", Committee to Protect Journalists, 8 July 2021.
610. Ronja Koskinen and Helsingin Sanomat, "Crackdown on press freedom in Eswatini", International Press Institute, 7 July 2021.
611. "Freedom in the World 2022: Eswatini", Freedom House, section D1.
612. Computer Crime & Cybercrime Act 6 of 2022, section 1.
613. Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022.
614. The Bill originally included a prohibition on the publication of "any statement or fake news through any medium, including social media with the intention to deceive any other person or group of persons" (section 19). "LEXOTA Country Analysis: Eswatini", last updated July 2022.
615. Ndimphiwe Shabangu,"eSwatini passes cyber laws under dark clouds", Association for Progressive Communications, 23 August 2022; "Fears that cybercrime bill will hit eSwatini's media freedom", The Economist Intelligence Unit, 14 September 2020.
616. Computer Crime & Cybercrime Act 6 of 2022, section 2 (definition of "Commission") and section 52.
617. Id, section 53.
618. "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022. This article cites the Botswana Cybercrime and Computer Related Crimes Act 18 of 2018 as a point of comparison, where a similar offence attracts a maximum fine of P20 000 (equivalent to E27 200) or imprisonment for a maximum of one year, or both. In Botswana, the related offence of unauthorised access to a computer service *with the intent to intercept data* attracts a doubled maximum penalty – which is still significantly less than the eSwatini penalty.
619. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
620. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 15.
621. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.

622. Id.
623. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
624. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
625. Id. SALC believes that this offence was incorrectly transcribed from the SADC Model Law.
626. Id.
627. Id.
628. Id.
629. Id.
630. "Computer, Cybercrime act: a necessary evil", *Times of Eswatini*, 31 October 2022.
631. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
632. Id.
633. Id.
634. Id.
635. Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.
636. *SADC Model Law on Computer Crime and Cyber Crime, 2012*, section 22: "A person, who initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, *using a computer system to support severe, repeated, and hostile behaviour*, commits an offence…".
637. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
638. Computer Crime & Cybercrime Act 6 of 2022, section 30. Section 2 defines "abetting" as "to encourage or assist someone to commit a crime or other offence".
639. "Computer, Cybercrime Act: a necessary evil", *Times of Eswatini*, 31 October 2022.
640. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020. It cites these examples: "Using an illegal device to commit an offence can lead to a fine of E100m or 25 years' imprisonment or both (section 9), even though the offence being committed might be quite benign. In contrast, committing computer related forgery or computer related fraud can result in a lesser sentence of E10m or 10 years' imprisonment or both (section 10 and 11 respectively), but using a botnet to disrupt a service can attach E100m or 20 years' imprisonment." The SALC also noted that there is a lack of congruence between the fine and the number of years in imprisonment in respect of the various offences in the bill, but the examples it cites do not match the final law indicating that this issue was addressed.
641. Ndimphiwe Shabangu was interviewed via Zoom on 19 July 2023.
642. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
643. Computer Crime & Cybercrime Act 6 of 2022, section 33. There is a wide and non-exhaustive definition of "thing" in section 2.
644. Id, section 2 (definition of "law enforcement agent").
645. Id, section 34.
646. Id section 38. Section 2 defines "traffic data" as "computer data that relates to a communication by means of a computer system and generated by a computer system that is part of the chain of electronic communication; and may show one or more of the following, the communication's origin, destination, route, time, date, size, duration or the type of underlying services".
647. Id, section 39.
648. Id, section 40. Section 2 defines a "remote forensic tool" as "an investigative tool including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address".
649. Id, section 35.
650. Id, sections 36-37.
651. *SADC Computer Crime and Cybercrime Model Law, 2012*, section 28; "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
652. "SALC Submission on the Computer Crime and Cybercrime Bill, 2020", 13 October 2020.
653. Id.
654. Computer Crime & Cybercrime Act 6 of 2022, section 48.
655. "Report of the Working Group on the Universal Periodic Review: Eswatini", A/HRC/49/14, 7 January 2022.
656. "U.S. Statement at the Universal Periodic Review of eSwatini", U.S. Mission Geneva, 8 November 2021.
657. "Statement: Concern as states continue to use terrorism laws to inhibit freedom of expression and access to information", Southern Africa Litigation Centre, 27 September 2021.
658. *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 18.
659. Id, paragraph 21.
660. Suppression of Terrorism Act 3 of 2008, as amended by the Suppression of Terrorism (Amendment) Act 11 of 2017, section 5(3)(e).
661. Id, section 11(1)(a)-(b).
662. *Maseko v The Prime Minister of Swaziland* [2016] SZHC 180, 16 September 2016, paragraph 28.
663. "Suppression of Terrorism Act undermines Human Rights in Swaziland", Amnesty International and International Bar Association, 2009. Amnesty International made the following comments after the 2017 amendment:
Although Eswatini amended the 2008 Suppression of Terrorism Act in 2017, the Act continues to be used to silence and punish dissent. The Act's amendments limit the definitions of what constitutes a terrorist act although the wording is overly

broad and vague in relation to terrorism related acts. The law also contained provisions that undermined the rights to freedom of expression, association and peaceful assembly. The STA (Amendment) Act 2017 remains inconsistent with Eswatini's obligations under international and regional human rights law as well as Eswatini's Constitution. "Eswatini: Broken Promises" Amnesty International Submission for the UN Universal Periodic Review, 39th Session of the UPR Working Group, 1 – 12 November 2021, "Restrictions to Fundamental Freedoms".
664. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 270.
665. Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.
666. Public Order Act 12 of 2017, sections 6 9 and 15(1), read with definition of "gathering" in section 2. See also section 16 on police power to prohibit any public event where "public disorder" is likely to arise.
667. Id, section 14.
668. Id, section 15(3)(b).
669. Id, section 15(3)(h).
670. Id, section 19.
671. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 272.
672. Proscribed Publications Act 17 of 1968, sections 3-4.
673. *Swaziland Independent Publishers (Pty) Ltd T/A The Nation Magazine v the Minister of Public Service and Information* (Case 1155/01), as summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: eSwatini", Konrad Adenauer Stiftung, 2021, page 282.
674. Cinematograph Act 31 of 1920, sections 4-5.
675. Id. section 3(1).
676. Id, section 3(1bis).
677. Id, section 3(4).
678. Id, section 6.
679. Hanifa Manda, "Eswatini Freedom Of Expression Summit", Inhlase Centre for Investigative Journalism, October 2022, page 19, citing Nqobile Ndzinisa.
680. Swaziland Communications Commission (Subscriber Registration) Regulations, 2016. Legal Notice No. 126 of 2016, issued in terms of section 54 of The Swaziland Communications Commission Act 10 of 2013 (which merely provides for regulations for the better carrying out of the Act).
681. Electronic Communications and Transactions Act 3 of 2022, section 40 read with the definition of "service provider" in section 2 and with sections 37-39.
682. Id, section 40(3).
683. "Eswatini to hold parliamentary elections in September", *Agence France-Presse*, 6 May 2023.
684. Katharine Bebington, "Eswatini: the year ahead", ACCORD, 24 February 2023.
685. "Freedom in the World 2022: Eswatini", Freedom House, section A3.
686. Elections Act 6 of 2013. Note that this Act is variously referred to as Act 6 of 2013 and Act 10 of 2013, with these differing references even appearing on material on the website of The Elections And Boundaries Commission.
687. Elections Act 6 of 2013, section 42.
688. See, for example, Nomfanelo Maziya, "Some current MPs perceived as campaigning in disguise", *Swazi Observer*, 4 July 2023; Delisa Thwala, "EBC half way through their weekend target", *Eswatini Positive News*, 31 May 2023.
689. Id, section 78(1). There is a similar provision on undue influence in the Voters Registration Act 4 of 2013, section 36.
690. Mfanukhona Nkambule. "2-yr imprisonment for telling people not to vote", *Times of Swaziland*, 14 May 2023, which also quotes the contrary opinion of Sikelela Dlamini, the Secretary General of the Swaziland Multi-Stakeholder Forum.
691. Id, section 79.
692. Id, section 83(1)(d)-(e).
693. The Broadcasting Code 2020 issued by the Eswatini Communications Commission does not cover this topic.
694. Broadcasting Code 2020, item 5.10.1.3.
695. Mathatisi Sebusi, "Press incises 'draconian' cyber law", *Public Eye News*, 1 July 2023. Local observers say that, even at this stage, the bill might still be withdrawn and revised on the basis of recent civil society input.
696. *Peta v Minister of Law, Constitutional Affairs and Human Rights* (CC 11/2016) [2018] LSHC 3 (18 May 2018).
697. Data Protection Act 5 of 2012.
698. "Access to information", MISA-Lesotho, undated.
699. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 301. The text of the legislation could not be located online.
700. "Position Paper for Multi-Sectoral Reforms", Media Institute Of Southern Africa (MISA-Lesotho Chapter), undated, page 11.
701. Communications Act 4 of 2012, section 56.
702. Id, section 6.
703. Id, section 3(3).
704. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 286.
705. Personal communication from MISA Lesotho, August 2023.

706. Communications Act 4 of 2012, section 38(2). See also the Lesotho Telecommunications Authority (Broadcasting) Rules 2004, Legal Notice No. 71 of 2004,
707. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, page 308.
708. "Proposed Internet Broadcasting Rules 2020", Internet Society Lesotho Chapter, 28 October 2020; "Proposed Promulgation of the Lesotho Communications Authority (Internet Broadcasting) Rules, 2020", Internet Society Lesotho Chapter, 28 October 2020.
709. Tawanda Karombo, "More African governments are quietly tightening rules and laws on social media", *Quartz*, 12 October 2020; "LEXOTA Country Analysis: Lesotho ", last updated July 2022.
710. "Proposed Promulgation of the Lesotho Communications Authority (Internet Broadcasting) Rules, 2020", Internet Society Lesotho Chapter, 28 October 2020.
711. Personal communication from MISA Lesotho, August 2023.
712. Communications Act 4 of 2012, section 20.
713. Id, sections 39(8)(a) and 40(1).
714. Id, section 40(2)
715. Id, section 40 (3)-(5). The Broadcasting Code, 2022 can be accessed here.
716. Id, section 41.
717. Personal communication from MISA Lesotho, August 2023.
718. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 7: Lesotho", Konrad Adenauer Stiftung, 2021, pages 310-311.
719. Id, page 311.
720. Personal communication from MISA Lesotho, August 2023.
721. "Lesotho: Protecting freedom of expression and information in 2020", MISA Lesotho, 3 May 2020; personal communication from MISA Lesotho, August 2023.
722. "Parliament adopts National media policy", MISA-Lesotho, 30 November 2021.
723. Lesotho Ministry of Information, Communications, Science, Technology and Innovation website here.
724. Lesotho's 1993 Constitution, section 14(4).
725. "MISA Lesotho calls for Constitutional Amendment", MISA Lesotho, 28 April 2022; "Lesotho: Protecting freedom of expression and information in 2020", MISA Lesotho, 3 May 2020; Tsebo Matšasa, Mzimkhulu Sithetho and Dr Bob Wekesa, "The Lesotho National Dialogue and Stabilization Project Media Sector Reforms", 26 August 2019; personal communication from MISA Lesotho, August 2023.
726. *Moafrika Newspaper: Rule Nisi (Sub-Judice Matter) (In R v. Mokhantso)* [2003] LSHC 24, 17 February 2003; see case summary by Global Freedom of Expression here.
727. Section 104 of the Penal Code stated that a person "who, by print, writing, painting or effigy, or by any means otherwise than, solely by a gesture, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another, with intent to defame that other person, commits an offence of defamation." Section 101 defined "defamatory matter" as "matter likely to injure the reputation of any person by exposing him or her to hatred, contempt or ridicule, or likely to damage the person in his or her profession or trade by injury to his or her reputation, and it is immaterial whether at the time of the publication of the defamatory matter the person concerning whom the matter is published is living or dead". Penal Code Act 6 of 2012, sections 101 and 104.
728. *Peta v Minister of Law, Constitutional Affairs and Human Rights*, CC 11/2016,. 18 May 2018; see case summary by Global Freedom of Expression here.
729. "Lesotho journalist Ralikonelo Joki killed after radio show", Committee to Protect Journalists, 15 May 2023.
730. "Lesotho police arrest a radio presenter, suspend one station's license, and raid another", Committee to Protect Journalists, 14 December 2021; Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane, "Lesotho: Attacks against journalists intensify" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), pages 35-37; "Freedom in the World 2022 – Lesotho", Freedom House, section D1.
731. "Lesotho police arrest a radio presenter, suspend one station's license, and raid another", Committee to Protect Journalists, 14 December 2021; Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane. "Lesotho: Attacks against journalists intensify", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA); "Freedom in the World 2022 – Lesotho", Freedom House, section D1.
732. Reyhana Masters, "An eventful #IDEI, a milestone for Botswana's LGBTQIA+ and a unanimous vote for media freedom", 6 December 2021; Lekhetho Ntsukunyane. "Lesotho: Attacks against journalists intensify", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA).
733. This may have been intended to reference the crime of sedition, which involves amongst other things bringing the government into "hatred or contempt". Penal Code Act 6 of 2012, section76(5)(a).
734. "Lesotho military spokesman threatens investigative journalist", Committee to Protect Journalists, 21 December 2018.
735. "Lesotho authorities accuse MoAfrika FM of incitement for critical reports", Committee to Protect Journalists, 15 August 2018.
736. Id.
737. "'Media self-regulation the way to go'", *Lesotho Times*, 5 May 2017.

738. "Lesotho authorities accuse MoAfrika FM of incitement for critical reports", Committee to Protect Journalists, 15 August 2018.
739. "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, pages 10-11.
740. Penal Code Act 6 of 2012, section 62(2). There is no definition of "electronic storage device"
741. Mathatisi Sebusi, "Press incises 'draconian' cyber law", *Public Eye News*, 1 July 2023.
742. Personal communication, July 2023.
743. "Freedom in the World 2022 – Lesotho", Freedom House, section D4; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 6.
744. Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, pages 6-7; "Non-State Actors' Solidarity Key To Media Freedom", MNN Centre for Investigative Journalism, 7 June 2023.
745. "Non-State Actors' Solidarity Key To Media Freedom", MNN Centre for Investigative Journalism, 7 June 2023.
746. "Computer Crime and Cybersecurity Bill, 2022 Statement of Objects and Reasons", Senate of Lesotho, 19 May 2022.
747. Id.
748. *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
749. SADC Model Law on Computer Crime and Cybercrime, section 4.
750. "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
751. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
752. Id, page 15.
753. Id.
754. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
755. "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
756. Communications Act 4 of 2012, section 44(1)(e) read with the definition of "communications service" in section 2.
757. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 15.
758. "Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
759. Id.
760. Penal Code Act 6 of 2012, section 78.
761. Matšeliso Phulane, "Cyber law slammed, again", *The Reporter*, 15 December 2022, quoting Mokitimi Tšosane of the Transformation Resource Centre (TRC); "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 6.
762. Computer Crime and Cybersecurity Bill, 2022, clause 42.
763. Thumbs up for Parliament Portfolio Committee on Information!", MISA Lesotho, 15 September 2021 (commenting on the 2021 bill).
764. Computer Crime and Cybersecurity Bill, 2022, clause 59.
765. Id, clause 2 (definition of "law enforcement officer").
766. Id, clause 59(3).
767. Id, clause 60.
768. Id, clause 61.
769. Id. clause 62.
770. Id, clause 63.
771. Id, clause 67.
772. Id, clause 68. Clause 2 defines a "remote forensic tool" as "an investigative tool, including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks that include keystroke logging or transmission of an internet protocol address". A "direct access forensic tool" is not defined.
773. Id, clause 77.
774. National Security Services Act 11 of 1998, sections 26-27, discussed in "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, page 8. (CIPESA mistakenly refers to the Act as being dated 1997.)
775. African Media Barometer: Lesotho 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 12. See also "Lesotho: National Overview", MISA-Lesotho, 2012 at page 47 which lists 13 laws that have concerning provisions: 1. Obscene Publication Proclamation No. 9 of 1912, 2. Sedition Proclamation No 44 of 1938, 3. Printing and Publications Act, 1967, 4. Official Secrets Act, 1967, 5. High Court Act, 1978, 6. Criminal Procedure and Evidence Act, 1981, 7. Internal Security Act (General) Act, 1984, 8. Emergency Powers Order 1988, 9. National Assembly Elections Order 1992, 10. Constitution of Lesotho 1993 (Article 14(2)), 11. The Parliamentary Powers and Privileges Act, 1994, 12. Police Service Act 1998, 13. Financial Institutions Act, 1999.
776. African Media Barometer: Lesotho 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 12.
777. Id.
778. Internal Security (General) Act 24 of 1984, section 7(a) read with definition of "subversive" in section 3.
779. Id, section 13.

780. Id, section 34.
781. Penal Code Act 6 of 2012, section 85.
782. Id, section 24.
783. Penal Code Act 6 of 2012, section 84.
784. See section 8.2 of this chapter. Sections 101-104 of the Penal Code Act 6 of 2012 were struck down on constitutional grounds.
785. Penal Code Act 6 of 2012, section 77
786. Id, section 79.
787. Id, section 78.
788. Id, section 90.
789. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33 (footnote omitted and emphasis added).
790. "2022 Country Reports on Human Rights Practices: Lesotho", US State Department, section 2A; "Lesotho: Authorities Should Withdraw Communications Regulations", Freedom House, 21 June 2021; "Lesotho: Communications Regulation 2021 (Subscriber Identity Module and Mobile Device Registration)", MISA Lesotho, 8 July 2021; "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 34.
791. Communications (Subscriber Identity Module Registration) Regulations 2021.
792. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 33; Nthabiseng Pule, "Digital Rights in Lesotho", Internet Freedom Project Lesotho, 2022, pages 8-9.
793. Draft Electronic Transactions and Electronic Commerce Bill 2013, clauses 45-48.
794. "Madagascar's 3rd Universal Periodic Review, 34th Session (Oct-Nov 2019), Submission by Southern Africa Litigation Centre", paragraphs 12-17.
795. Law No. 2014-038 relating to protection of personal data (Malagasy Data Protection Law). A summary of the law in English can be found here.
796. "Republic of Madagascar", IMF Country Report No. 23/117, March 2023, paragraph 35.
797. "2023 World Press Freedom Index: Madagascar", Reporters Without Borders.
798. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A. Similarly, BTI states: "In practice, the media are free to publish a variety of opinions, but the government does not hesitate to call them to order if it considers them to have overstepped their role. This means they are often subject to interference or government restrictions, and some journalists consequently practice self-censorship." "Madagascar Country Report 2022", BTI Transformation Index, Bertelsmann Stiftung, 2022.
799. "African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.
800. Loi n°2016-029 du 14 juillet 2016: Code de la Communication Médiatisée, often referred to simply as the "Communications Code". It was amended by Loi n°2020-006: portant modification de certaines dispositions de la Loi n° 2016-029 du 24 août 2016 portant Code de la Communication Médiatisée. The 2020 amendments also changed the date of the original law in its title. Loi n°2020-006, Article 1 on the amendment of the law's title: L'intitulé de la Loi n°2016-029 du 14 juillet 2016 sus visée est modifié comme suit : «**Loi n°2016-029 du 24 août 2016** portant Code de la communication Médiatisée».
801. *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, 12 August 2016; Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant", 31 August 2020.
802. Madagascar's 2010 Constitution, Article 117.
803. Loi n°2016-029, Article 1 (see definitions of "media communications", "audiovisual communications" and "communications") and Article 2.
804. Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant", paragraphs 13-14.
805. Loi n°2016-029, Articles 5-8.
806. Loi n°2016-029, Article 5 new and Article 7 new.
807. In French: "Toutefois, est interdite la publication des débats à huis clos, des rapports ou tout autre document tenus ou établis au sein des Institutions de la République."
808. *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraph 12.
809. Id, paragraph 11.
810. Id, Article 51.
811. Loi n°2020-006, Article 52 new.
812. Id, Article 53 new.
813. Id, Articles 51*bis* new.
814. Loi n°2016-029, Article 49, prior to the 2020 amendments.
815. Loi n°2020-006, Article 51*bis* new.
816. *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraph 15, referring to *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraph 53.
817. Frederic Ange Toure, "In Madagascar, criticizing the president can be expensive", *Le Journal de Afrique*, 31 March 2023; "Liberté de presse: la mise en place de l'ANRCM sollicitée", *Newsmada*, 5 mai 2023.
818. Loi n°2016-029, Article 121, as amended by Loi n°2020-006.

