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[1]
DATA PROTECTION: South Africa has a data protection law.[2]
ACCESS TO INFORMATION: South Africa has access to information law.[3]

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.[4]

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.[5]

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.[6]

[1] 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)

[2] 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.

[3] 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.

[4] Imprint Act 43 of 1993, as amended by the Imprint Amendment Act 18 of 1994.

[5] Films and Publications Act 65 of 1996, original version.

[6] 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.[7]

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,[8] and by the Cybercrimes Act, 2015 which repealed one provision.[9] 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.[10] The Council appoints the Films and Publications Board which in turn appoints classification committees to deal with individual classifications.[11] 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.[12] There is also an Appeal Tribunal appointed by the Minister after consultation with Cabinet.[13] 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.[14]

[7] *Print Media South Africa v Minister of Home Affairs* 2012 (6) SA 443 (CC).
[8] Films and Publications Amendment Act 11 of 2019.
[9] 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.
[10] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 4, 6.
[11] Id, sections 9A-10.
[12] Id, sections 6A- 6B.
[13] Id, section 5.
[14] 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.[15]

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.[16] 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.[17] It also has the power to conduct enquiries into matters related to its functions.[18] 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.[19]

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.[20]

The **Electronic Communications Act 36 of 2005** provides specific powers and functions for ICASA concerning the electronic communications and broadcasting sectors.[21] It provides for the licencing of electronic communications services, electronic communications network services and broadcasting services.[22] 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.[23] 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.[24] The only content provisions in the Act relate to election periods and are discussed in section 14.5 of this chapter.

The **South African Broadcasting Corporation (SABC)** is generally considered to be a

[15] South African 1996 Constitution, as amended through 2012, Article 192.
[16] Independent Communications Authority of South Africa Act 13 of 2000 (current version).
[17] "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.
[18] Independent Communications Authority of South Africa Act 13 of 2000 (current version), section 4B.
[19] Id, sections 5 and 8.
[20] Broadcasting Act 4 of 1999 (current version). section 38.
[21] Electronic Communications Act 36 of 2005 (current version).
[22] Id, section 5
[23] Id, section 54 read with Independent Communications Authority of South Africa Act 13 of 2000 (current version), sections 17A-17B
[24] Electronic Communications Act 36 of 2005 (current version), section 69.

public broadcaster with an independent board rather than a state broadcaster – although it is still vulnerable to political pressures.[25] 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.[26] 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.*[27]

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.[28]

There are several self-regulating industry bodies all of which issue industry codes of conduct that contain some provisions on content.[29]

- 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

[25] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 2*, "Chapter 13: South Africa", Konrad Adenauer Stiftung, 2021, page 285.
[26] Broadcasting Act 4 of 1999 (current version), section 13.
[27] 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).
[28] 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.
[29] 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.

Code of Ethics and Conduct for South African Print and Online Media.[30] 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.[31]

- 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**.[32] 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.[33]
- 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.[34]
- The **Internet Service Providers' Association (ISPA)** is the self-regulatory industry body for ISPs. It has a **Code of Conduct**,[35] a complaints procedure,[36] and directions for lodging a take-down notification in terms of the Electronic Communications and Transactions Act 25 of 2002.[37]
- 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).[38]

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. The Tribunal highlighted the fact that the statements aired could have "life-and-death consequences on society at large".

[30] Code of Ethics and Conduct for South African Print and Online Media, 2020.
[31] "Complaints Procedures", Press Council, effective January 2020.
[32] All three Codes are available here.
[33] "Criteria for a complaint", BCCSA, undated.
[34] DMMA Professional Code of Conduct, 2010.
[35] ISPA Code of Conduct, Version 3.1 (revised 5 June 2023).
[36] "Complaints process", ISPA, undated.
[37] "How to lodge a take down", ISPA, undated.
[38] WASPA Code of Conduct, Version 17.5 (revised 28 June 2023)

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.[39]

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**. [40]

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.[41]

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.[42] 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 public complaints through the existing mechanisms and the rulings of the Press Ombud, which indicates the good faith of the media industry itself.[43]

---

[39] *Media Monitoring Africa v. eNCA Channel 403*, Case No. 09/2020, 30 June 2021; see the case summary by Global Freedom of Expression here.

[40] 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.

[41] 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)

[42] Id, "Normative debates" (online unpaginated version).

[43] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 12.157, 12.160-12.162.

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.[44] 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.*[45]

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.[46]

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."[47]

[44] Id, paragraph C34.
[45] Id, paragraph 12.165.
[46] 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).
[47] 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.[48]

(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.[49]

(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".[50] 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 to guide the assessment of whether the limitation is reasonable and justifiable –

[48] 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).
[49] *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.
[50] South African 1996 Constitution, as amended through 2012, section 16(2)(c) (emphasis added).

- 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.[51]

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.[52]

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.[53] 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.[54] The Court held that this crime strikes an appropriate balance between the protection of freedom of expression and the value of human dignity.[55] 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".[56] 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".[57] The Court concluded that criminal defamation is an acceptable method for protecting people's reputations in a democratic society.[58]

A similar approach was recently followed by the High Court in Gauteng in the

[51] South African 1996 Constitution, as amended through 2012, section 36(1).
[52] *Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International* 2006 (1) SA 144 (CC); see paragraph 47.
[53] *Hoho v The State* [2008] ZASCA 98; 2009 (1) SACR 276 (SCA).
[54] Id, paragraph 2.
[55] Id at paragraphs 27-36.
[56] Id, paragraph 32.
[57] Id, paragraph 33.
[58] Id, paragraph 36-37.

Motsepe case decided in 2014.[59] 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.[60] 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".[61] 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.[62] 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,[63] 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. [64]

Prosecutions for criminal defamation are rare and convictions even rarer.[65] 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".[66] 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."[67]

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":

[59] Motsepe v S (A 816/2013) [2014] ZAGPPHC 1016; 2015 (2) SACR 125 (GP); 2015 (5) SA 126 (GP) (5 November 2014).
[60] Id, paragraph 3.
[61] Id, paragraph 40.
[62] Id, paragraph 46.
[63] Id, paragraphs 20-22.
[64] Id, paragraphs 49-50.
[65] "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.
[66] See also Koko v Tanton, Johannesburg High Court. Case no 2021/2212, 7 September 2021.
[67] 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.*[68]

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.[69]

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".[70]

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.[71]
- In the 2016 *Primedia* case, the Supreme Court of Appeal of South Africa struck down provisions in Parliament's rules and policies that prohibited live television

[68] Id, paragraph 94.
[69] Id, paragraph 96.
[70] Id, paragraph 100.
[71] *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.

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.[72]

- 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.[73]
- 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.[74]

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. […]*

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. […]*

[72] *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.
[73] 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.
[74] *M&G Media Ltd v Chipu NO* [2013] ZACC 32; 2013 (6) SA 367 (CC).

[…] 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.[75]

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,[76] 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. [77] More recent incidents of this nature were listed in the US State Department's 2022 Report,[78] and reported by the Committee to Protect Journalists.[79] Both online and physical harassment is disproportionately directed at women journalists.[80]

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. 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.[81]

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

[75] "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
[76] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraphs 10.50-10.56, 10.77-10.80.
[77] Id, paragraphs 10.57-10.63.
[78] "2022 Country Reports on Human Rights Practices: South Africa", US State Department, section 2A.
[79] "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.
[80] Chris Roper, "South Africa", Reuters Institute for the Study of Journalism, 14 June 2023.
[81] *South African National Editors' Forum (SANEF) v The Economic Freedom Fighters (EFF)* (90405/18) [2019] ZAEQC 6 (24 October 2019).

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".[82] 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".[83] 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.[84] 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.*[85]

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 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.[86]

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.**[87] An ex parte order refers to an order issued

[82] *Enquiry into Media Ethics and Credibility*, Independent Panel Report, updated April 2021("Satchwell Report"), paragraph 10.17.
[83] Id, paragraph 10.13.
[84] 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.
[85] See Jon Alsop, "Were the Gupta Leaks South Africa's Watergate?", *Daily Maverick*, 24 September 2018.
[86] *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.
[87] "South Africa judge strikes down gag order against investigative outlet amaBhungane", Committee to Protect Journalists, 3 July 2023.

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.[88] 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".[89] *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.[90] 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",[91] which required that an application prohibiting publication must be brought with notice to the journalist concerned.[92]

[88] *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.
[89] "South African court's gag on amaBhungane raises fears for investigative journalism, sources", Committee to Protect Journalists, 7 June 2023.
[90] *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.
[91] Id, paragraph 34.
[92] Id, paragraph 45.