819. Loi n°2016-029, Articles 157-168; "African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 37. The Board is established by a ministerial order.
820. Loi n°2020-006, Article 194 new; Loi n°2016-029, Article 198.
821. Loi n°2020-006, Article 100 new. Identifying information must also appear on every press publication. Loi n°2016-029, Article 102.
822. Loi n°2020-006, Article 174*bis* new; Loi n°2016-029, Article 175 as amended by Loi n°2020-006.
823. Loi n°2020-006, Article 74*bis* new. This article defines "online press" as "any communication service to the public on digital media published on a professional basis by a natural or legal person who has editorial control of its content, consisting of the production and making available to the public of 'original content, of general interest, regularly renewed, composed of information presenting a link with current events and having been the subject of treatment of a journalistic nature, which does not constitute a promotional tool or an accessory of an industrial or commercial activity".
824. Loi n°2016-029, Article 176: "Le fournisseur d'accès internet et tout autre prestataire de service en ligne a le devoir de vérifier le contenu des sites qu'il héberge. Il notifie l'Autorité Nationale de Régulation des Communications Médiatisées de toute activité ou contenu illicite dont il a connaissance. A défaut de notification immédiate, il est sanctionné par une peine d'amende de 1.000.000 à 3.000.000 Ariary. Les clients d'un hébergeur ou les propriétaires de site web doivent lui fournir leur identité réelle et leurs coordonnées exactes."
825. Loi n°2016-029, Article 53; Loi n°2020-006, Articles 54*bis* new, 54b new, 54c new, 55 new.
826. Loi n°2020-006, Article 54 new, read with Loi n°2016-029, Article 1 (definition 30).
827. Loi n°2020-006, Article 56*bis* new.
828. *Décision n°13-HCC/D3 du 31 août 2020 relative à la loi n°2020-006 portant*, paragraphs 18-21.
829. Loi n°2016-029, Article 58.
830. Id, Article 59. The final point on privacy is also discussed in Article 60, which says: "Every journalist claims free access to all sources of information and the right to investigate freely on all the facts which condition public life. The secret of public or private affairs may, in this case, be revealed to the journalist only by way of exception and by virtue of clearly expressed reasons."
831. Id, Article 59.
832. Id, Articles 70-ff.
833. Id, Articles 9-12.
834. Id, Article 69.
835. Id, Explanatory Memorandum on the first page of the law.
836. Id, Articles 15, 18, 26-27 and 33, for example.
837. **"**Madagascar: Controversial Mass Media Code Approved", Library of Congress, 9 September 2016 (references omitted).
838. African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.
839. Loi n°2005-023: portant refonte de la loi n°96-034 du 27 janvier 1997 portant Réforme institutionnelle du secteur des Télécommunications (revising law no. 96-034 of January 27, 1997 on institutional reform of the telecommunications sector). ARTEC replaced the Malagasy Office for the Study and Regulation of Telecommunications (OMERT) as of 1 April 2015. "Madagascar Telecommunications", Logistics Cluster, 2022.
840. Constitution de la Quatrieme Republique: "Article 7.- Les droits individuels et les libertés fondamentales sont garantis par la Constitution et leur exercice est organisé par la loi."
841. *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraph 15.
842. Id, paragraph 14.
843. Id, paragraph16.
844. Id, paragraphs 20-21.
845. Id, paragraph 30.
846. Id, paragraph 60.
847. The Court explicitly confirmed the constitutionality of the first paragraph of Article 6, provided that public order is interpreted narrowly. It also withheld several other articles, subject to some conditions, including the last paragraph of Article 7 (regarding the limitation of right of access to information by means of conditions, terms and procedures defined by a specific text. provided that these are set by law.), the first paragraph of Article 20 (invasion of privacy) and its reiteration in Article 59, Article 30 (false news), Article 44 (the Ministry's power to permanently close a media company or suspend a journalist for repeated violation of the Code,on the condition that this power is exercised constitutionally), Article 51 (on guarantees for the independence of ANRCM), Article 85 (requiring that a publication director must be the owner or majority shareholder or legal representative of the media entity), Article 157 (on the obligations of public service radio and television, subject to the condition of political neutrality and the obligation to provide a diversity of views), the differentiated penalties for different offences under the Code and several provisions restricting the broadcast of advertisements for private non-commercial radio and television advertisements in the public interest.
848. "**Article 6.-** L'information sous toutes ses formes n'est soumise à aucune contrainte préalable, sauf celle portant atteinte à l'ordre public et aux bonnes moeurs.
La liberté d'information, quel qu'en soit le support, est un droit. L'exercice de ce droit comporte des devoirs et des responsabilités et est soumis à certaines formalités, conditions, ou sanctions prévues par les textes législatifs et règlementaires en vigueur, lesquelles constituent des mesures nécessaires dans une société démocratique."

849. *Décision no 30-HCC/D3 du 12 août 2016 relative à la loi no 2016-029 portant Code de la communication médiatisée*, paragraphs 24-28.
850. "Freedom in the World 2023: Madagascar", Freedom House, section D1.
851. "2023 World Press Freedom: Madagascar", Reporters Without Borders, "Safety".
852. Frederic Ange Toure, "In Madagascar, criticizing the president can be expensive", *Le Journal de Afrique*, 31 March 2023.
853. "Freedom in the World 2023: Madagascar", Freedom House, section B1; "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
854. Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
855. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
856. Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
857. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
858. Id.
859. Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
860. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
861. "Madagascar bans public protests ahead of presidential election", *Aljazeera,* 3 April 2023; "Freedom in the World 2023: Madagascar", Freedom House, section B1.
862. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
863. Id.
864. Id.
865. Id.
866. Id. "A court notice published in September [2021] indicated that he was accused of acts that may compromise public security, lead to serious political trouble, or incite hatred of the government or infringement of the laws." This describes Article 91 of the Penal Code.
867. Id.
868. "LEXOTA Country Analysis: Madagascar", last updated July 2022; "Madagascar journalist Arphine Helisoa jailed on false news, incitement allegation", Committee to Protect Journalists, 22 April 2020.
869. African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 12 (footnotes omitted); Loi n°2014-006, as amended by Loi n°2016-031, which contains a new Article 20.
870. "Madagascar: municipal authorities short-circuit overly critical radio station", Reporters Without Borders, 9 August 2016; "Madagascar goes after Jupiter", IFEX, 10 May 2017; "Journalist freed after receiving suspended sentence", Reporters Without Borders, 28 September 2017; "Southern Africa: Media freedom muzzled as journalists are targeted for telling the truth", Amnesty International, 3 May 2019. Note that the Amnesty International source states that Cello spent two years in jail, while Reporters Without Borders and IFEX refer to a suspended sentence of two years.
871. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
872. Lizette Feris, "The State of Media and Information Literacy in Southern Africa", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 65, citing "Facebook 'troll farms' play outsized role in Madagascar's politics", France 24, 5 October 2021. A "troll farm" refers to a body that employs people to make deliberately offensive, provocative or false online posts to cause conflict, discredit certain individuals or institutions or manipulate public opinion.
873. Loi n°2014-006 du 17 juillet 2014: sur la lutte contre la cybercriminalité.
874. Loi n°2016-031 du 14 juillet 2016 et du 15 juillet 2016: modifiant et complétant certaines dispositions de la loi n°2014-006 du 17 juillet 2014 sur la lutte contre la cybercriminalité. The amending law provides a new section 20 and also provides for regulatory texts to be adopted, as necessary, for the application of the law.
875. Loi n°2014-006: Article 1.
876. "Freedom in the World 2023: Madagascar", Freedom House, section D4.
877. *Assessing Cybercrime Laws from a Human Rights Perspective,* Global Partners Digital, [2022], page 14.
878. Loi n°2014-006, Article 10.
879. Code Pénal, Mis à jour au 31 mars 2005 (as amended to 31 March 2005). There have been some subsequent amendments on trafficking in persons that do not affect the provisions discussed in this chapter.
880. Loi n°2016-031, which amended Loi n°2014-006, contains a new Article 20.
881. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A. The original source is not indicated.
882. Loi n°2014-006, Articles 23 and 24 (discussed below).
883. Code Pénal, Mis à jour au 31 mars 2005 (as amended to 31 March 2005), Article 346: It is an offence to fix, record or transmit the image of a minor, with a view to its dissemination, when this image presents a pornographic character. The minimum offence is two years' imprisonment and a fine. The penalties are increased when the child involved is under age 15.
884. Loi n°2014-006, Article 18: The import, distribution, export, production, publication, exhibition and sale of pornographic materials involving children are punishable by the penalties provided for in Article 346 of the Penal Code. Article 146: All production, filming and distribution of cinematographic work of a child pornography nature or incitement to debauchery in any form of violence are prohibited. Any breach of this provision is liable to the penalties provided for in the various laws in force and the confiscation of the materials used in the commission of the offence.
885. See "2021 Country Reports on Human Rights Practices: Madagascar", US State Department, section 6: "The Ministry of Interior ordered the cancellation of an evening event that members of the LGBTQI+ community organized in an

Antananarivo bar for July 3 to celebrate Pride Month. The event had taken place in the same location during previous years. Authorities cancelled the event because they claimed it was an incitement to **debauchery** and **offense to morals**."

886. Loi n°2014-006, Article 146: All production, filming and distribution of cinematographic work of a child pornography nature or incitement to debauchery in any form of violence are prohibited. Any breach of this provision is liable to the penalties provided for in the various laws in force and the confiscation of the materials used in the commission of the offence.
887. Id, as amended by Loi n°2020-006.
888. Loi n°2020-006, Article 20 new.
889. "*Pour l'information du public, le consentement du sujet n'est pas requis*".
890. African Media Barometer: Madagascar 2016", Media Institute of Southern Africa (MISA) and Friedrich Ebert Stiftung (FES), page 6.
891. Loi n°2020-006, Article 30 new.
892. "LEXOTA Country Analysis: Madagascar", last updated July 2022.
893. **"**Madagascar: Controversial Mass Media Code Approved", Library of Congress, 9 September 2016 (references omitted).
894. Loi n°2014-006, Articles 36-46.
895. Id, Article 43.
896. Id, Articles 44-45
897. "2022 Country Reports on Human Rights Practices: Madagascar", US State Department, section 2A.
898. "2023 World Press Freedom Index: Madagascar", Reporters Without Borders, "Legal Framework".
899. "Madagascar: Journalist acquitted but severe civic space restrictions persist", CIVICUS, 13 March 2020.
900. "Madagascar's 3rd Universal Periodic Review, 34th Session (Oct-Nov 2019), Submission by Southern Africa Litigation Centre" March 2019, paragraph 16.
901. "LEXOTA Country Analysis: Madagascar", last updated July 2022.
902. Loi n°2014-006, Articles 25-27 and 31.
903. Id, Article 40.
904. Loi n°2016-029, Articles 11-12.
905. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, pages 36-37, citing the Code of Criminal Procedure, Articles 103, 129-130. The primary source has not been checked. Note that the text of the secondary source refers incorrectly to the Penal Code, but footnotes the Code of Criminal Procedure.
906. Id, pages 36-37, citing Article 9 of Law No. 2016-017, which modified and amended some provisions of the Code of Criminal Procedure (which the secondary source mistakenly refers to as the Penal Code). See the Explanatory Memorandum for Loi n° 2016-17, which states that Article 9 of this amending law concerns additions to the Code of Criminal Procedure to enable the fight against money laundering and other financial offences, incuding a new article 260.1 that extends the jurisdiction and power of the investigating judge to order the placement under surveillance of bank accounts, access to these systems and telephone tapping. The primary source was not checked.
907. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 37.
908. See, for example, "Freedom in the World 2023: Madagascar", Freedom House, section D4; "Freedom in the World 2022: Madagascar", Freedom House, section D4.
909. Law 2005-023, Article 7(1).
910. See, for example, "Africa: SIM Card Registration Only Increases Monitoring and Exclusion", Privacy International, 5 August 2019; "Access to Mobile Services and Proof of Identity 2021: Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19". GMSA, April 2021, page 55.
911. Loi n°2020-006, Article 20 new.
912. Loi n°2020-006, Article 74*bis* new.
913. Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
914. "Madagascar Country Report 2022", Bertelsmann Transformation Index (BTI), Bertelsmann Stiftung, "Political Participation".
915. Id, "Executive Summary".
916. Id, "Political and Social Integration".
917. Madagascar election: campaigns on social media, AfricaNews, 5 November 2018.
918. Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
919. "Freedom in the World 2023: Madagascar", Freedom House, section A3.
920. Loi n° 2018-008, relative au regime general des elections et des referendums (Organic Law no. 2018–008 relating to the general regime of elections and referendums). which repealed Organic Law no. 2012-005 on the Electoral Code.
921. Id, Article 92.
922. Id, Article 95.
923. Id, Article 93.
924. Id, Article 94.
925. Id, Article 96; see also Article 116.
926. Id, Articles 97-99.
927. Id, Articles 100-109.

928. Id, Article 110.
929. Id, Article 111-115.
930. Id, Article 117: "L'utilisation des nouvelles technologies de l'information et de la communication ou de toute autre ressource des réseaux sociaux est admise dans le cadre de la période électorale. Elles demeurent assujetties au respect des principes de pluralité, d'équité et de transparence, sous le contrôle de l'Autorité nationale de régulation de la communication médiatisée."
931. Id, Article 118. This is an offence under Article 228, punishable by a stiff fine.
932. Id, Article 119.
933. Id, Article 218.
934. Id, Article 221.
935. Id, Article 222.
936. Id, Article 224.
937. Id, Article 227.
938. "Freedom in the World 2023: Madagascar", Freedom House, sections B1-B2.
939. "Recueil de Recommandations", CENI/PADEM, 13 October 2021, page 56.
940. "Freedom in the World 2023: Madagascar", Freedom House, section E1.
941. "Madagascar Bans Public Protests Ahead of Presidential Election", ICTJ, 4 April 2023; Laurence Caramel, "A Madagascar, le président Andry Rajoelina confine l'opposition", *Le Monde Afrique*, 6 April 2023.
942. *Mbele v R* (Misc. Criminal Case No. 04 of 2022) 2022 MWHC 74 (20 June 2022) (issue of unconstitutionality referred to Chief Justice for certification as a constitutional matter to be heard by a three-judge panel); "Supreme Court rebuffs State on Army General Nundwe's defamation case against Chisa Mbele", *Nyasa Times*, 18 September 2022.
943. Data Protection Bill, 2021. There are some provisions pertaining to data protection in the Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].
944. Access to Information Act 13 of 2016.
945. Printed Publications Act 18 of 1947 [*Chapter 19:01*].
946. Censorship and Control of Entertainments Act 11 of 1968 [*Chapter 21:01*], sections 19-ff.
947. Id, sections 9-ff.
948. Id. sections 14-ff.
949. Id, section3 (appointment of Board of Censors); on offences, see the sections on each type of permit read with section 32.
950. Communications Act 34 of 2016 [*Chapter 68:01*], section 2; definition of "communications service" in section 3.
951. Id, sections 5 and 8.
952. Id, section 5(3).
953. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 370-371.
954. Communications Act 34 of 2016 [*Chapter 68:01*], Second Schedule.
955. Id, section 43(1)(a).
956. Id, Part XIV.
957. Id, sections 111-112.
958. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 406-ff. The Media Council of Malawi Code of Ethics and Professional Conduct is available here. The MCM's own website could not be accessed in mid-2023 as it was infected with a computer virus.
959. Id, page 347.
960. *Malawi Law Society v The President* (2002) AHRLR 110 (MwHC 2002); see the case summary by Global Freedom of Expression here.
961. *Attorney General v Trapence*, Supreme Court of Appeal, MSCA Civil Appeal No. 55 of 2019, 30 September 2019l see the case summary by Global Freedom of Expression here.
962. *S v MACRA; Ex Parte The Registered Trustees of National Media Institute of Southern Africa & 2 Others* (Constitutional Reference 3 of 2019) [2020] MWHC 193 (29 May 2020), paragraph 26.
963. Id, paragraph 27.
964. Id, paragraphs 33-35.
965. Penal Code [*Chapter 7:01*], section 200. The Penal Code was recently further amended by the Penal Code (Amendment) Act 8 of 2023, which does not affect this section, but (as discussed below) did repeal some other provisions of the Penal Code relevant to expression.
966. *Mbele v R*, Misc. Criminal Case No. 04 of 2022, High Court of Malawi, 20 June 2022.
967. "2023 World Press Freedom: Malawi", Reporters Without Borders, "Safety".
968. "Freedom on the Net 2022: Malawi". Freedom House, "Overview". See also section B4.
969. Antonio Prokscha. "Malawi: Recent detentions of journalists overshadow positive press freedom image", **International Press Institute, 12 April 2021.**
970. "Malawi police detain, charge journalist Dorica Mtenje over story she did not write", Committee to Protect Journalists, 22 February 2023.
971. "Malawi journalist Gregory Gondwe detained, questioned about sources for article on alleged corruption", Committee to Protect Journalists, 8 April 2022.