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* [93]

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.[94]

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.[95]

[93] *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.
[94] *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.
[95] "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).

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.[96]

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).[97]

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.[98]

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).

[96] Murray Hunter was interviewed via Zoom on 13 July 2023.
[97] Cybercrimes Act 19 of 2020, section 1
[98] 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.

	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".[99] 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".[100]
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)) • 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.

[99] *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.
[100] 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.

	○ 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.[101] ○ 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) • 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). ○ 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). ○ 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.[102]

[101] 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.
[102] Id, page 69.

	○ 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. ○ It is been noted that unlawful activities such as website defacement would fall within the ambit of sections 5 and 6.[103]
Section 7: Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device	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 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

[103] Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).

	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.[104] 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'" [105].
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". [106] 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. [107]

[104] 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.
[105] Id, page 74.
[106] Sizwe Snail ka Mtuze and Melody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).
[107] Id.

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.[108]
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 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.[109] Depictions of sexual assault and violence against children, are also addressed in the **Films and Publications Act 65 of 1966**, along with "revenge porn"**.**[110]

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. [111]

Note that the Cybercrimes Act covers certain forms of **hate speech** in sections 14 and

[108] Id.

[109] 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.

[110] See the discussion of the Films and Publications Act 65 of 1996 below.

[111] Protection from Harassment Act 17 of 2011, as amended by the Domestic Violence Amendment Act 14 of 2021.

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. "**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. o 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). o "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." [112] o 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).

[112] Sizwe Snail ka Mtuze andMelody Musoni, "An overview of cybercrime law in South Africa", *Int Cybersecur Law Rev* (2023).

	• *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". o It is not clear why the offences relating to "intimate images" are in one law and those related to "pornography" are in another. o 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**.[113]

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 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, [114] 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.

[113] Cybercrimes Act 19 of 2020, section 17.
[114] 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.

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.[115] 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.[116] 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.[117]

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.[118] 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",[119] 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.[120] **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,[121] as in the case of other offences.[122]

[115] Cybercrimes Act 19 of 2020, section 20. *Ex parte* means that the application can be made without notice to the other party.
[116] Id, section 22(2).
[117] Id, section 22(1).
[118] Id, section 29.
[119] Id, section 30.
[120] Id, section 1, definition of "specifically designated police official".
[121] Id, section 32.
[122] Criminal Procedure Act 51 of 1977, section 25.

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).[123] 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.[124] 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**.[125]

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.[126]

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*.[127]

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.[128]

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.[129]

[123] Cybercrimes Act 19 of 2020, section 40.
[124] 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".
[125] Id, section 44.
[126] Id, sections 48, 52.
[127] Id, section 54.
[128] Id, section 56.
[129] 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.

- It establishes a register of **cryptography providers**.[130]
- 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.[131] Some believe that these wide-ranging powers are overbroad, creating the potential for infringements of the right to privacy.[132]

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.[133]

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 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". [134]

[130] Id, sections 29-ff.
[131] Id, sections 80-ff.
[132] Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.
[133] Electronic Communications and Transactions Act 25 of 2002 (current version), section 77.
[134] Jane Duncan, "Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa", Global Information Society Watch (GISWatch), 2011.

C) FILMS AND PUBLICATIONS ACT 65 OF 1966

The **Films and Publications Act, 1996**[135] has been expanded to apply to films,[136] games,[137] and publications (defined broadly to include "any content made available using the internet").[138] 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.

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".[139]

Commercial online distributors have certain duties relating to the classification of materials for commercial distribution. However, more broadly, any person can allege

[135] 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.

[136] "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

[137] "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.

[138] "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.

[139] Id, definition of "identifiable group characteristic" in section 1.

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.*[140]

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**.[141]

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.[142]

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.[143] There is a higher penalty where individuals in the photographs or films are identified or identifiable.[144] "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.[145]

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.

[140] John Paul Ongeso, "South Africa: Films and Publications Amendment Act comes into Operation", Bowmans, 3 March 2022.
[141] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G.
[142] Id, sections 18G and 24F.
[143] Id, sections 18F and 24E.
[144] Id, section 24E.
[145] Id, section 18F(4) and (5).