972. Freedom on the Net 2022: Malawi", Freedom House, section C8; Lameck Messina, "Malawi Police Accused of Hacking Website of Investigative Media Group", *VOA*, 17 April 2022; "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
973. "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 1F; "Malawi 2022", Amnesty International, "Freedom of expression".
974. "Freedom on the Net 2022: Malawi", Freedom House, section C3.
975. "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A. See also Duncan Mlanjira, "Law Professor Accuses Army General of Abusing his Power in Social Media Activist Arrest", *Nyasa Times*, 2022.
976. "Freedom on the Net 2022: Malawi", Freedom House, section C3. See also "Malawi Police arrest social media activist", *Malawi24*, 11 January 2022/
977. "Freedom on the Net 2022: Malawi", Freedom House, section C3.
978. "Malawi police question journalist Watipaso Mzungu over article calling president 'a joker'", Committee to Protect Journalists, 14 April 2021.
979. Id.
980. "LEXOTA Country Analysis: Malawi", last updated December 2022.
981. Id.
982. "Malawi police beat, detain radio reporter Oliver Malibisa", Committee to Protect Journalists, 21 July 2021.
983. "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020].
984. "Malawi detains, charges 3 journalists seeking to cover EU delegation's return", Committee to Protect Journalists, 10 January 2020.
985. "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, page 8 (footnote omitted).
986. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*].
987. Id, section 2
988. Id, sections 5-6.
989. Id, sections 69-70.
990. Id, section 3 (definition of "online public communication").
991. Id, section 24(2).
992. "Freedom on the Net 2022: Malawi", Freedom House, section A3.
993. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 26.
994. *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
995. SADC Model Law on Computer Crime and Cybercrime, section 4.
996. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 17. Note that some of the section numbers referred to by Bande in respect of the Malawi law are incorrect.
997. Id, page 22.
998. Id, page 15 (reference omitted).
999. Id, page 24.
1000. Id, page 19.
1001. Id, page 20.
1002. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 24(2)(b) and (c).
1003. Penal Code [*Chapter 7:01*], section 217A.
1004. "Freedom on the Net 2022: Malawi". Freedom House, section C2.
1005. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 29.
1006. See, for example, "Statement by Michael Kaiyatsa, Acting Executive Director for the Centre for Human Rights and Rehabilitation" [2020] and the case studies in section 10.3 of this chapter.
1007. The wording on this point a somewhat ambiguous: "…makes a threat with the intent to instil reasonable fear in that person for his safety or *to a member of that person's immediate family*". It is not entirely clear if this refers to making *a similar threat to an immediate member of the family*, or making *a threat to a person that instils fear in that person for the safety of immediate family members*.
1008. Teresa Temweka Chirwa-Ndanga, "New Access to Information Law Brings Hope" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), page 39.
1009. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 93.
1010. Id, sections 52 and 67 (quoted on the box in the text).
1011. "Freedom on the Net 2022: Malawi". Freedom House, section C4.
1012. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 31(1).
1013. Id, section 95.
1014. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, page 376.

1015. "Freedom on the Net 2022: Malawi". Freedom House, section C4.
1016. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 70.
1017. Id, section 83.
1018. Electronic Transactions and Cyber Security Act 33 of 2016 [*Chapter 74:02*], section 30 read with sections 27-28. These requirements technically apply to the "intermediary service provider". which is the person or entity "that provides electronic communications services consisting of the provision of access to communications networks, storage, hosting or transmission of information through communication networks" (definition in section 2).
1019. The Penal Code (Amendment) Act 8 of 2023 repealed sections 50-53 of the Penal Code [*Chapter 7:01*]. Note that sections 46-49 of the Penal Code, which previously prohibited the importation or re-publication of publications which the minister believed to be contrary to the public interest, were repealed by Act 24 of 2012. Penal Code [*Chapter 7:01*].
1020. Penal Code [*Chapter 7:01*], section 60.
1021. "LEXOTA Country Analysis: Malawi", last updated December 2022.
1022. See section 10.3 of this chapter.
1023. "2022 Country Reports on Human Rights Practices: Malawi", US State Department, section 2A.
1024. See section 10.2 of this chapter.
1025. Preservation of Public Security Act 11 of 1960 section 3(2)(a).
1026. The Public Security Regulations (reproduced below the text of the act on this website), regulation 4 read with regulation 14.
1027. "LEXOTA Country Analysis: Malawi", last updated December 2022.
1028. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 8: Malawi", Konrad Adenauer Stiftung, 2021, pages 284-285.
1029. Protected Flag, Emblems and Names Act [*Chapter 18:03*], section 4.
1030. Prisons Act [Chapter 9:02], section 83(3)-(4).
1031. Communications Act 34 of 2016 [*Chapter 68:01*], section 92.
1032. Communications (SIM Card Registration) Regulations, 2023, regulation 5.There are additional details for other categories of registrations, including minors, foreigners, refugees and diplomatic institutions.
1033. Freedom on the Net 2022: Malawi". Freedom House, section C4.
1034. Personal communications, July 2023.
1035. Id, section C5 (references omitted).
1036. *Kimu v Access Malawi Limited and Others* (Commercial Case No. 54 of 2011) [2012] MWComm C1 (02 May 2012).This judgment could not be located online.
1037. Case description and quotes as reported in Jimmy Kainja, "Mapping Digital Surveillance and Privacy Concerns in Malawi", Media Policy and Democracy Project, November 2021, pages 9-10; "Navigating Litigation During Internet Shutdowns In Southern Africa", Southern Africa Litigation Centre, June 2019, pages 47-49.
1038. The placement of the last clause of Article 12(2) is crucial to the Article's meaning. The 1968 Constitution published by constitute.org (which is hyperlinked here because it is updated to 2016) joins this clause to paragraph c, as does the 1968 Constitution published by the Mauritius Director of Public Prosecutions. This placement is supported by Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 9: Mauritius", Konrad Adenauer Stiftung, 2021, page 9. However, the 1968 Constitution published by the Attorney-General of Mauritius places this clause *below* paragraph c, *which makes it applicable to paragraphs a-c and not just to paragraph c*. This placement of the clause is supported by Geoffrey Robertson QC, "Media Law and Ethics in Mauritius: Preliminary Report", 2013, paragraph 24. It is also the version found in Amos Jenkins Peaslee and Dorothy Peaslee Xydis, *Constitutions of Nations: Volume I, Africa*, Brill, 1974, page 525. It is also how the provision is quoted in the 1999 Privy Council case of *Gilbert Ahnee v The Director of Public Prosecutions*.
The original publication is in the Schedule to the "Mauritius Independence Order 1968" published in Mauritius Government Notice No. 54 of 1968, which could not be located online.
The latter placement seems to be correct, based on the balance of sources, as well as being the version that ties in best grammatically with the reference to "provision" in the opening clause of Article 12(2). This placement of the closing clause is the one reproduced here.
1039. Data Protection Act 20 of 2017. This Act came into force in 15 January 2018, replacing the Data Protection Act 2004. "Mauritius: Cybercrime policies/strategies", Octopus Cybercrime Community, Council of Europe, undated.
1040. See Chelvin Ramsamy, "A Long-Awaited Freedom of Information Act for Mauritius. But When?", blog post on Friedrich Ebert Stiftung website, 6 January 2023.
1041. "2023 World Press Freedom Index: Mauritius", "Media landscape" and "Political Context".
1042. Newspapers and Periodicals Act [*Cap 37*].
1043. Criminal Code amended to 2006, section 289. The amendments made to the Criminal Code after the date of this consolidated copy do not affect this section.
1044. Independent Broadcasting Authority Act 29 of 2000. This version of the Act includes amendments made through December 2021.
1045. Id, section 6.
1046. Id, section 11.
1047. Id, section 3.
1048. Id, section 19(3)(c)-(e).
1049. Id, section 19(3)(g).
1050. Id, section 19(3B).

1051. Id, section 22.
1052. Ambareen Beebeejaun, "Media Regulation in Mauritius: A Critical Analysis" in David Crowther and Shahla Seifi, *Preparing for a Sustainable Future*, Springer, 2023, page 55 (reference omitted); Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.
1053. Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.
1054. Independent Broadcasting Authority Act 29 of 2000, section 38.
1055. Id, section 6(6).
1056. Ambareen Beebeejaun, "Media Regulation in Mauritius: A Critical Analysis" in David Crowther and Shahla Seifi, *Preparing for a Sustainable Future*, Springer, 2023, page 54.
1057. Independent Broadcasting Authority Act 29 of 2000, sections 24-25.
1058. Id, sections 29-30L.
1059. "Mauritian parliament imposes tougher regulations on broadcast media", Reporters Without Borders, 1 December 2021.
1060. Independent Broadcasting Authority Act 29 of 2000, section 18A.
1061. "Mauritian parliament imposes tougher regulations on broadcast media", Reporters Without Borders, 1 December 2021.
1062. Christina Chan-Meetoo, Senior Lecturer in Media and Communication, University of Mauritius, "Assessing the Independent Broadcasting Authority (IBA) Amendment Bill 2021", 1 December 2021.
1063. Information and Communication Technologies Act 44 of 2001 (as amended to December 2021). The most recent amendments to the Act are contained in section 5 of The Judicial and Legal Provisions (No. 2) Act 14 of 2018 and section 39 of The Finance (Miscellaneous Provisions) Act 15 of 2021. For purposes of comparison, the Act as it stood prior to these two amending laws can be found here and here.
1064. Information and Communication Technologies Act 44 of 2001, section 16.
1065. Id, section 18(d), (f), (j), (m), (o), (u), and (aa).
1066. Information and Communication Technologies Act 44 of 2001, section 5.
1067. Id, section 14.
1068. Id, sections 36 and 39.
1069. Id, sections 12-13.
1070. Id, sections 34-35.
1071. "Note on Mauritius' Information and Communication Technologies Act 2001", Centre for Law and Democracy, May 2021, pages 3-4 (hereinafter "Centre for Law and Democracy Note on the ICT Act", May 2021).
1072. Information and Communication Technologies Act 44 of 2001, section 20(1).
1073. "Centre for Law and Democracy Note on the ICT Act", May 2021, page 7.
1074. Information and Communication Technologies Act 44 of 2001, section 24(5)(a)-(b).
1075. "Centre for Law and Democracy Note on the ICT Act", May 2021, page 8.
1076. Id, section 46.
1077. Id, section 25.
1078. ICTA website, "Internet: Overview", 2023.
1079. Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
1080. ICTA website, "CSA filtering", 2023.
1081. As quoted in Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
1082. This is covered by all the versions of section 46(ga) – as it stood before the 2018 amendments, after the 2018 amendments and after the 2021 amendments.
1083. The Act as it stood prior to the 2018 and 2021 amendments can be found here and here. See section 46(ga) and (h)(ii).
1084. See the amendments made by The Judicial and Legal Provisions (No. 2) Act 14 of 2018, section 5.
1085. Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021.
1086. The judges said in the *Seegum* case that "we are not hereby making any pronouncement as to the constitutionality of the new redrafted section 46 (h)(ii), as amended by Act No 14 of 2018", as quoted in ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021.Note that section 46(ga) was not at issue in the *Seegum* case.
1087. *Seegum J v The State of Mauritius* 2021 SCJ 162, as summarised here by Denton's, the law firm that represented the appellant, on 1 June 2021; Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021; Jillian C York, "Amendments to Mauritius' ICT Act Pose Risks for Freedom of Expression", Electronic Frontier foundation, 6 December 2018.
1088. Information and Communication Technologies Act 44 of 2001, section 46(1)(ga).
1089. Id, section 46(2)-(3).
1090. "Comments on Proposed Amendments to the Mauritian Information and Communications Technologies Act", Centre for Law and Democracy, May 2021; "Mauritius: Proposals to Monitor and Control All Social Media Traffic Very Repressive" Centre for Law and Democracy, 12 May 2021; Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023.
1091. Iqbal Ahmed Khan, "ICT Act: Why the law is still in limbo...", *lexpress.mu*, 22 March 2023; "ICTA Clause Unconstitutional – An Excellent Judgment", *lalit,* 1 June 2021.
1092. Mauritius Broadcasting Corporation Act 22 of 1982, section 6.
1093. Id, section 4(d), (f) and (g).

1094. Id, section 19.
1095. The right of reply in respect of newspapers in the Criminal Code, section 289 (discussed above), has considerably more teeth.
1096. Media Trust Act 9 of 1994, sections 2-4.
1097. Mauritius Digital Promotion Agency Act 4 of 2023, sections 3-4 and 20.
1098. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 9: Mauritius", Konrad Adenauer Stiftung, 2021, page 64.
1099. *Duval v The Commissioner of Police* 1974 MR 130.
1100. Geoffrey Robertson QC, "Media Law and Ethics in Mauritius: Preliminary Report", 2013, paragraph 24. No final version of the report was ever published. Christina Chan-Meetoo, "On the subject of Media Regulation in Mauritius", 24 November 2021.
1101. *DPP v Boodhoo* (1992) MR 284, as quoted in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 3.
1102. *Gilbert Ahnee & Ors v The Director of Public Prosecutions (Privy Council)* (1999) MR 208 (Judgment of the Lords of the Judicial Committee of the Privy Council, 17 March 1999.
1103. Id, discussion in the judgment of issue 2(a).
1104. Id.
1105. *Soornack Nandanee v Le Mauricien Ltd & Ors* 2013 SCJ 58. The *Ahnee* and *Soornack* cases were identified by the government as being particularly significant cases on Article 12 of the Constitution in the media context. "General Assembly Resolution 72/175 on 'The safety of journalists and the issue of impunity': Inputs of the Government of Mauritius", undated. paragraph 4
1106. *Seegum J v The State of Mauritius* 2021 SCJ 162, pages 17-18.
1107. "2023 World Press Freedom Index: Mauritius", "Safety".
1108. "Freedom in the World 2022: Mauritius", Freedom House, section D1.
1109. "2022 Country Reports on Human Rights Practices: Mauritius", US State Department, section 2A.
1110. Id, section 1D.
1111. Id.
1112. Id, section 2A.
1113. Id.
1114. "LEXOTA Country Analysis: Mauritius", last updated July 2022.
1115. Cybersecurity and Cybercrime Act 16 of 2021.
1116. The Computer Misuse and Cybercrime Act 22 of 2003 (now repealed) can be found here and here.
1117. Mohammud Nabeel Khodabux, "Mauritius: Compliance Automation: A New Dawn In The Financial Services Sector", *mondaq* 29 March 2022.
1118. "2022 Country Reports on Human Rights Practices: Mauritius", US State Department, section 2A.
1119. Cybersecurity and Cybercrime Act 16 of 2021, sections 3-4.
1120. Id, sections 38-39.
1121. *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime (UNODC), draft dated February 2013. page 82.
1122. SADC Model Law on Computer Crime and Cybercrime, section 4.
1123. Child Protection Act 30 of 1994, sections 15 read with the definitions of "child", "film", "indecent photograph", "photograph" and "pseudo-photograph" in section 2. What constitutes indecency is not defined, however, nor is there any exception for artistic, educational or scientific materials.
1124. There is an extensive definition of "act of terrorism" in section 3(2) of the Prevention of Terrorism Act 2 of 2002.
1125. Cybersecurity and Cybercrime Act 16 of 2021, section 33.
1126. Id, section 26.
1127. Id, section 27.
1128. Id, section 28. A local newspaper provided a helpful description of the difference between "traffic data" and "stored data" for the layperson, describing "*traffic data*" as "the history of your everyday websites and online platforms that you visit, including your mobile internet traffic, phone calls, SMS, etc" and "*stored data*" as "your email content if your email is hosted by the service provider". Ish Sooken, "My thoughts on the Cybersecurity and Cybercrime Bill", *lexpress*, 2 November 2021.
1129. Id, sections 29-30.
1130. Id, section 31.
1131. Id, section 23.
1132. Satyajit Boolell, SC, "Director Of Public Prosecutions, Mr. Satyajit Boolell, Explains Role Of An Administrator Of A Whatsapp Group", *Le Matinal,* 21 March 2022.
1133. Information and Communication Technologies Authority Act 44 of 2001, section 2.
1134. Id, section 46(1).
1135. "Centre for Law and Democracy Note on the ICT Act", May 2021, page 12.
1136. Id.
1137. "LEXOTA Country Analysis: Mauritius", last updated July 2022.
1138. "Centre for Law and Democracy Note on the ICT Act", May 2021, page 11.
1139. "LEXOTA Country Analysis: Mauritius", last updated July 2022.
1140. Information and Communication Technologies Act 44 of 2001, section 47.

1141. "Centre for Law and Democracy Note on the ICT Act", May 2021, page 13.
1142. Information and Communication Technologies Act 44 of 2001, section 47.
1143. Id, section 32(5). This power is buried in a section entitled "Confidentiality".
1144. "Centre for Law and Democracy Note on the ICT Act", May 2021 pages 10-11.
1145. Information and Communication Technologies Act 44 of 2001, section 32(6)(a).
1146. Criminal Code amended to 2006. Note that it has been further amended by the Criminal Code (Amendment) Act 11 of 2012 (section 285 and 285A on abortion), the COVID (Miscellaneous Provisions) Act 1 of 2020 (details of sections 4, 5, 6, 378, 382, and 385) and the Criminal Code (Amendment) Act 17 of 2021 (which adds a new section 76B: Misrepresenting the sovereignty of Mauritius over any part of its territory). See also the See also Criminal Code (Supplementary), which covers, amongst other things, dealing in obscene matter, exhibiting slides and video tapes in public, and bomb and fire hoaxes.
1147. Criminal Code amended to 2006, section 288.
1148. *DPP v Masson* (1972) M.R. 204, as discussed in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 10.
1149. "LEXOTA Country Analysis: Mauritius", last updated July 2022.
1150. *R v Boodhoo* [1990] MR 191, as discussed in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 11.
1151. *Seneque & anor v DPP* [2002] UKPC 42 (PC), as quoted in "Délits de Presse" published by the Office of the Director of Public Prosecutions (DPP), undated, paragraph 12.
1152. National Assembly (Privileges, Immunities and Powers) Act 22 of 1953, section 6(1)(g), (n), (o) and (s), read with section 6(2).
1153. Information and Communication Technologies (Registration of SIM) Regulations 2021 (not located online).
1154. Information and Communication Technologies (Registration of SIM) (Amendment) Regulations 2023. The amendments concern the dates of coming into force.
1155. ICTA Communique on Amendments to the Information and Communication Technologies (Registration of SIM) Regulations 2021, 18 January 2023.
1156. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 38 (referring to a previous section number).
1157. Section 18(u), as discussed in id, page 38 (referring to a previous paragraph number).
1158. Cybersecurity and Cybercrime Act 16 of 2021, section 23.
1159. Mauritius's 1968 Constitution, revised 2016, Articles 28(2) and 59(1).
1160. "The World Bank in Mauritius: Overview", The World Bank, 23 March 2023, "Political Context".
1161. "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
1162. Jean Paul Arouff**.** "Mauritius elects incumbent PM for five-year term," *Reuters*, 8 November 2019.
1163. "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
1164. Id, "Executive Summary".
1165. Mauritius's 1968 Constitution, revised 2016. Articles 38-41. The relevant sections are quoted in the box. The omitted portions relate to the Electoral Boundaries Commission, which makes recommendations on the borders of constituencies.
1166. All of these laws and regulations can be downloaded from the website of the Office of the Electoral Commissioner, "Legislation".
1167. Representation of the People Act 14 of 1958, section 70.
1168. National Assembly Elections Regulations 2014, section 28.
1169. Code of Conduct for the National Assembly Elections 2019, point 3.
1170. "Mauritius Country Report 2022", BTI (Bertelsmann Transformation Index), "Political Participation".
1171. Mauritius Broadcasting Corporation Act 22 of 1982, section 19.
1172. Lei n.º 1/18 de 12 de Junho: Lei da Revisão Pontual da Constituição da República de Moçambique. The 2018 amendments are briefly summarised in English here ("Structure of the Constitution").
1173. See the following:
    - The Civil Code (Decree-Law no. 47344, of 25 November 1966, in force in Mozambique through Edict no. 22869, dated 4 September 1967);
    - The Penal Code (Law no. 24/19, of 24 December, as amended by Law no. 17/20 of 23 December);
    - The Labour Law (Law no. 23/07, of 1 August); and
    - The Electronic Transactions Law (Law no. 3/17, of 9 January).