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.[146]

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.[147] 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.[148]

D) HATE SPEECH

An analysis of this complex issue is beyond the scope of the paper.[149] 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".[150] 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 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.[151] The reference in this law to hate speech that is "hurtful" was found to be unconstitutional by the Constitutional Court in 2021,

[146] Id, section 18E(3).
[147] Id, section 27A.
[148] 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)
[149] 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).
[150] South African 1996 Constitution, as amended through 2012, section 16(2).
[151] 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.

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.[152]

- 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".[153]

- 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.[154]

- Various **codes of conduct issued by industry self-regulatory bodies** also cover hate speech.

- 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.[155]

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

[152] *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).

[153] Films and Publications Act 65 of 1996, updated to 1 March 2022, sections 18H and 24G, definition of "identifiable group characteristic" in section 1.

[154] 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.

[155] 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.

contains procedures for the interception of communications by law enforcement officials.[156]

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.[157] It directs the relevant minister to establish Interception Centres for this purpose.[158]

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 prescribed manner.[159] Failure on the part of the service provider to collect the required information is an offence.[160] ICASA has reportedly proposed linking SIM cards to biometric data.[161]
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.

[156] 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.
[157] Id, Chapters 2-3.
[158] Id, Chapter 6.
[159] Id, Chapter 7.
[160] Id, section 51(3)(a).
[161] Ruan Jooste, "Rica SIM card registration laws in SA are ineffective in reducing crime", IOL Business Report, 30 August 2022.

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.[162]

In addition, the Court held that the **bulk surveillance** that was being undertaken in practice by the National Communication Centre was not authorised by the law and was therefore unlawful and invalid.[163]

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.[164]

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.[165]

---

[162] *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.

[163] Id, paragraphs 124-135

[164] 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

[165] The ISPA statistics can be found here.

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.[166]

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**.[167] Elections are governed by the **Electoral Act 73 of 1998**.[168] According to Freedom House: "The Independent Electoral Commission (IEC) is largely considered independent, and the electoral framework is considered fair."[169]

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

[166] See "Freedom in the World 2023: South Africa", Freedom House, sections A1-A2.
[167] Electoral Commission Act 51 of 1996.
[168] Electoral Act 73 of 1998.
[169] "Freedom in the World 2023: South Africa", Freedom House, section A3.

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.[170] 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 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.*[171]
>
> *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.*[172]

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.

[170] "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".
[171] "South Africa Country Report 2022", BTI (Bertelsmann Transformation Index), Bertelsmann Stiftung, "Political and Social Integration".
[172] Id, "Executive Summary".

- 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.[173]

There is an extensive range of potential penalties and remedies for violation of the Electoral Act.[174]

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 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.[175] 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.[176]

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.[177]

Parties and candidates are also required to publicly condemn any action that may undermine the free and fair conduct of elections.[178]

[173] Electoral Act 73 of 1998.
[174] Id, section 96(2).
[175] Electoral Code of Conduct, Electoral Act 73 of 1998, Schedule 2.
[176] Id, item 3.
[177] Id, item 4(1)(a).
[178] Id, item 4(1)(b).

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.[179]

No person may deface or unlawfully remove or destroy the billboards, placards, posters or any other election materials of a party or candidate.[180]

There is also a specific provision on the role of the media in elections.[181].

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.

An example of the difficulties of interpretation can be seen in the case of ***Democratic Alliance v African National Congress***.[182] 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."[183]

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

[179] Id, item 9(1)(a)-(c).
[180] Id, item 9(2)(d).
[181] Id, item 8.
[182] *Democratic Alliance v African National Congress* [2015] ZACC 1, 19 January 2015; see the case summary by Global Freedom of Expression here.
[183] 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).

fractious debate".[184] 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.[185] 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.[186] 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.[187] 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.[188] The differing opinions in this case illustrate the difficulty of applying the prohibitions on false statements.

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.[189]

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***

[184] 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:
[185] Id, paragraphs 139-140.
[186] Id paragraphs 144-147.
[187] Opinion of Van der Westhuizen J (Madlanga J concurring), paragraphs 170-ff.
[188] Opinion of Zondo J (Jafta J and Leeuw AJ concurring), starting at paragraph 1.
[189] 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.

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.[190]

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.

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.

[190] *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.

(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.