    Article 71 of the Constitution identifies the need to legislate on access, generation, protection and use of computerized personal data (either by public or private entities); however, implementing legislation has not yet been approved. "Data Protection Laws of the World: Mozambique", DLA Piper, 10 December 2022.
1174. Law no. 34/14 of 31 December (in English).
1175. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 10: Mozambique", Konrad Adenauer Stiftung, 2021, page 84 (hereinafter "Limpitlaw"). See also Leandro Gastão Paul, "CSCS: Conselho Superior de Comunicação Social - Um Órgão Inútil" (which translates as "A Useless Organ"), 2022; "Press Freedom: Mozambique", International Press Institute, December 2022, page 9.
1176. Lei nº 18/91 de 10 de Agosto: Lei de Imprensa, Article 37. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 10: Mozambique", Konrad Adenauer Stiftung, 2021, page 92.
1177. Limpitlaw, pages 93, 95-96, 129.

1178. Id, pages 120, 129-130.
1179. Lei nº 18/91, Article 19(1); Limpitlaw, page 96. As noted above, references in the Press Law to the Minister of Information are to be understood as references to Gabinfo.
1180. Id, Article 22; Limpitlaw page 97.
1181. Id, Article 24. Limpitlaw, page 97.
1182. Id, Articles 15(1) and 50. Limpitlaw, page 98.
1183. Limpitlaw, pages 101-103.
1184. Lei nº 18/91 de 10 de Agosto, Article 13; Limpitlaw, page 103.
1185. Id, Article 27; Limpitlaw, page 94.
1186. Id, Article 28; Limpitlaw, page 94-95.
1187. Id, Article 32; Limpitlaw, page 95.
1188. Id, Articles 33-34; Limpitlaw, page 100.
1189. Id, Articles 41-42, 49, 53-54; Limpitlaw, page 110.
1190. Id, Articles 43-ff.
1191. Limpitlaw, pages 121-123.
1192. Id, page 124. (Decree No 18/1994 governs Radio Mozambique, and Decree No 31/2000 governs Mozambique TV.)
1193. Id, page 89, with details at pages 124-ff.
1194. Lei n.º 8/04 de 21 de Julho: Aprova a lei das Telecomunições. This law was amended by Lei n.º 4/16. For a brief overview of this law in English, see Vanessa Manuela Chiponde, "Brief Remarks on the Licensing of Telecommunications Services under the New Telecommunications Legislation", *SAL & Caldeira Newsletter*, N.º 32, 2017, page 2; "Mozambique Regulatory Authority Name Changed to ARECOM", Approve-IT, 6 August 2019; "Mozambique Type Approval Authority Changes to INCM", Approve-IT, 29 May 2020.
1195. Law n.º 3/17 de 9 de Janeiro establishes INTIC as the regulatory entity of the ICT sector. **Decree no. 60/2017** of November 6 redefines INTIC's authority to regulate and supervise the ICT sector. **Decree no. 82/2020** of September 10, establishes INTIC as a Regulatory Public Institute of ICT, coordinator of digital governance and Internet governance. **Decree No. 90/2020** of October 9 revokes Decree No. 60/2017 and establishes INTIC as a Public Institute regulating ICT and coordinating digital and Internet governance. Prof. Doutor Eng. Lourino Chemane, "Política para a Sociedade de Informação de Moçambique e Lei das Transacções Electrónicas: Grau de Implementação, Desafios e Perspectivas", INTIC. 29 Julho de 2021, Powerpoint: " 2. Contexto de Governação de TIC no País".
1196. "Mozambique: Urgent action needed to safeguard press freedom and democracy", International Press Institute, 21 August 2022
1197. Lei da Comunicação Social (draft law in Portuguese).
1198. Lei da Radiodifusão (draft law in Portuguese).
1199. "Press Freedom: Mozambique", International Press Institute, December 2022, page 9; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.
1200. Armando Nhantumbo was interviewed via Zoom on 20 July 2023.
1201. "Press Freedom: Mozambique", International Press Institute, December 2022, page 9; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.
1202. "Preliminary Analysis of Mozambique's 2022 Draft Law on Non-Profit Organizations", American Bar Association Center for Human Rights, November 2022 contains a detailed analysis.
1203. "Mozambique: Lawmakers should reject restrictive NGO law", International Press Institute, 27 February 2023.
1204. Limpitlaw, page 74.
1205. This discussion draws in part on Limpitlaw, pages 72-74, 88. Limpitlaw says at page 74 that Article 48 includes an explicit reference to "training of journalists", but no reference to such training could be located.
1206. Mozambique's 2004 Constitution (revised 2007) (in English), Article 43.
1207. The six petitioners were the Media Institute of Southern Africa (MISA) Mozambique Chapter, the Association of Journalistic Companies, the National Forum of Community Radios, the Centre for Public Integrity, the Mozambican Bar Association and the Emergency Committee for the Protection of Fundamental Freedoms.
1208. Mozambique's 2004 Constitution (revised 2007) (in English), Articles 240-248. Note that Article 244 was amended in 2018 by Lei n.º 1/18.
1209. "Digital Rights in Mozambique", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraphs 6-7; "Mozambique: New Media Fees Assault Press Freedom", Human Rights Watch, 17 August 2018; "Mozambique: Government revokes decree on media fees", Club of Mozambique, 21 May 2020.
1210. *Public Ministry v Castel-Branco and Mbanze* (in Portuguese), 15 September 2015. The discussion of the case in the text relies entirely on the case summary by Global Freedom of Expression here.
1211. Limpitlaw, page 78.
1212. "Mozambique: Urgent action needed to safeguard press freedom and democracy", International Press Institute, 21 August 2022.
1213. "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1A, 1C and 2A.
1214. "Press Freedom: Mozambique", International Press Institute, December 2022, page 8.
1215. Id, page 14; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), pages 41-43.

1216. "Mozambican journalist Arlindo Chissale faces lesser charge after terrorism accusation", Committee to Protect Journalists, 15 November 2022; "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, section 2A.
1217. "Press Freedom: Mozambique", International Press Institute, December 2022, page 11; "Mozambique expels British journalist Tom Bowker, bans him for 10 years", Committee to Protect Journalists, 16 February 2021.
1218. "Radio journalist Ibraimo Abú Mbaruco missing in Mozambique", Committee to Protect Journalists, 17 April 2020; "Mozambique: Journalist Feared 'Disappeared'", Human Rights Watch, 17 April 2020; "Media, Rights Watchdogs Worry Over Missing Mozambique Journalist", AFP - Agence France Presse. 17 April 2020; "Cabo Delgado: Two years on, Ibraimo Mbaruco's disappearance remains unanswered – DW", *Deutsche Welle*, 8 April 2022; Nompilo Simanje, "The right to truth: IPI demands justice for killed journalists in Africa", International Press Institute, 30 March 2023.
1219. "Mozambique: IPI calls on authorities to drop criminal defamation and slander case against journalist Leonardo Gimo". International Press Institute, 30 June 2023; "Mozambican journalist Leonardo Gimo investigated for criminal defamation over report on alleged police corruption", Committee to Protect Journalists, 27 June 2023; Olalekan Adigun, "Calls to Drop Criminal Defamation Case against Journalist Leonardo Gimo in Mozambique", 30 June 2023.
1220. Olalekan Adigun, "Calls to Drop Criminal Defamation Case against Journalist Leonardo Gimo in Mozambique", 30 June 2023.
1221. "Mozambique: Arbitrary arrests, teargassing and brutal assault of peaceful protesters a violation of the right freedom of assembly", Amnesty International, 18 March 2023.
1222. "Mozambique border police detain, beat radio journalist Rosário Cardoso", Committee to Protect Journalists, 15 February 2023.
1223. "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
1224. "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1A, 1C, 2A and 2B. See also "Two journalists in Mozambique attacked by police while covering officer's funeral", Committee to Protect Journalists, 15 August 2022.
1225. See "Mozambique Archive", Committee to Protect Journalists.
1226. Lei n.º 24/19 de 24 de Dezembro: Lei da Rivisão do Código Penal, which replaces the 2014 Penal Code, as amended by Lei n.º17/20 de 23 de Dezembro (which adds a provision on trafficking in persons).
1227. Lei n.º 3/17 de 9 de Janeiro: Lei das Transacções Electrónicas (Law on Electronic Transactions).
1228. Lei nº 18/91.
1229. Lei n.º 24/19 de 24 de Dezembro.
1230. Lei n.º 14/13 de 12 de Agosto: Lei de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo (Law to Prevent and Combat Money Laundering and Terrorism Financing), as amended by Lei n.º 11/22 de 7 de Julho; "Mozambique: State of cybercrime legislation", Octopus Cybercrime Community, Council of Europe, undated.
1231. Lei n.º 24/19 de 24 de Dezembro; summary based on "Mozambique: Substantive Law", Octopus Cybercrime Community, Council of Europe, undated.
1232. Lei n.º 3/17, sections 67-68; see also "Mozambique: Substantive Law", Octopus Cybercrime Community, Council of Europe, undated.
1233. Proposed Law on Cybersecurity (in Portuguese). This is "Version 3.0" of the draft, dated 30 March 2023. Note that it is dated *after* the version marked "Version 4" on the INTIC website and identified by INTIC as being the most up-to-date version. See "Proposta de Lei de Segurança Cibernética", the page of the INTIC website which has links to download the different versions of the bill. The initial bill has already been revised from previous versions to take account of public and stakeholder input, but as of July 2023, the process of consultation on the proposed bill was still underway.
1234. "Mozambique: New cybersecurity law proposed", alt.advisory, 29 November 2022 (note that the link in this article references the initial version of the bill which has since been revised); "Mozambique examines proposed cybersecurity law", *360 Mozambique*, 12 July 2023.
1235. Proposed Law on Cybersecurity, Version 3.0 (in Portuguese), Articles 26-31.
1236. Id, Article 7-ff.
1237. Lei nº 18/91.
1238. Lei n.º 24/19 de 24 de Dezembro.
1239. Id, Article 2(2).
1240. Lei nº 18/91, Article 51(1); Limpitlaw, pages 111-112.
1241. Limpitlaw, pages 112-113.
1242. Id, , pages 110-112.
1243. Lei n.º 24/19, Article 386, Limpitlaw, page 113; "LEXOTA Country Analysis: Mozambique ", last updated December 2022.
1244. Lei nº 18/91, Article 48; Limpitlaw, page 113; "LEXOTA Country Analysis: Mozambique ", last updated December 2022.
1245. Lei n.º 24/19, Article 345; Lei nº 18/91, Article 51(1); Limpitlaw, page 114
1246. Id, Article 190(2)-(3).
1247. Id, Article 345; Limpitlaw, page 114.
1248. Id, Article 211-ff; Limpitlaw, page 114; "Disrupting Harm in Mozambique – Evidence on online child sexual exploitation and abuse", ECPAT, INTERPOL, and UNICEF, 2022, page 20.
1249. Id, Article 252; Digital Rights in Mozambique ", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraph 25.

1250. Lei nº 13/22 de 8 de Julho: Lei que Estabelece o Regime Jurídico de Prevenção, Repressão e Combate ao Terrorismo e Proliferação de Armas de Destruição em Massa. This law repealed the previous terrorism law, Lei n.º 5/2018, de 2 de Agosto.
Law on the Prevention, Suppression and Countering of Terrorism and Proliferation of Weapons of Mass Destruction (8 July 2022).
1251. "Proposed amendment to Mozambique's anti-terror law threatens press freedom", Committee to Protect Journalists, 7 June 2022; "Press Freedom: Mozambique", International Press Institute, December 2022, page 13; 2022 Country Reports on Human Rights Practices: Mozambique", US State Department, section 2A; Dércio Tsandzana, "Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023; "LEXOTA Country Analysis: Mozambique ", last updated December 2022. Note that some secondary sources refer to the 2022 law as constituting amendments to the 2018 law on terrorism. The law as finally enacted *repealed* the 2018 law ("revoga a Lei n.º 5/2018, de 2 de Agost").
1252. Mozambique's 2004 Constitution (revised 2007) (in English), Articles 41, 65(3) and 68.
1253. For example, Article 10 of Decree no. 44/2019 on "Telecommunications Service Consumer Protection" provides for the consumer's right to privacy and protects against the unauthorised use personal information from their communications. Article 7 of Decree no. 66/2019 on "regulation of the security of telecommunications networks" also highlights privacy. Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
1254. "2022 Country Reports on Human Rights Practices: Mozambique", US State Department, sections 1F and 2A.
1255. Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
1256. Id, page 6.
1257. Law nº 25/19 de 26 de Dezembro: Lei de revisão do Código de Processo Penal. Article 222; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
1258. Lei n.º 2/17 de 9 de Janeiro: Cria o Serviço Nacional de Investigação Criminal, abreviadamente designado por SERNIC (Creating the National Criminal Investigation Service, abbreviated as SERNIC), Article 21; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
1259. Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 5.
1260. "Assessment of Media Development in Mozambique" MISA Mozambique for the UNESCO Communication and Information Sector, UNESCO 2011; Ernesto Nhanale, "Armed Conflicts Worsen Plight of Journalists", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa (MISA), page 6. Law no. 19/91 could not be located online.
1261. Lei nº 13/22 de 8 de Julho, Article 8; **Dércio Tsandzana, "**Freedom of expression and combating terrorism in Mozambique: the challenge of enacting laws in a context of conflict", AfricLaw, 6 February 2023.
1262. Law n.º 3/17 de 9 de Janeiro, Article 19: User identification record.
1263. Decree no. 13/23 of 11 April, which approves the Regulation on the Registration of Telecommunications Services (not located online); James Barton, "Mozambique implements biometric SIM registration in major overhaul", 25 April 2023; "Biometric registration of SIM cards and other changes on their way: Mozambique", Carta de Moçambique, 21 April 2023.
1264. "Digital Rights in Mozambique ", Submission to the 38th session of the Universal Periodic Review: Mozambique, CIPESA, undated [2021], paragraph 24.
1265. Law n.º 3/17, Article 18(1) and (2)(d) ("identificar os utilizadores que transmitem ou armazenem dados com conteúdo ofensivo, usando o serviço de comunicação com remetente não identificado").
1266. "Freedom in the World 2023: Mozambique", Freedom House, sections A1-A2.
1267. "Mozambique Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
1268. The website for these two bodies can be found here.
1269. Lei n.º 1/18 de 12 de Junho: Lei da Revisão Pontual da Constituição da República de Moçambique. The current composition of the CNE is summarised here.
1270. "Freedom in the World 2023: Mozambique", Freedom House, section A3.
1271. Lei n.º 8/13 de 22 de Fevereiro, Article 22.
1272. Id, Article 31.
1273. Id, Article 12.
1274. Id, Articles 207 and 209.
1275. Id, Article 23.
1276. Id, article 36.
1277. Id, Article 24.
1278. Lei n.º 18/91, Article 12.
1279. Cláudia Aranda, "Handbook on Journalistic Ethics in Media Coverage of Electoral Processes", UNDP, June 2011, pages 85-86; "African Media Barometer; Mozambique 2018", Media Institute of Southern Africa (MISA) and Friedrich-Ebert Stiftung (FES), page 8.
1280. Namibia Draft Data Protection Bill, accessed 21 June 2023.
1281. Access to Information Act 8 of 2022.

1282. Newspaper and Imprint Registration Act 63 of 1971, section 2. Prior to Namibian independence, in 1985, *The Namibian* newspaper was asked to provide a hefty deposit as a decision of registration pursuant to a Cabinet decision. This requirement was invalidated by the High Court of South West Africa (Namibia) in the case *The Free Press of Namibia (Pty) Ltd. v. Cabinet of the Interim Government of South West Africa* 1987 (1) SA 614 (SWA).
1283. Newspaper and Imprint Registration Act 63 of 1971, section 1.
1284. Information from MISA Namibia, 23 June 2023.
1285. Namibia Film Commission Act 6 of 2000, sections 20-21.
1286. Communications Act 8 of 2009, sections 4-5 read with definition of "communications" in section 1.
1287. Id, sections 8-9. "The process of appointing CRAN board members is ostensibly transparent, with the Ministry of Public Enterprises advertising calls for applications for all appointments on various boards. These applicants are interviewed by a panel drawn from the government and civil society. A recommended shortlist is drawn up from which the Ministry of ICT makes the final decision.[…] However, members of the CRAN board of directors are generally seen as political appointees. While none of them hold positions in the ruling party, SWAPO, they are known to be aligned with the party's governing faction." *African Media Barometer Namibia 2022*, Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), pages 46-47.
1288. Communications Act 8 of 2009, section 7.
1289. Id, Chapter IX.
1290. Id, section 2(b).
1291. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, pages 162-163.
1292. New Era Publication Corporation Act 1 of 1992, section 3.
1293. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, page 152.
1294. Namibia Press Agency Act 3 of 1992, section 3.
1295. Id, section 6.
1296. Id, section 12; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, page 164.
1297. Namibian Broadcasting Act 9 of 1991, section 3.
1298. Id, sections5-6.
1299. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 11: Namibia", Konrad Adenauer Stiftung, 2021, pages 165-166.
1300. The Code of Ethics and Conduct for Namibian Print, Broadcast and Online Media defines "online media" as "media which is published over the Internet, and includes, without limitation, web-sites, blogs, and social media". Section 1(f).
1301. Article 21(1)(a) of the Namibian Constitution, quoted above on the first page of this chapter.
1302. Article 21(2) of the Namibian Constitution, quoted above on the first page of this chapter.
1303. *Director General of the Namibian Central Intelligence Service v Haufiku & Others* 2019 (2) NR 556 (SC), summarised and analysed by Global Freedom of Expression here.
1304. The Government relied on the Protection of Information Act 84 of 1982 read with the Namibian Central Intelligence Service Act 10 of 1997. Section 4(1)(b) of the Protection of Information Act 84 of 1982 makes it a criminal offence to disclose any information obtained by means of a violation of the Act, or information relating to "a prohibited place, anything in a prohibited place, armaments, the defence of the Republic, a military matter, a security matter or the prevention or combating of terrorism", amongst other things. The Government argued that the information in question fell into the category of "security matter" because it related to the national security functions of the Namibia Central Intelligence Service as set out in section 5(1)(a) the Namibian Central Intelligence Service Act 10 of 1997.
1305. *Director General of the Namibian Central Intelligence Service v Haufiku & Others*, paragraph 74.
1306. Id, paragraphs 106-108.
1307. "2023 World Press Freedom Index: Namibia", section on "Safety".
1308. "Freedom in the World 2022:Namibia", Freedom House, section D1.
1309. "2022 Country Reports on Human Rights Practices: Namibia", US State Department, section 2A.
1310. Personal communication with the counter-protester, June 2023.
1311. "Namibian journalists investigated for trespassing for drone journalism", Committee to Protect Journalists, 28 March 2022
1312. Personal communication with John Grobler, 24 August 2023.
1313. June Shimuoshili, "A Beacon of Hope for Press Freedom" in "The State of Press Freedom in Southern Africa 2020-2021", Media Institute of Southern Africa (MISA), pages 44-46.
1314. "African Media Barometer Namibia 2022", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), pages 66-67; "CIPESA and Small Media UPR Submission, Session 38", [2020]. paragraph 12.
1315. "African Media Barometer Namibia 2022", Media Institute of Southern Africa (MISA) and Friedrich-Ebert-Stiftung (FES), page 67.
1316. Id, page 67. No further details about this incident were provided.
1317. Id, page 68.
1318. Tom Rhodes, "In Namibia seal hunt, journalists said to become prey", Committee to Protect Journalists, 17 July 2009.
1319. Tom Rhodes, "A quiet victory for The Namibian", Committee to Protect Journalists, 9 September 2011.
1320. *Geingos (born Kalondo) v Hishoono* 2022 (2) NR 512 (HC).
1321. "Freedom in the World 2022: Namibia", section D1; Maria Amakali, "Nujoma sues over N$1.5m extortion claims",

New Era, 30 September 2021.
1322. *Free Press of Namibia (Pty) Ltd and Others v Nyandoro* 2018 (2) NR 305 (SC).
1323. *Nghiwete v Nekundi* 2009 (2) NR 759 (HC).
1324. *Shikongo v Trustco Group International Ltd and Others* 2009 (1) NR 363 (HC).
1325. Roman Grynberg, Shinovene Immanuel and Tangeni Amupadhi, *Fishrot: Fisherties and Corrupton in Namibia*, 2023.
1326. Lesotho's cybercrime law had been passed by Parliament as of mid-2023, but had not yet received Royal Assent and was still a under debate.
1327. The government invited written submissions from the public, but these do not appear to have had much influence on the revised 2017 Bill. See Frederico Links, "Tackling Cyber Security/Crime In Namibia – Calling For A Human Rights Respecting Framework", Institute for Public Policy Research, January 2018 at 1-2, 11.
1328. The splitting of the two bills was recommended by civil society; see id at 12.
1329. Electronic Transactions Act 4 of 2019.
1330. The government circulated a draft Computer Security and Cybercrimes Bill for comment in 2021, but this version of the bill was the same as the one circulated in 2019.The Ministry of Information and Communication Technology (MICT) has indicated that the bill has been revised since it was last circulate, but the revised version has not yet been made available to the public. MICT input to Child Online Protection Task Force quarterly meeting, 28 June 2023. For more information about the background to the bill, see "Familiar Flaws – Unpacking Namibia's draft Cybercrime Bill", Institute for Public Policy Research (IPPR), February 2022, sections 1 and 2.
1331. See also "Situation Report Namibia: Legislation on cybercrime and electronic evidence", GLACY+ (Global Action on Cybercrime Extended), Version 20 March 2020, page 8 on this clause: "The carveouts are well-drafted and a positive addition to the draft legislation […]."
1332. *Draft Combating of Sexual Exploitation Bill*, October 2020, which would create offences aimed at child pornography, voyeurism, non-consensual distribution of intimate images, grooming and other forms of sexual exploitation, with particular attention to the protection of children and persons with severe mental disabilities. The development of this bill was commissioned by Sisters for Change (an international NGO which is a member of the Equality & Justice Alliance), acting in consultation with the Minister of Justice, from the Legal Assistance Centre (a Namibian NGO)
1333. *Draft Combating of Harassment Bill*, October 2020. which was part of the same project. The two bills were initially combined, but split at the suggestions of a consultation with key stakeholders in February 2020.
1334. This is the *Prohibition of Discrimination, Discriminatory Harassment and Hate Speech Bill*, which was discussed at a public consultation in May 2021.
1335. Discussions at consultations around these bills attended by the authors during 2021-2023.
1336. The offence is contained in clause 13 of the *Draft Computer Security And Cybercrime Bill, 2019,* and the definition appears in clause 1.
1337. *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse Adopted by the Interagency Working Group in Luxembourg* ("Luxembourg Guidelines)", adopted by the Interagency Working Group in Luxembourg, 28 January 2016 at 27-28 (footnotes omitted).
1338. *Draft Computer Security and Cybercrime Bill, 2019*, clause 15.
1339. See the section on criminal defamation in Chapter 2 of this report.
1340. "Input on the Cybercrime Bill as discussed during the workshop held on 17-28 February 2020", Legal Assistance Centre, 30 April 2020.
1341. *Draft Computer Security and Cybercrime Bill, 2019*, clause 18(1): "The provisions of Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) are construed to relate to computer systems, computer equipment, storage media or data."
1342. Criminal Procedure Act 51 of 1977, sections 21-23.
1343. Id, clause 20.
1344. *Draft Computer Security and Cybercrime Bill, 2019*, clause 19.
1345. Id, clause 21(1) and definition of "forensic tool" in clause 1.
1346. Id, clause 21(1).
1347. Id, clause 21(4).
1348. Id, clause 21(8).
1349. Id, clause 21(2).
1350. Communications Act 8 of 2009, section 117(1)(d). The Act does not define a "telecommunications device", but "telecommunications services" means "services whose provision consists wholly or partly in the transmission or routing of information on telecommunications networks by means of telecommunications processes but does not include broadcast services" (section 1)
1351. Communications Act 8 of 2009, section 117(1)(e).
1352. Id, section 117(1)(f) and (g).
1353. Id, section 117(1)(g).
1354. Id, section 70.
1355. Id, sections 71-72.
1356. Regulations in terms of Part 6 of Chapter V of the Communications Act, issued on 15 March 2021. This discussion draws on "Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?", Legal Assistance Centre [written by one of the authors of this paper], June 2021.
1357. "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014.

1358. Regulations in terms of Part 6 of Chapter V of the Communications Act,, regulation 5.
1359. Section 22 of the Criminal Procedure Act 51 of 1977 allows a police official to search any person or container or premises without a search warrant if *that police official* believes on reasonable grounds that a search warrant would be issued but that the delay in obtaining the warrant would defeat the object of the search.
1360. Regulations in terms of Part 6 of Chapter V of the Communications Act,, regulation 5(7).
1361. "Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?", Legal Assistance Centre [written by one of the authors of this paper], June 2021, page 4 (reference omitted).
1362. Namibian Constitution, Article 13(1).
1363. Frederico Links "Quality of Democracy Under Threat", *IPPR blog*, 20 June 2023, quoting
1364. Namibian Central Intelligence Service Act 10 of 1997, section 24(2).
1365. Id, section 25(1)(b).
1366. Id, section 25(3)-(4).
1367. Prevention and Combating of Terrorist and Proliferation Activities Act 4 of 2014, section 40.
1368. Id, section 41(1)(b).
1369. Id, section 41(3)-(4).
1370. Electronic Transactions Act 4 of 2019, sections 51-52 and 54(1) and (8).
1371. Id, section 54(3)-(7).
1372. Id, section 54(2)
1373. See, for example, "Submission: Draft Provisions of the Electronic Transactions and Cybercrime Bill", Access to Information Namibia (ACTION) Coalition, 13 September 2017.
1374. Namibian Constitution, Articles 28(2), 46, 49 and 69(1).
1375. Article 94B was inserted into the Namibian Constitution by the Namibian Constitution Third Amendment Act 8 of 2014.
1376. Electoral Act 5 of 2014.
1377. See, for example, "Namibia and South Africa's ruling parties share a heroic history - but their 2024 electoral prospects look weak", *The Conversation*, 10 May 2023; "Namibia election: president wins second term despite scandal and recession", *The Guardian*, 1 December 2019.
1378. *Itula & Others v Minister of Urban & Rural Development & Others* 2020 (1) NR 86 (SC); Ndjodi Ndeunyema,"Vote, But You Cannot Verify: The Namibian Supreme Court's Presidential Election Decision", Oxford Human Rights Hub, 17 February 2020.
1379. "Namibia Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
1380. Namibian Constitution, Article 29(3).
1381. Edward Mumbuu, "Road to State House gets crowded", *New Era*, 5 May 2023.
1382. Electoral Act 5 of 2014, sections 174(1)(d) and 175(1)(d)(i).
1383. Id, section 178(1)(b).
1384. Id, section 180.
1385. Id, Schedule ,: Bill of Fundamental Voters' Rights and Duties, items 3.3 and 3.5, read with section 95(b) of the Act.
1386. Id, section 187.
1387. General Notice 143/1992 (Government Gazette 503).
1388. The Broadcasting Code for Broadcasting Licensees is issued under the Communications Act 8 of 2009, section 89. It is contained in General Notice 602/2018 (Government Gazette 6750), Part C, and definitions in section 1. The Code is amended by General Notice 134/2019 (Government Gazette 6915) and by General Notice 24/2021 (Government Gazette 7445), but these amendments do not affect the provisions discussed here.
1389. See Part C, in particular sections 19, 20(2), 21 and 22. The references in section 21 to the "formulae" in section 22 are unclear.
1390. Penal Code (Amendment) Act 42 of 2021. See "President Ramkalawan Assents to the Penal Code (Amendment) Act 2021", Office of the President of the Republic of Seychelles, 20 October 2021.
1391. Data Protection Act 9 of 2003. Section 28 of the Constitution contains a few basic data protection provisions.
1392. Access to Information Act 4 of 2018.The Constitution protects the right to information in section 28.
1393. Newspaper Act [*Cap 147*] (revised 1991), sections 3 and 8 in particular.
1394. Film Classification Board Act 2 of 1994; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, pages 217-218.
1395. Broadcasting and Telecommunication Act 2 of 2000.
1396. Communications Act 3 of 2023.
1397. "Communications Bill 16 of 2022", "Objects and Reasons".
1398. "New regulatory authority to be established under approved Communications Bill", National Assembly, 23 March 2023. The Seychelles Licensing Authority (SLA) is established by section 3 of the Licences Act 23 of 2010. The Broadcasting and Telecommunications Act 2 of 2000 requires all broadcasting services to have a licence issued by the SLA, but this requirement will fall away under the Communications Act 3 of 2023 (see section 173(2)(b)). The SLA is responsible for many types of licences issued in Seychelles in areas unrelated to the media, so it will continue to exist. See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, at page 202 (published before the Communications Act 3 of 2023 was enacted).
1399. Communications Act 3 of 2023, section 4.
1400. Id, sections 148 and 158.
1401. Id, section 163(2).

1402. Id, section 149(4).
1403. Id, sections 6 and 172.
1404. Id, sections 132-133.
1405. Id, section 136.
1406. Id, sections 134-135.
1407. Id, sections 143-144.
1408. Seychelles 1993 Constitution, revised 2017, section 168.
1409. Seychelles Broadcasting Corporation Act, 2011 (as amended to 2012).
1410. Id, section 4.
1411. Id, section 3(3).
1412. "The National Information Services Agency", *Seychelles NATION*, 28 June 2021. The original National Information Services Agency Act, 2010 can be found here. The revised version could not be located online.
1413. "Freedom of the Press 2015: Seychelles", Freedom House, "Legal Environment".
1414. Seychelles Media Commission Act 36 of 2010, as amended by the Seychelles Media Commission (Amendment) Act 7 of 2017 (affecting sections 4, 6, 7, 10A and 12) and by the Seychelles Media Commission (Amendment) (No. 2) Act 18 of 2017 (affecting section 4).
1415. Id, section 13(1).
1416. Id, section 4 (as amended by the Seychelles Media Commission (Amendment) Act 7 of 2017 and by the Seychelles Media Commission (Amendment) (No. 2) Act 18 of 2017).
1417. Id, section 10A (as inserted by by the Seychelles Media Commission (Amendment) Act 7 of 2017).
1418. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 12: Seychelles", Konrad Adenauer Stiftung, 2021, page 209.
1419. Id, selected duties from section 13(2)/
1420. Id, section 19.
1421. Code of Conduct for the Media in Seychelles, 2013.
1422. Facebook post, Seychelles Media Commission, 25 May 2020; Facebook post, Seychelles Media Commission 15 Oct 2019. Note that the SMC website was inaccessible during the preparation of this chapter.
1423. Seychelles Media Commission Act 36 of 2010, section 14; Code of Conduct for the Media in Seychelles, 2013, Preamble.
1424. Code of Conduct for the Media in Seychelles, 2013, sections 1.2 and 2.
See, for example, "Seychelles Media Commission: Complaint by the Chief Press Secretary against Le Seychellois Hebdo", reproduced in Facebook post by State House Seychelles, 30 November 2013.
1425. Code of Conduct for the Media in Seychelles, 2013, Annexe.
1426. Seychelles 1993 Constitution, revised 2017, section 22.
1427. *Seychelles National Party v Michel* [2010] SCCA 9.
1428. Id, Part II (unpaginated online version).
1429. Id, Part III (unpaginated online version).
1430. *Sullivan v Attorney General and another* (SCA 25 of 2012) [2014] SCCA 29 (14 August 2014).
1431. Id, paragraph 29
1432. Id, paragraph 32.
1433. *The Seychelles National Party and Others v The Government of Seychelles*, CC No 02/2014 / *Dhanjee v Alix and Others*, CC No 03/2014 [2015] SCCC 2. This was a consolidation of two cases raising similar issues.
1434. Id, paragraphs 15-16.
1435. Id, paragraph 54.
1436. Id, paragraphs 62 and 65.
1437. Id, paragraphs 65-68.
1438. Id, paragraphs 95-102.
1439. Id, paragraph 225.
1440. Id, paragraphs 227-229.
1441. "World Press Freedom Index 2023: Seychelles", Reporters Without Borders (subheadings omitted).
1442. "2022 Country Reports on Human Rights Practices: Seychelles ", US State Department, section 2A.
1443. Id.
1444. Id.
1445. "Freedom in the World 2023: Seychelles", Freedom House, section D.
1446. "Southern African Development Community Cybersecurity Maturity Report 2021", Cybersecurity Capacity Centre for Southern Africa (C3SA), 2022. The amendments were made by the Penal Code (Amendment) (No. 2) Act 12 of 2016. The new offences are oddly placed in Chapter XXXVI of the Penal Code, which is entitled "Offences relating to coin and to bank and currency notes".
1447. Cybercrimes and Other Related Crimes Act 59 of 2021.
1448. "Technology, Media and Telecommunications Africa Quarterly e-Bulletin", Werkman's Attorneys, 26 May 2022, citing the Cybercrimes and Other Related Crimes Act, 2021 (Commencement) Notice gazetted on 31 January 2022.
1449. "New law to better fight cyber, other crimes committed on social media, digital platforms", *Seychelles NATION*, 25 November 2021.
1450. Vidya Gappy, "Cybercrime Unit in the offing", *Seychelles Nation*, 28 January 2023.
1451. Electronic Transactions Act 8 of 2001.

1452. Penal Code (updated to 1 June 2021), as amended by the Penal Code (Amendment) Act 42 of 2021.
1453. Penal Code (updated to 1 June 2021).
1454. Cybercrimes and Other Related Crimes Act 59 of 2021, section 30.
1455. Id, section 42 read with sections 25. 30 and 30A of the Penal Code (updated to 1 June 2021).
1456. Id, section 20 read with the definitions in section 2.
1457. Id, section 21.
1458. Id, section 22.
1459. Id, section 23.
1460. Id, section 24.
1461. Id, section 25. We did not locate any broader take-down provisions in any other laws in Seychelles.
1462. Id, section 41.
1463. Penal Code (updated to 1 June 2021), as amended by the Penal Code (Amendment) Act 42 of 2021.
1464. Penal Code (Amendment) Act 42 of 2021, which repealed Chapter VIII of the Penal Code in its entirety.
1465. Penal Code (Amendment) Bill, 2021 (Bill No. 42 of 2021), Explanatory Statement, *Supplement to Official Gazette*, 16th September 2021, following page 725.
1466. "LEXOTA Country Analysis: Seychelles", last updated July 2022.
1467. Electronic Transactions Act 8 of 2001, section 45. In the judicial hierarchy I nSeychelles, the Supreme Court is below the Court of Appeal and the Constitutional Court, but above the Magistrates' Courts.
1468. Communications Act 3 of 2023, section 90.
1469. "2022 Country Reports on Human Rights Practices: Seychelles ", US State Department, section 2A.
1470. Broadcasting and Telecommunication Act 2 of 2000, section 34.
1471. Communications Act 3 of 2023, section 95.
1472. "Stricter SIM card registration to curb criminality", *Seychelles NATION*, 16 December 2020.
1473. This offence is not contained in any statute, but is a common-law offence (referring to laws that are developed over time through court decisions). See *Hoho v The State* [2008] ZASCA 98; 2009 (1) SACR 276 (SCA); Motsepe v S (A 816/2013) [2014] ZAGPPHC 1016; 2015 (2) SACR 125 (GP); 2015 (5) SA 126 (GP) (5 November 2014)
1474. Protection of Personal Information Act 4 of 2013 (popularly known as POPI). The Act came fully into force on 1 July 2020, with a one-year grace period for compliance ending on 30 June 2021. As of mid-2023, there have been no amendments to the law. There is a right of access to information in section 32 of the South African Constitution which requires that national legislation must be enacted to give effect to this right.
1475. Promotion of Access to Information Act 2 of 2000 (popularly known as PAIA), with its amending acts listed separately (with hyperlinks) on the same webpage. A consolidated version dated 30 June 2021 can be found here.
1476. Imprint Act 43 of 1993, as amended by the Imprint Amendment Act 18 of 1994.
1477. Films and Publications Act 65 of 1996, original version.
1478. Films and Publications Act 65 of 1996, as amended in 2009. The relevant amendments were made by the Films and Publications Amendment Act 3 of 2009.
1479. *Print Media South Africa v Minister of Home Affairs* 2012 (6) SA 443 (CC).
1480. Films and Publications Amendment Act 11 of 2019.
1481. The Cybercrimes Act 19 of 2020 repealed section 24B of the Films and Publication Act 65 of 1996. The version of the Cybercrimes Act linked in this footnote includes full details of all the repeals and amendments to other laws made by Act 19 of 2020.
1482. Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 4, 6.
1483. Id, sections 9A-10.
1484. Id, sections 6A- 6B.
1485. Id, section 5.
1486. Id, section 3(2).
1487. South African 1996 Constitution, as amended through 2012, Article 192.
1488. Independent Communications Authority of South Africa Act 13 of 2000 (current version).
1489. "Manual issued in terms of section 14 of the Promotion of Access to Information Act 2 of 2000", ICASA, 2020, section 2; Independent Communications Authority of South Africa Act 13 of 2000 (current version), section 4.
1490. Independent Communications Authority of South Africa Act 13 of 2000 (current version), section 4B.
1491. Id, sections 5 and 8.
1492. Broadcasting Act 4 of 1999 (current version). section 38.
1493. Electronic Communications Act 36 of 2005 (current version).
1494. Id, section 5
1495. Id, section 54 read with Independent Communications Authority of South Africa Act 13 of 2000 (current version), sections 17A-17B
1496. Electronic Communications Act 36 of 2005 (current version), section 69.
1497. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, page 285.
1498. Broadcasting Act 4 of 1999 (current version), section 13.
1499. Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" and "Political-economic and regulatory shifts" (online unpaginated version).

1500. Justine Limpitlaw, "Non-appointment of SABC Board raises spectre of lapdog broadcaster for 2024 elections", *Daily Maverick*, 20 February 2023; "Ramaphosa finally appoints SABC board", *IOL*, 18 April 2023; Chris Roper, "South Africa", Reuters Institute for the Study of Journalism, 14 June 2023; Dianne Kohler Barnard (DA Shadow Minister of Communications), "SABC Board: President's conduct "grossly unlawful" – DKB", *Politics Web*, 13 July 2023. The case was brought by Media Monitoring Africa (MMA) and others.
1501. See generally Joe Thloloe, "Chapter 7: The South African Regulatory Regimes in Print, Broadcasting and Online" in Una Seery, ed, *Media Landscape 2012*, Government Communication and Information System, 2012.
1502. Code of Ethics and Conduct for South African Print and Online Media, 2020.
1503. "Complaints Procedures", Press Council, effective January 2020.
1504. All three Codes are available here.
1505. "Criteria for a complaint", BCCSA, undated.
1506. DMMA Professional Code of Conduct, 2010.
1507. ISPA Code of Conduct, Version 3.1 (revised 5 June 2023).
1508. "Complaints process", ISPA, undated.
1509. "How to lodge a take down", ISPA, undated.
1510. WASPA Code of Conduct, Version 17.5 (revised 28 June 2023)
1511. *Media Monitoring Africa v. eNCA Channel 403*, Case No. 09/2020, 30 June 2021; see the case summary by Global Freedom of Expression here.
1512. Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "Normative debates" (online unpaginated version); *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.126-ff.
1513. Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" and "Normative debates" (online unpaginated version); *Report on Press Regulation in South Africa*, Press Freedom Commission, 2012; *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.92-ff (background to Press Freedom Commission), paragraphs 12-155-12.156 (summary of key points in Press Freedom Commission report)
1514. Id, "Normative debates" (online unpaginated version).
1515. *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.157, 12.160-12.162.
1516. Id, paragraph C34.
1517. Id, paragraph 12.165.
1518. Media Development and Diversity Agency Act 14 of 2002 (definition of "media" in section 1); Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, page 271; Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The South African media landscape" (online unpaginated version).
1519. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, pages 261-262.
1520. This discussion draws on Eshed Cohen. "Chapter 11: Freedom of Expression" in Allsop et al, eds, *Constitutional Law for Students: Part 2*, UCT Libraries, 2020 (Chapter 11, sections 13(b) and 5).
1521. *Moyo v Minister of Police* [2019] ZACC 40, 22 October 2019. paragraph 66. The Court went on to invalidate the provision in question on the grounds that it did not pass the test for a justifiable restriction of freedom of expression.
1522. South African 1996 Constitution, as amended through 2012, section 16(2)(c) (emphasis added).
1523. South African 1996 Constitution, as amended through 2012, section 36(1).
1524. *Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International* 2006 (1) SA 144 (CC); see paragraph 47.
1525. *Hoho v The State* [2008] ZASCA 98; 2009 (1) SACR 276 (SCA).
1526. Id, paragraph 2.
1527. Id at paragraphs 27-36.
1528. Id, paragraph 32.
1529. Id, paragraph 33.
1530. Id, paragraph 36-37.
1531. Motsepe v S (A 816/2013) [2014] ZAGPPHC 1016; 2015 (2) SACR 125 (GP); 2015 (5) SA 126 (GP) (5 November 2014).
1532. Id, paragraph 3.
1533. Id, paragraph 40.
1534. Id, paragraph 46.
1535. Id, paragraphs 20-22.
1536. Id, paragraphs 49-50.
1537. "Criminal Defamation", Bregmann's Law Firm, undated. See also *2022 Country Reports on Human Rights Practices*, "South Africa", US State Department, section 2A. The US State Department notes that the common law also prohibits blasphemy, although reports indicated that the last known prosecution for blasphemy was in 1968.
1538. See also Koko v Tanton, Johannesburg High Court. Case no 2021/2212, 7 September 2021.
1539. Mineral Sands Resources (Pty) Ltd v Reddell [2022] ZACC 37, 14 November 2022, paragraphs 42-43.
1540. Id, paragraph 94.
1541. Id, paragraph 96.

1542. Id, paragraph 100.
1543. *Van Breda v Media 24 Ltd*, Supreme Court of Appeal, Case no: 425/2017, 21 June 2017; see the Global Freedom of Expression case summary here. Some other cases on media access to courts and similar proceedings are *Mail and Guardian Ltd v Judicial Service Commission*, Johannesburg High Court, Case No. 09/30894, 29 July 2009; *South African Broadcasting Co. v Thatcher*, High Court, Cape of Good Hope Provincial Division, Case No:8924/2004, 31 August 2005; *Dotcom Trading 121 (Pty) Ltd v King* [2000] 4 All SA 128 (C), 2 August 2000.
1544. *Primedia Broadcasting v Speaker of the National Assembly*, Supreme Court of Appeal, Case no: 784/2015, 29 September 2016; see the Global Freedom of Expression case summary here.
1545. Trustees For The Time Being of the Media Monitoring Project Benefit Trust v SABC Soc Ltd, ICASA Complaints and Compliance Committee, Case No. 195/2016, 24 February 2016.
1546. *M&G Media Ltd v Chipu NO* [2013] ZACC 32; 2013 (6) SA 367 (CC).
1547. "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
1548. *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 10.50-10.56, 10.77-10.80.
1549. Id, paragraphs 10.57-10.63.
1550. "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
1551. "South African journalists attacked, threatened, harassed in separate incidents", Committee to Protect Journalists, 7 April 2023; "Two South African journalists assaulted in separate incidents", Committee to Protect Journalists, 9 March 2023; "News crews harassed, reporter arrested during South Africa's municipal elections", Committee to Protect Journalists, 9 December 2021; "South African journalists attacked and threatened amid civil unrest, 4 radio stations looted", Committee to Protect Journalists, 13 July 2021; "South African EFF party supporters block journalists from covering protest", Committee to Protect Journalists, 29 June 2021; "South African journalists attacked covering farmer protest", Committee to Protect Journalists, 9 October 2020.
1552. Chris Roper, "South Africa", Reuters Institute for the Study of Journalism, 14 June 2023.
1553. *South African National Editors' Forum (SANEF) v The Economic Freedom Fighters (EFF)* (90405/18) [2019] ZAEQC 6 (24 October 2019).
1554. *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraph 10.17.
1555. Id, paragraph 10.13.
1556. Id, paragraphs 10.10-10.18; Herman Wasserman, "The state of South African media: A space to contest democracy", 65(3) *Publizistik* 451 (2020), "The impact of democratic transition on the media" (unpaginated online version); "Bell Pottinger collapses after South African scandal", *BBC News*, 12 September 2017; "Deal that undid Bell Pottinger: inside story of the South Africa scandal", *The Guardian*, 5 September 2017.
1557. See Jon Alsop, "Were the Gupta Leaks South Africa's Watergate?", *Daily Maverick*, 24 September 2018.
1558. *Maughan v Zuma* High Court of South Africa, Kwazulu-Natal Division, Pietermaritzberg, Case No 12770/22P, 7 June 2023; "South African court prohibits former president's private prosecution of journalist Karyn Maughan", Committee to Protect Journalists, 8 June 2023; "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
1559. "South Africa judge strikes down gag order against investigative outlet amaBhungane", Committee to Protect Journalists, 3 July 2023.
1560. *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 1.
1561. "South African court's gag on amaBhungane raises fears for investigative journalism, sources", Committee to Protect Journalists, 7 June 2023.
1562. *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 16.
1563. Id, paragraph 34.
1564. Id, paragraph 45.
1565. *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 25, quoting *Bosasa Operation (Pty) Ltd v Basson* 2013 (2) SA 570 (GSJ) at para 38, which was also quoted with approval by the Constitutional Court in *AmaBhungane Centre for Investigative Journalism v. Minister of Justice and Minister of Police v AmaBhungane Centre for Investigative Journalism* 2021 (3) SA 246 (CC), 4 February 2021, paragraph 115.
1566. *Mazetti Management Services (Pty) Ltd v AmaBhungane Centre for Investigative Journalism NPC*, High Court, Gauteng Division, Case no 2023-050131, 3 July 2023, paragraph 45.
1567. "Cybercrimes Act in South Africa: Overview and Read", Michaelson's, undated. "The national legislature or Parliament consists of two Houses: the National Assembly and National Council of Provinces, whose members are elected by the people of South Africa. Each House has its own distinct functions and powers, as set out in the Constitution. The National Assembly is responsible for choosing the President, passing laws, ensuring that the members of the executive perform their work properly, and providing a forum where the representatives of the people can publicly debate issues. The National Council of Provinces is also involved in the law-making process and provides a forum for debate on issues affecting the provinces. Its main focus is ensuring that provincial interests are taken into account in the national sphere of government." "Parliament", National Government of South Africa, undated. For an overview of the crimes in the

Cybercrimes Act, see Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).

1568. Murray Hunter was interviewed via Zoom on 13 July 2023.
1569. Cybercrimes Act 19 of 2020, section 1
1570. Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 69.
1571. *Memorandum on the Objects of the Cybercrimes and Cybersecurity Bill, 2017*, appended to the Cybercrimes and Cybersecurity Bill, 2017 [B6-17]. Note that this is not the final version of the Bill.
1572. Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 67.
1573. Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, page 72.
1574. Id, page 69.
1575. Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
1576. Brian Sang YK and Ivan Sang, "A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards", *Commonwealth Cybercrime Journal*, undated online version, pages 73, 74.
1577. Id, page 74.
1578. Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
1579. Id.
1580. Id.
1581. Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, as amended up to July 2022; this includes the amendments by the Cybercrimes Act 19 of 2020 (with effect from 1 December 2021) and the subsequent amendments by the Criminal Law (Sexual Offences and Related Matters) Amendment Act Amendment Act 13 of 2021 (with effect from 31 July 2022). The Cybercrimes Act inserts Part 3A into that Act, comprising section 11A on **Harmful disclosure of pornography,** and related provisions 11B-11D. It also inserts section 19A on **Offences relating to child pornography**. For more information on the amendments made by the Cybercrimes Act, this version of the Cybercrimes Act 19 of 2020 includes full details of all its repeals and amendments to other laws.
1582. See the discussion of the Films and Publications Act 65 of 1996 below.
1583. Protection from Harassment Act 17 of 2011, as amended by the Domestic Violence Amendment Act 14 of 2021.
1584. Sizwe Snail ka Mtuze andMelody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
1585. Cybercrimes Act 19 of 2020, section 17.
1586. In this section of the Constitution, an "organ of state" means any department of state or administration in the national, provincial or local sphere of government, or any other functionary or institution that is exercising a power or performing a function in terms of the Constitution, a provincial constitution or any legislation, but does not include a court or a judicial officer. South African 1996 Constitution, as amended through 2012, section 239.
1587. Cybercrimes Act 19 of 2020, section 20. *Ex parte* means that the application can be made without notice to the other party.
1588. Id, section 22(2).
1589. Id, section 22(1).
1590. Id, section 29.
1591. Id, section 30.
1592. Id, section 1, definition of "specifically designated police official".
1593. Id, section 32.
1594. Criminal Procedure Act 51 of 1977, section 25.
1595. Cybercrimes Act 19 of 2020, section 40.
1596. Id, sections 41-43. As noted above, a "specifically designated police official".is a police official of the rank of captain or higher who has been designated in writing by the National Commissioner and the National Head of the Directorate for this purpose. Id, section 1, definition of "specifically designated police official".
1597. Id, section 44.
1598. Id, sections 48, 52.
1599. Id, section 54.
1600. Id, section 56.
1601. Electronic Communications and Transactions Act 25 of 2002 (current version), sections 53-ff, read with definition of "critical data" and "critical database" in section 1.
1602. Id, sections 29-ff.
1603. Id, sections 80-ff.
1604. Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.
1605. Electronic Communications and Transactions Act 25 of 2002 (current version), section 77.
1606. Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.
1607. Films and Publications Act 65 of 1996, updated to 1 March 2022. Note that (as of mid-2023) the PDF on this page contained the Act as updated only to 2009, while the "rtf" download contained the Act as updated to March 2022.

1608. "Film" means "any sequence of visual images recorded in such a manner that by using such recording, such images will be capable of being seen as a moving picture, and includes any picture intended for exhibition through any medium, including using the internet, or device". Id, section 1
1609. "Game" means "a computer game, video game or other interactive computer software for interactive game playing, including games accessed or played using the internet, where the results achieved at various stages of the game are determined in response to the decisions, inputs and direct involvement of the game player or players". Id.
1610. "Publication" means, and includes where applicable, "any of the following, published using the internet -
    (a) any newspaper, magazine, book, periodical, pamphlet, poster or other printed matter;
    (b) any writing or typescript which has in any manner been duplicated;
    (c) any drawing, picture, illustration or painting;
    (d) any print, photograph, engraving or lithograph;
    (e) any record, magnetic tape, soundtrack or any other object in or on which sound has been recorded for reproduction;
    (f) computer software which is not a film;
    (g) the cover or packaging of a film; and
    (h) any figure, carving, statue or model;
    (i) any content made available using the internet, excluding a film or game". Id.
1611. Id, definition of "identifiable group characteristic" in section 1.
1612. John Paul Ongeso, "South Africa: Films and Publications Amendment Act comes into Operation", Bowmans, 3 March 2022.
1613. Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G.
1614. Id, sections 18G and 24F.
1615. Id, sections 18F and 24E.
1616. Id, section 24E.
1617. Id, section 18F(4) and (5).
1618. Id, section 18E(3).
1619. Id, section 27A.
1620. Wilmari Strachan and Naledi Ramoabi, **"**Amendments to the Films and Publications Act, 1996 are now in force", ENSight, ENS Africa law firm, 17 March 2022, referring to the Electronic Communications and Transactions Act 25 of 2002, section 78(1)
1621. For information on South African jurisprudence on hate speech, see Jacob Mchangama & Natalie Alkiviadou, "South Africa The Model? A Comparative Analysis of Hate Speech Jurisprudence of South Africa and the European Court of Human Rights" 1 *Journal of Free Speech Law* 543 (2022).
1622. South African 1996 Constitution, as amended through 2012, section 16(2).
1623. Promotion of Equality and Prevention of Discrimination Act 4 of 2000 (PEPUDA), section 10 read with the definition of "prohibited grounds" in section 1 and the proviso to section 12.
1624. *Qwelane v South African Human Rights Commission*, [2021] ZACC 22, 30 July 2021; see case summary by Global Freedom of Expression here. See also *AfriForum v EFF, Malema and Ndlozi*, Equality Court, 25 August 2022 and *Afriforum NPC v. Nelson Mandela Foundation Trust*, Supreme Court of Appeal(Case no 371/2020) [2023] ZASCA 58 (21 April 2023).
1625. Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G, definition of "identifiable group characteristic" in section 1.
1626. Code of Conduct for Broadcasting Service Licensees, 2009, issued in terms of section 54 of the Electronic Communications Act No. 6 of 2005, regulation 3.
1627. Prevention and Combating of Hate Crimes and Hate Speech Bill [B9B-2018]; see the *Memorandum on the Objects of the Prevention and Combating of Hate Crimes and Hate Speech Bill* appended to the Bill and the history prepared by the Parliamentary Monitoring Group on the same webpage. "The national legislature or Parliament consists of two Houses: the National Assembly and National Council of Provinces, whose members are elected by the people of South Africa. Each House has its own distinct functions and powers, as set out in the Constitution. The National Assembly is responsible for choosing the President, passing laws, ensuring that the members of the executive perform their work properly, and providing a forum where the representatives of the people can publicly debate issues. The National Council of Provinces is also involved in the law-making process and provides a forum for debate on issues affecting the provinces. Its main focus is ensuring that provincial interests are taken into account in the national sphere of government." "Parliament", National Government of South Africa, undated.
1628. Regulation of Interception of Communications and Provision of Communication related Information Act 13 of 2002 (RICA), as amended to 1 December 2021. There have been no further amendments as of mid-2023.
1629. Id, Chapters 2-3.
1630. Id, Chapter 6.
1631. Id, Chapter 7.
1632. Id, section 51(3)(a).
1633. Ruan Jooste, "Rica SIM card registration laws in SA are ineffective in reducing crime", IOL Business Report, 30 August 2022.
1634. *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* [2021] ZACC 3, 4 February 2021; see the case summary by Global Freedom of Expression here.

1635. Id, paragraphs 124-135
1636. General Intelligence Laws Amendment Bill; Heidi Swart, "GILAB: New Intelligence Bill a blueprint for State Capture 3.0", *News24*, republished by *Intelwatch*, 11 July 2023. For more detailed information on potential law reforms on communications surveillance in South Africa, see Catherine Kruyer, "Reforming Communication Surveillance in South Africa: Recommendations in the wake of the *AmaBhungane* judgment and beyond", Intelwatch & The Media Policy and Democracy Project Report, May 2023
1637. The ISPA statistics can be found here.
1638. See "Freedom in the World 2023: South Africa", Freedom House, sections A1-A2.
1639. Electoral Commission Act 51 of 1996.
1640. Electoral Act 73 of 1998.
1641. "Freedom in the World 2023: South Africa", Freedom House, section A3.
1642. "Namibia and South Africa's ruling parties share a heroic history - but their 2024 electoral prospects look weak", *The Conversation*, 10 May 2023; "South Africa Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
1643. "South Africa Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political and Social Integration".
1644. Id, "Executive Summary".
1645. Electoral Act 73 of 1998.
1646. Id, section 96(2).
1647. Electoral Code of Conduct, Electoral Act 73 of 1998, Schedule 2.
1648. Id, item 3.
1649. Id, item 4(1)(a).
1650. Id, item 4(1)(b).
1651. Id, item 9(1)(a)-(c).
1652. Id, item 9(2)(d).
1653. Id, item 8.
1654. *Democratic Alliance v African National Congress* [2015] ZACC 1, 19 January 2015; see the case summary by Global Freedom of Expression here.
1655. Nkandla is the name of then-President Zuma's private residence. The Nkandla Report was the report of an investigation by South Africa's Public Protector [Ombud] into complaints about the enormous costs of installing security measure at that residence. Id, paragraphs 7-ff and footnote 7 (dissenting opinion of Zondo, J).
1656. Id, paragraph 135 in the joint opinion of Cameron J, Froneman J and Khampepe J (Moseneke DCJ and Nkabinde J concurring), which begins at paragraph 116:
1657. Id, paragraphs 139-140.
1658. Id paragraphs 144-147.
1659. Opinion of Van der Westhuizen J (Madlanga J concurring), paragraphs 170-ff.
1660. Opinion of Zondo J (Jafta J and Leeuw AJ concurring), starting at paragraph 1.
1661. Brown v Economic Freedom Fighters, High Court of South Africa, Gauteng Local Division, Johannesburg, Case No: 14686/2019, 6 June 2019; see the case summary by Global Freedom of Expression here. See also Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, pages 333-334.
1662. *My Vote Counts v Minister of Justice and Correctional Services* [2018] ZACC 17, 21 June 2018. see the case summary by Global Freedom of Expression here.
1663. See The Written Laws (Miscellaneous Amendments) Act, 2023 (published in bill form); the final amendment Act could not be located online.
1664. *Media Council of Tanzania & 2 Others v Attorney General of the United Republic of Tanzania*, East African Court of Justice, Case No 2 of 2017, 28 March 2019. Some amendments to the Act in question were made in 2023 but they did not remove criminal defamation.
1665. The Personal Data Protection Act 11 of 2022.
1666. The Access to Information Act 6 of 2016.
1667. United Republic of Tanzania's 1977 Constitution, as amended through 2005, Article 2(1).
1668. The Cybercrimes Act 14 of 2015, section 2: "Save for section 50 [on the compounding of offences], this Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar."
1669. The Tanzania Communications Regulatory Authority Act 12 of 2003, section 2(3)-(4). The Act does not apply to Tanzania Zanzibar with respect to broadcasting and content matters.
1670. The Electronic and Postal Communications Act [Chapter 306 R E. 2022], section 2 (with an exception for the activities that fall within the jurisdiction of the Zanzibar Broadcasting Commission under the Zanzibar Broadcasting Commission Act 7 of 1997). The initial Electronic and Communications Act was Act 3 of 2010, but it has been amended several times since it was passed.
1671. The Tanzania Telecommunications Corporation Act 12 of 2017, section 2.
1672. The Tanzania Communications Regulatory Authority Act 12 of 2003 as amended by The Electronic and Postal Communications Act, 2010 (amending sections 3, 15, 21, 26-27, 33-35, 41-42, 45, 47-48, 51 and the Schedule), Part II read with the definition of "regulated sector" in section 3.
1673. Id, section 13.

1674. Id, section 22.
1675. Id, section 23.
1676. Id, Part IV.
1677. Id, Part VII.
1678. Further details regarding the TBC are set out in the Public Corporation (The Tanzania Broadcasting Services) (Establishment) Order, 2002, G.N. No. 239 of 2002 (not located online), See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 37-39. The TBC is established under section 4 of the Public Corporation Act.
1679. The Electronic and Postal Communications Act [Chapter 306 R E. 2022]. Note that section 167A of this law repeals the Broadcasting Services Act 6 of 1993 and the Tanzania Communications Act 18 of 1993. See Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 30-ff.
1680. The Tanzania Telecommunications Corporation Act 12 of 2017.
1681. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 68-ff and 122. The Media Council of Tanzania recently produced an analysis of the Electronic and Postal Communications (Online Content) Regulations 2020 which is discussed below.
1682. "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 31.
1683. Media Services Act 12 of 2016, section 2.
1684. Id, section 59.
1685. "Tanzania: Victory for media freedom as ban on four newspapers lifted", Amnesty International, 11 February 2022.
1686. Media Services Act 12 of 2016, Part V.
1687. Id, Part VII.
1688. *Media Council of Tanzania & 2 Others v Attorney General of the United Republic of Tanzania*, East African Court of Justice, Case No 2 of 2017, 28 March 2019; see the case summary by Global Freedom of Expression here.
1689. "Tanzania ruling party newspaper Uhuru returns after two-week suspension", Commitee to Protect Journalists, 10 September 2021.
1690. See The Written Laws (Miscellaneous Amendments) Act, 2023, published as a bill in January 2023; the version of the bill that was actually passed by Parliament could not be located online. See also "What media law changes mean", *The Citizen*, 14 June 2023. According to one source: "After a tireless discussion with the state actors, the Coalition on the Right to Information (CoRI) proposed about 35 changes desired in the Media Services Act of 2016 to increase media freedoms and individual freedoms. However, the amendment Bill that the Attorney General of the Government submitted to the parliament in 2023 has proposed changes to eight sections, leaving critical sections such as the ones that criminalise defamation." Francis Nyonzo, "Tanzania's Media Services Act: A Manifestation of the Man With the Hammer Syndrome?", The Chanzo Initiative, 27 March 2023.
1691. The Films and Stage Plays Act 14 of 1976, as amended by the Local Government (District Authorities) Act 7 of 1982 (which amends section 9) and the Written Laws (Miscellaneous Amendments) (No 3) Act, 2019; see also "Corporate Commercial Law Update: The Tanzania Film Regulations of 2020; Implications to Businesses as far as Video Ads and Digital Content Regulation is Concerned in Tanzania", Breakthrough Attorneys, 21 March 2021.
1692. "Tanzania: Discard new law restricting human rights", Amnesty International. 28 June 2019.
1693. Francis Kamuzora, "Amendments to Copyright and Film Laws set the Scene for Change", Bowman's. 14 August 2019.
1694. Leonard Chimanda, "Law and Censorship of Artistic Works in Tanzania: The Case of BASATA", Sanaa: Journal of African Arts, Media and Cultures, 3(1), 2018, pages 13-26. The underlying law, which could not be located online, was amended by the Written Laws (Miscellaneous Amendments) (No. 5) Act 2019.
1695. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 97-101.
1696. *Mseto v Attorney General*, East African Court of Justice, Case No 7 of 2016, 21 June 2018; see the case summary by Global Freedom of Expression here.
1697. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 101-102. The Bill is available here.
1698. Id, pages 102-110,113.
1699. Id, pages 110-113.
1700. Article 18 is quoted in the table on the first page of this chapter.
1701. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, page 7.
1702. "The constitutional reform as a reason for optimism about the future of democracy in Tanzania", Robert Lansing Institute, 17 May 2023. According to this article, President Samia Suluhu Hassan appointed a task team in 2022 to review the political situation in the country, and this task team a revival of the constitution-writing process that had stalled in 2014-2015. A round of public consultations held by the task team on this issue was concluded in September 2022.
1703. The Constitution of Zanzibar, 1984 [Revised Edition 2006], Article 18.
1704. Id, Article 24.
1705. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, page 82.
1706. Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 49.

1707. "CPJ returns to Tanzania", *CPJ Insider: June 2022 edition*, 2 June 2022.
1708. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, "Executive Summary" and section 2A.
1709. Muthoki Mumo, "'A rush of relief': Tanzanian investigative newspaper allowed to publish after 5-year ban". Committee to Protect Journalists, 21 March 2022.
1710. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
1711. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A; "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023; "Tanzanian regulator suspends DarMpya online news outlet, citing expired license", Committee to Protect Journalists, 12 July 2022.
1712. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
1713. Id.
1714. "LEXOTA Country Analysis: Tanzania", last updated December 2022; "Tanzania ruling party newspaper Uhuru returns after two-week suspension", Committee to Protect Journalists, 10 September 2021.
1715. "LEXOTA Country Analysis: Tanzania", last updated December 2022; "Tanzanian authorities suspend Raia Mwema newspaper for 1 month", Committee to Protect Journalists, 15 September 2021.
1716. "Tanzania police arrest cartoonist, journalists on cybercrime and illegal assembly allegations", Committee to Protect Journalists, 7 October 2021.
1717. "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 10.
1718. Id, pages 10-11.
1719. Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 48.
1720. "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1721. Fumbuka Ng'wanakilala, "Optimism in the Media Industry after a Dark Period", *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page 48.
1722. "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1723. *The State of Press Freedom in Southern Africa 2020-2021*, Media Institute of Southern Africa, page Misa state of press freedom 2020-2020, page 9.
1724. "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1725. Id.
1726. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
1727. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 33.
1728. "Freedom of expression in Tanzania is on a downward spiral", Global Voices, 6 December 2022; "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 30.
1729. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 29.
1730. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 33.
1731. The Cybercrimes Act 14 of 2015, sections 28-29.
1732. Id, section 48.
1733. One commentator reads it in the broad sense as criminalising initial entering of a computer system, as well as conduct done after access is gained. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 14.
1734. *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.
1735. Lewis C Bande, "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities", *International Journal of Cyber Criminology*, Vol 12 Issue 1, Jan-June 2018, page 16.
1736. Id.
1737. Id, page 21.
1738. Id.
1739. "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, page 23.
1740. Id.
1741. "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1742. "Tanzania Media Trends Analysis Report, 2021", The Media Institute of Southern Africa, Tanzania Chapter (MISA-Tanzania), 2021, pages 23-24.
1743. "2022 Country Reports on Human Rights Practices: Tanzania", US State Department, section 2A.
1744. "Freedom of expression in Tanzania is on a downward spiral", Global Voices, 6 December 2022.

1745. The Cybercrimes Act 14 of 2015, sections 25-27. Section 2 defines "abetting" as "to encourage or assist someone to commit a crime or other offence".
1746. Id, section 31.
1747. Id, section 32.
1748. Id, section 33.
1749. Id, section 34-35.
1750. Id, section 38.
1751. Id, section 39. A "forensic tool" is defined in section 3 as "forensic tool" means "an investigative tool or device including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks which includes keystroke logging or collection of investigation information about a use of a computer or computer system".
1752. Id, section 45.
1753. Id, section 45(4).
1754. Id, section 41.
1755. Id, section 43.
1756. Id, section 42.
1757. Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 4 and pages 12-13, discussed below.
1758. The Electronic and Postal Communications Act [Chapter 306 R E. 2022], section 118(a)-(c).
1759. See "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1760. Electronic and Postal Communications (Online Content) Regulations, 2020.
1761. The Electronic and Postal Communications Act [Chapter 306 R E. 2022], sections 103-ff.
1762. Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022.
1763. Electronic and Postal Communications (Online Content) Regulations, 2020, as amended by the Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, regulation 2 read with the definition of "online content service providers" and "content" in regulation 3.
1764. Id, as amended by the Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, regulation 4 read with the definition of "online media services" in regulation 3.
1765. Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, pages 3 and 6.
1766. "The Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2021: Submission to the Tanzania Ministry of Information, Culture and Sports", Article 19, section B(ii) (footnote omitted).
1767. Id, section 16(1).
1768. Id, regulation 21.
1769. Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 11.
1770. Id.
1771. Id, page 3.
1772. "LEXOTA Country Analysis: Tanzania", last updated December 2022.
1773. Electronic and Postal Communications (Online Content) Regulations, 2020, regulation 11(3)-(4).
1774. Analysis of the Electronic and Postal Communications (Online Content) Regulations, 2020, Tanzania Media Council, 2020, page 4.
1775. Id, pages 12-13. See also "Tanzania: Electronic and Postal Communications (Online Content) Regulations 2018: Legal Analysis", Article 19, April 2018, at pages 21-15, making similar points about a similar take-down notification procedure in the previous 2018 regulations.
1776. Id, pages 5, 6-7. Note that regulation 9(d) was initially 9(e), prior to the 2022 amendments (Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022).
1777. Id. Note that regulation 9(c) was initially 9(d), prior to the 2022 amendments (Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022).
1778. See the discussion of this ruling in section 16.1 above.
1779. Media Services Act 12 of 2016, as amended by The Written Laws (Miscellaneous Amendments) Act, 2023
1780. The Penal Code [*Chapter 16*], Revised Edition 2022.
1781. Zanzibar Penal Act 6 of 2018.
1782. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 14: Tanzania", Konrad Adenauer Stiftung, 2021, pages 117, 120-122.
1783. Id, page 118.
1784. The Electronic and Postal Communications (SIM Card Registration) Regulations, 2020.
1785. The Data Protection Act 3 of 2021.
1786. Printed Publications Act, 1947, as amended [*Chapter 161*].
1787. Id, section 2.
1788. Id, section 5.
1789. Independent Broadcasting Authority Act 17 of 2002, as amended by the Independent Broadcasting Authority (Amendment) Act 26 of 2010 and the Independent Broadcasting Authority (Amendment) Act 18 of 2017
1790. Id, section 7.

1791. Id, sections 19-31, and sections 33-34.
1792. Id, section 29(1)(j)-(k), as amended in 2010.
1793. "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022; "Zambia's broadcasting regulator threatens to revoke Muvi TV's license", Committee to Protect Journalists, 16 June 2021.
1794. "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022; "Zambia cancels broadcaster Prime TV's license, police shutter office", Committee to Protect Journalists, 13 April 2020.
1795. "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022.
1796. Id.
1797. Zambia National Broadcasting Corporation Act 16 of 1987 [Chapter. 154], as amended by Zambia National Broadcasting Corporation (Amendment) Act 16 of 2002, Zambia National Broadcasting Corporation (Amendment) Act 16 of 2010, Zambia National Broadcasting Corporation (Amendment) Act 17 of 2017.
1798. Id, section 4.
1799. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 154; see the 2002, 2010 and 2017 amendment acts cited above.
1800. Information and Communication Technologies Act 15 of 2009 as amended by the Information and Communication Technologies (Amendment) Act 3 of 2010 (substituting sections 43, 47 and 48).
1801. Id, First Schedule.
1802. Id, section 6.
1803. Id, sections 9-10.
1804. Id, section 18(1)(h).
1805. Id, section 85.
1806. Abraham Kalito, "WhatsApp group admins will be required to register, warns ZICTA", *News Diggers!*, 31 May 2018; Nahashon Musungu, "Zambia: New Rule Compels Whatsapp Admins in Zambia to Register Groups or Be Arrested", *Nairobi News*, 2 June 2018.
1807. Jasper Mangwana, Twitter post, 15 November 2019. ZICTA issued a press release in 2018 entitled "Response to Correct the Allegation that ZICTA was Pushing for the Law to Start Registering WhatsApp Administrators". "ZICTA Annual Report 2018, page 46.
1808. Naomi Hunt, "IPI welcomes launch of Zambia Media Council", International Press Institute, 6 July 2012.
1809. *Report of the Committee on Media, Information and Communication Technologies for the Third Session of the Twelfth National Assembly*, June 2019, section 9.5.
1810. "Zambia media self–regulation; what the media must know!", MISA-Zambia, 20 March 2020; "State of the Media in Zambia". MISA-Zambia, July-September 2021.
1811. Some of the views on the Bill's pros and cons are canvassed in the *Report of the Committee on Media, Information and Communication Technologies for the Third Session of the Twelfth National Assembly*, June 2019. See also, for instance, "The Disquieting Questions about ZAMEC as Means for Media Self-Regulation in Zambia", *Lusaka Times,* 13 August 2022; Media Owners Reject Draft Bill", *Nation*, 16 June 2022; "State of the Media Regulation Roadmap", MISA-Zambia statement, 10 June 2022; Michael Kaumba, "Resubmit Zamec Bill To Ministry Of Justice, Media Stakeholders Told", ZNBC, 5 April 2022; "Ministry of Justice wants Self-Regulation Bill to include the regulation of visiting international journalists", *Lusaka Times,* 7 March 2022.
1812. "State of the Media Regulation Roadmap", MISA-Zambia, 10 June 2022.
1813. Richard Mulonga was interviewed via Zoom on 21 July 2023.
1814. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 131.
1815. *The People v Bright Mwape and Fred Mmembe* (1995) S.J., 17 March 1995; Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 187.
1816. "Freedom on the Net 2022: Zambia", Freedom House, section C3.
1817. Penal Code (Amendment) Act 23 of 2022, section 11; Marisa Lourenço and Mwai Daka, "You Have The Right to Insult a President: Repealing Zambia's Penal Code Section 69", Oxford Human Rights Hub, 26 January 2023.
1818. "Repeal Of Section 69 Of The Penal Code Is A Job Half Done For President Hichilema….the Police still has power to arrest and charge any person with criminal defamation of the President", *Zambian Observer*, 24 December 2022.
1819. *Attorney General v Clarke*, 2008 ZR 38, 24 January 2008; see the case analysis by Global Freedom of Expression here.
1820. *Chipenzi v The People*, HPR/03/2014, 4 December 2014; see the case analysis by Global Freedom of Expression here.
1821. "LEXOTA Country Analysis: Zambia", last updated July 2022.
1822. *The People v Kasonkomona*, HPA/53/2014, 15 May 2015; see the case analysis by Global Freedom of Expression here.
1823. Chapter One Foundation v Zambian Information and Communications Technology Authority, 2021/HP/0955, 21 March 2021; see the case analysis by Global Freedom of Expression here.
1824. Kelsey Carolan, "Zambian Supreme Court rules liquidation of The Post was illegal", International Press Institute, 3 March 2022.
1825. "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
1826. "Zambian police briefly detain 2 Millennium TV journalists covering protest", Committee to Protect Journalists, 14 March 2023.

1827. "Muvi TV journalists arrested, fined after filming Zambian police raid on politician's home", Committee to Protect Journalists, 18 November 2022.
1828. "Zambian journalist Eric Chiyuka charged with assault after covering land altercation", Committee to Protect Journalists, 6 April 2022.
1829. "Police investigate journalist Petty Chanda over leaked audio of government officials", Committee to Protect Journalists, 3 February 2022.
1830. "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
1831. "Zambian columnist Sishuwa Sishuwa could face sedition charge for opinion piece on election", Committee to Protect Journalists, 12 May 2021; "CPJ, Paradigm Initiative urge Zambian President Hakainde Hichilema to institute press freedom reforms", Committee to Protect Journalists, 17 November 2022.
1832. "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A. Section 69 was repealed by the Penal Code (Amendment) Act 23 of 2022, section 11.
1833. "Zambian officials threaten journalist Wellington Chanda over reporting", Committee to Protect Journalists, 30 September 2022.
1834. "2022 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
1835. Id.
1836. "Ruling party supporters raid Zambia's Mpika FM Radio, halt show featuring opposition", Committee to Protect Journalists, 5 January 2022.
1837. The Cyber Security and Cyber Crimes Act, 2021. This Act replaces The Computer Misuse and Crimes Act 13 of 2004, which was repealed by section 114 of the Electronic Communications and Transactions Act 21 of 2009.
1838. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 30; "2023 World Press Freedom: Zambia", Reporters Without Borders.
1839. "2021 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A.
1840. "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
1841. The Cyber Security and Cyber Crimes Act, 2021, section 4 and definition of "authority" in section 2.
1842. Id, section 6.
1843. Id, section 7.
1844. Id, section 8.
1845. The Electronic Communications and Transactions Act 4 of 2021, section 2
1846. Public Interest Disclosure (Protection of Whistleblowers) Act 4 of 2010.
1847. Vaughan O'Grady, "Will Zambia review its cyber security law?", Developing Telecoms, 17 May 2022 (quoting Richard Mulonga).
1848. "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
1849. Id.
1850. Id.
1851. The Cyber Security and Cyber Crimes Act, 2021, section 75; Criminal Procedure Code [*Chapter 88*], section 118.
1852. The Cyber Security and Cyber Crimes Act, 2021, sections 9 and 11.
1853. Id, section 15.
1854. Id. section 10.
1855. Id, section 27.
1856. Id, section 28.
1857. "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
1858. The Cyber Security and Cyber Crimes Act, 2021, section 29.
1859. Id, section 30.
1860. Id, sections 38 and 40.
1861. Id, section 39.
1862. Freedom on the Net 2022: Zambia", Freedom House, section C4.
1863. "Implications of Zambia's Cyber Security and Cyber Crimes Act 2021 on Digital Rights", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), May 2021.
1864. "Zambia's newly enacted cybercrime law challenged in court", MISA-Zimbabwe, 4 April 2021.
1865. "Deluge of Digital Repression Threatens African Security", Nathaniel Allen and Catherine Lena Kelly African Center for Strategic Studies, 4 January 2022.
1866. "Call for Comments on the Review of the Cyber Security and Cyber Crimes Act No. 2 of 2021", Ministry of Technology and Science, September 2022. The period between this call for input and the deadline for submission appears to have been less than one month.
1867. Chapter One Foundation, Bloggers of Zambia, Gears Initiative, People's Action for Accountability and Good Governance in Zambia and the Alliance for Community Action.
1868. "Zambia's newly enacted cybercrime law challenged in court", MISA-Zimbabwe, 4 April 2021; "New Cyber law goes to Court", *Lusaka Times*, 2 April 2021.
1869. "Joint CSO Press Statement dated 1st April 2021 on the Cyber Security and Cyber Crimes Act No 2 of 2021", quoted in "New Cyber law goes to Court", *Lusaka Times*, 2 April 2021.

1870. Susan Mwape, "Lungu law looms dangerously over Zambian digital rights", Association for Progressive Communications. 24 October 2022.
1871. Vaughan O'Grady, "Will Zambia review its cyber security law?", Developing Telecoms, 17 May 2022
1872. "Call for Comments on the Review of the Cyber Security and Cyber Crimes Act No. 2 of 2021", Ministry of Technology and Science, September 2022. The period between this call for input and the deadline for submission appears to have been less than one month.
1873. Penal Code, 1930 [Chapter 87]. This version, as accessed on 29 June 2023, presents the law as it stood on 31 August 2000.
1874. "What Prompted the Review of the Penal Code Act and the Criminal Procedure Code Act?", Zambia Law Development Commission, undated; "Call for Written Submissions: Review of the Penal Code Act, Chapter 87 of the Laws of Zambia, and the Criminal Procedure Code Act, Chapter 88 of the Laws of Zambia", Zambia Law Development Commissionm, undated (submission deadline: 20 February 2021).
1875. Penal Code (Amendment) Act 13 of 2022.
1876. Not located online.
1877. Penal Code (Amendment) Act 23 of 2022.
1878. Id, sections 11-12.
1879. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 15: Zambia", Konrad Adenauer Stiftung, 2021, page 170.
1880. "Submission by the Southern Africa Litigation Centre on the Review of the Penal Code and Criminal Procedure Code", 20 February 2021.
1881. Id.
1882. Mandy Rossouw, "Zambian president challenged over violation of freedom of speech", *Mail & Guardian*, 1 June 2010.
1883. Penal Code, 1930 [Chapter 87], Chapter XVIII, sections 191-198.
1884. "Submission by the Southern Africa Litigation Centre on the Review of the Penal Code and Criminal Procedure Code", 20 February 2021.
1885. Chipenzi v The People, HPR/03/2014, 4 December 2014; see the case analysis by Global Freedom of Expression here. The Court held as follows: "In conclusion, I find and hold that Section 67 does not fit under Article 20 (3) of the Constitution. It goes beyond what is permissible under that clause. I, therefore, find that Section 67 does not pass the test of being 'reasonably justifiable in a democratic society.' It contravenes Article 20 of the Constitution and is null and void, and therefore invalid for unconstitutionality. It follows also that the invalidity and the constitutional guarantee of freedom of expression preclude the prosecution of persons and the criminalization of alleged false statements under Section 67."
1886. Penal Code (Amendment) Act 23 of 2022, section 11.
1887. Prisons Act 56 of 1965, subsections 79(3) and (4).
1888. State Security Act, 1969 [*Chapter 111*], section 3.
1889. "ARTICLE 19's Submission to the UN Universal Periodic Review of The Republic of Zambia, 14th Session of the Working Group of the Human Rights Council, October-November 2012", paragraph 4.
1890. The Anti-Terrorism And Non-Proliferation Act 6 of 2018, section 26.
1891. Article 19 expressed concern over a similar provision in a previous law. "ARTICLE 19's Submission to the UN Universal Periodic Review of The Republic of Zambia, 14th Session of the Working Group of the Human Rights Council, October-November 2012", paragraph 4.
1892. Defamation Act 46 of 1953, sections 7, 9, 14 and 18 in particular. For an example of the limitations of the defence of fair comment see *Post Newspaper Ltd v Mulenga*, Supreme Court for Zambia, Appeal 22/2014, 13 May 2020.
1893. "2021 Country Reports on Human Rights Practices: Zambia", US State Department, section 2A, citing a report by the University of Toronto Citizen Lab entitled *Running in Circles:Uncovering the Clients of Cyberespionage Firm Circles*, released in December 2020
1894. "Mandatory SIM Card Live Facial Capture Directive", ZICTA, 6 January 2023; ZICTA webpage, "Sim registration (FAQ)", undated (accessed 4 August 2023); Lucky Phiri, "ZICTA to Deregister Half a Million SIM Cards", ZNBC, 8 February 2022.
1895. ZICTA webpage, "Sim registration (FAQ)", undated (accessed 4 August 2023)
1896. Electronic Communications and Transactions Act 4 of 2021, sections 81-82.
1897. Madanhire & Another v AG (CCZ 2/14 Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.
1898. Data Protection Act, 2021 [Chapter 11:22] originally, now part of the Cyber and Data Protection Act, 2021 [Chapter 12:07].
1899. Zimbabwe's 2013 Constitution, as amended through 2017, section 62.
1900. Freedom of Information Act, 2020 [Chapter 10:33], which replaced the Access to Information and Protection of Privacy Act of
2003. See also Freedom of Information (General) Regulations, 2021 [Statutory Instrument 229 of 2021, CAP. 10:33].
1901. Scanlen & Holderness v Zimbabwe, Case No. 297/2005, decided 3 April 2009; the case is analysed by Global Freedom of Expression here.
1902. Section 41 of the Freedom of Information Act preserved regulations made under the repealed law the extent that they could have been made under the appropriate provisions of the new law – but the Freedom of Information Act makes no provision for accrediting journalists or registering media services and news agencies. "AIPPA Resurrected : New Media Accreditation & Registration Fees Gazetted", Commissions Watch: Zimbabwe Media Commission. 1 February 2021; "Zimbabwe: 2022 Media Accreditation Fees Gazetted", *The Herald*, 2 April 2022

1903. Zimbabwe's 2013 Constitution, as amended through 2017, section 248.
1904. Id, section 249.
1905. Zimbabwe Media Commission Act, 2020 [*Chapter 10:35*], section 4.
1906. Id, section 8.
1907. Id, sections 12 and 15.
1908. Broadcasting Services Act, 2001 [*Chapter 12:06*], section 4.
1909. Id, section 4B.
1910. Id, Part III.
1911. Id, section 24.
1912. Id, section 39.
1913. Id, Fifth Schedule (section 11(1)(b)), Standard Conditions of Licences, item 7. This provision is contained in a section on political matters and medicines. but it is worded generally.
1914. Id, sections 11(1) and 16(1)(b).
1915. Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 3*, "Chapter 16: Zimbabwe", Konrad Adenauer Stiftung, 2021, pages 229-ff.
1916. Postal and Telecommunications Act, 2000 [*Chapter 12:05*].
1917. Id, section 5.
1918. Id, section 25.
1919. Id, section 26.
1920. "Freedom on the Net 2022: Zimbabwe", Freedom House, section A5.
1921. Postal and Telecommunications Act, 2000 [*Chapter 12:05*] section 84.
1922. Id, section 88.
1923. Zimbabwe's 2013 Constitution, as amended through 2017, sections 61 and 86 (quoted in the table at the beginning of this chapter).
1924. Madanhire & Another v AG (Judgment No CCZ 2/14, Const. Application No CCZ 78/12) [2014] ZWCC 2 (12 June 2014); see the summary of case by Global Freedom of Expression here.
1925. MISA-Zimbabwe v Minister of Justice (Const. Application No CCZ 7/15) (order available here); see the summary of the case by Global Freedom of Expression here and the summary by Southern Africa Litigation Centre here.
1926. Chavunfuka v Minister of Home Affairs 2000 JOL 6540 (ZS); see the summary of the case by Global Freedom of Expression here.
1927. Chimakure v Attorney-General of Zimbabwe (Judgment No. CCZ 6/201411, Const. Application No. CCZ 247/09), 22 July 2014; see the analysis of the case by Global Freedom of Expression here.
1928. Zimbabwe Lawyers for Human Rights v. Minister of State, National Security**,** HC 261/19, 21 January 2021. See Veritas, "Court Watch: Internet Shutdown Case – High Court's Ruling", as published in The Zimbabwean, 1 February 2019; "High Court sets aside internet shut down directives", MISA-Zimbabwe. 21 January 2019; "Freedom on the Net 2022: Zimbabwe", Freedom House, section B3; and case analysis by Global Freedom of Expression here.
1929. Id, section 61(2).
1930. "2023 World Press Freedom: Zimbabwe", Reporters Without Borders, "Legal Framework".
1931. "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
1932. "2023 World Press Freedom: Zimbabwe", Reporters Without Borders. "Safety".
1933. "Freedom on the Net 2022: Zimbabwe", Freedom House, "Overview".
1934. Amnesty International Report 2022/23, "Zimbabwe 2022"; "Zimbabwean journalist Hopewell Chin'ono denied bail", Reporters Without Borders, 12 November 2020.
1935. Freedom on the Net 2022: Zimbabwe", Freedom House, section C3; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.
1936. "LEXOTA Country Analysis: Zimbabwe", last updated May 2023; "Journalists charged with publishing false data messages", African Freedom of Expression Exchange, 6 August 2022.
1937. "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
1938. Freedom on the Net 2022: Zimbabwe", Freedom House, section C3.
1939. "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
1940. Id. Chin'ono has been repeatedly arrested under various laws for his online reporting activities. for instance, in July 2020, he was charged with **incitement to violence** in connection with photos and videos anti-government protests posted on Twitter, with some speculating that his arrest could have been a consequence of series of Facebook posts alleging that the president's son was involved in corrupt business dealings related to government contracts for medical supplies. Chin'ono was released on bail in September 2020, but banned from using social media for his activism as part of his bail conditions. In November 2020, Chin'ono was arrested for violating his bail conditions with a Twitter post about the initial denial of bail in his case. He was granted bail again in November 2020, on the condition that he would not anything on Twitter that would "obstruct justice."
1941. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 8.
1942. Malvern Mkudu, "Policy Brief: Zimbabwe's Cyber Crime and Cyber Security Bill 2017", 2018.
1943. Id, section B8, citing "Zimbabweans unfazed by cyber attacks", *The Herald*, 28 August 2020.
1944. "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4; Otto Saki and Nompilo Simanje, "Affordable connectivity and privacy violations plague Zimbabwe", Association for Progressive Communications, 8 November 2022.

1945. "Freedom on the Net 2022: Zimbabwe", Freedom House, section B4.
1946. This law replaced sections 163-166 of the Criminal Law (Codification and Reform) Act [Chapter 9:23] with new provisions, added new provisions to the Criminal Procedure and Evidence Act [Chapter 9:07] and amended the Interception of Communications Act [Chapter 11:20].
1947. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 32.
1948. "An Analysis of the Southern African Development Community Cybersecurity Legal Framework: A Human Rights Based Approach", American Bar Association, Rule of Law Initiative & American Bar Association, Center for Human Rights, November 2020, page 35; "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 33.
1949. Criminal Law (Codification and Reform) Act [*Chapter 9:23*] as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*]. section 35.
1950. Criminal Procedure and Evidence Act [*Chapter 9:07*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 36.
1951. Interception of Communications Act, 2007 [*Chapter 11:20*], as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*], section 37.
1952. "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)
1953. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.
1954. See section 13.2 above.
1955. "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023).
1956. See section 13.2 above.
1957. "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
1958. "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights", MISA-Zimbabwe/Konrad Adenauer Stiftung, [2021], page 34.
1959. "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
1960. Dr Allen Munoriyarwa was interviewed via Zoom on 25 July 2023.
1961. Criminal Law (Codification and Reform) Act [*Chapter 9:23*], section 34.
1962. "LEXOTA Country Analysis: Zimbabwe", last updated May 2023.
1963. "Cybersecurity and Data Protection Bill entrenches surveillance: MISA Zimbabwe analysis of the Cybersecurity and Data Protection Bill, 2019". MISA-Zimbabwe, undated (accessed 26 June 2023)
1964. Postal and Telecommunications Act, 2000 [*Chapter 12:05*], section 88. This provision, making it an offence to send by telephone any message that is grossly offensive, indecent, obscene or threatening, or to send a message known to be false by telephone "for the purpose of causing annoyance, inconvenience or needless anxiety to any other person". It is also an offence to make any telephone call without reasonable cause for the purpose of causing annoyance, inconvenience or needless anxiety.
1965. Criminal Law Codification and Reform Amendment Bill [H.B. 15, 2022], clause 2 which would insert a new section 22A into the Criminal Law (Codification and Reform) Act [*Chapter 9:23*]. See section 20 of this law for the penalty for treason. Section 20 refers to the death penalty, but section 48 of the 2013 Constitution states that the death penalty may be imposed only for murder committed in aggravating circumstances. The Act was published as a bill 23 December 2022. The Bill was passed by the lower house of the National Assembly on 31 May 2023 and by the Senate on 7 May 2023. It was signed by the President on 14 July 2023. "Zimbabwe: President's signing of 'Patriotic Bill' a brutal assault on civic space", Amnesty International, 15 July 2023.
1966. "'Patriotic Bill' is a threat to democracy and the future of Zimbabwe", Southern Africa Litigation Centre, 8 June 2023. See also, for example, Columbus Mavhunga, "Amnesty International to Zimbabwe Leader: Don't Sign 'Patriotic Act' Into Law", *VOA News*, 9 June 2023; Columbus Mavhunga, "Zimbabwe Opposition, Rights Groups Bemoan Passing of 'Patriotic Bill'", *VOA News*, 9 June 2023.
1967. Criminal Procedure and Evidence Act [*Chapter 9:07*].
1968. Id, section 379A, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1969. Id, section 379B, as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1970. Id, subsection 379C(3), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1971. Id, subsection 379C(9), as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1972. Id, subsection 397C(11) as inserted by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1973. "Freedom on the Net 2022: Zimbabwe", Freedom House, section B2 assume that these provisions impose penalties providers that fail to remove illegal content when ordered by a court or other public authority or *upon discovery by the service provider*.
1974. Interception of Communications Act, 2007 [*Chapter 11:20*], section 5, as amended by the Cyber and Data Protection Act, 2021 [*Chapter 12:07*].
1975. The offences are listed in the Third Schedule and in paragraphs 1-8 of the Ninth Schedule to the Criminal Procedure and Evidence Act [*Chapter 9:07*].
1976. Interception of Communications Act, 2007 [*Chapter 11:20*], section 6.

1977. Id, section 11.
1978. Postal and Telecommunications (Subscriber Registration) Regulations, 2013 (Statutory Instrument 142 of 2013), replaced by Postal and Telecommunications (Subscriber Registration) Regulations, 2014 (Statutory Instrument 95 of 2014).
1979. Freedom on the Net 2022: Zimbabwe", Freedom House, section C6.
1980. "Zimbabwe: New SIM registration database law represses twin rights to privacy and expression", Association for Progressive Communications, 3 October 2012; "Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.
1981. Freedom on the Net 2022: Zimbabwe", Freedom House, section C4.
1982. "Econet judgement guarantees privacy", *The Standard*, 13 September 2020.
1983. "Zimbabwe holds harmonized elections (presidential, parliamentary and local government elections) every five years." "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political Participation".
1984. Electoral Act [*Chapter 2:13*].
1985. "Zimbabwe Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Executive Summary".
1986. Id, "Political Participation".
1987. Id, "Executive Summary"
1988. Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
1989. Id.
1990. Electoral Act [*Chapter 2:13*], as amended through 2018, section 160G.
1991. Id, section 160H.
1992. Id, section 160I.
1993. Id, section 160J.
1994. Broadcasting Services Act, 2001 [*Chapter 12:06*], sections 2-3 read with the definitions in section 1.
1995. Electoral Act [*Chapter 2:13*], as amended through 2018, section 147.
1996. Id, section 160K. Penalties can be provided n statutory instruments issued by the Commission in terms of the Act. See section 192.
1997. "Zimbabwe's uneven electoral field: Data protection laws used to deny digital voter roll inspection", Advox, 13 June 2023; "ZEC wins voters' roll case… Releasing electronic format compromises security, court rules", *The Herald*, 8 March 2023.
1998. Wallace Mawire, "MISA-Zimbabwe pleased by POTRAZ bid to investigate violations of the Cyber and Data Protection Act", April 2023.
1999. "ZEC denies journalists access to voter registration stats", *The Zimbabwean*, 12 March 2023.