CHAPTER 6

DEMOCRATIC REPUBLIC OF CONGO (DRC)

CHAPTER 6: DEMOCRATIC REPUBLIC OF CONGO (DRC)

DRC KEY INDICATORS
2023 WORLD PRESS FREEDOM RANKING: **124th globally; 37th out of 48 African countries** "Media pluralism is a reality in the DRC but, in the eastern province of Nord-Kivu, the media have been badly affected by fighting between the army and M23 rebels. Against this backdrop, the national assembly passed a new media law in April 2023, just months ahead of general elections."
MALABO CONVENTION: NOT signatory or party but the Council of Ministers approved a draft bill authorising ratification on 6 December 2022[1]
BUDAPEST CONVENTION: NOT signatory or party
CONSTITUTIONAL PROTECTION FOR FREEDOM OF EXPRESSION: Democratic Republic of the Congo 2005 Constitution The 2005 Constitution was amended in 2011, but the amendments did not affect these provisions.[2] **ARTICLE 23** All persons have the right to freedom of expression. This right implies the freedom to express their opinions and convictions, in particular by speech, in print and through pictures, subject to respect for the law, public order and morality. **ARTICLE 24** All persons have the right to information. The freedom of the press, the freedom of information and broadcasting by radio and television, written press or any other means of communication are guaranteed, subject to respect for the law, public order and the rights of others. The law determines the conditions for the exercise of these liberties. The audiovisual and written media of the State are public services to which all political and social movements are guaranteed access in an equitable manner. The status of the State media is established by law which guarantees objectivity, impartiality and plurality of views in the processing and distribution of information.
KEY LAWS: • Loi n° 20/17 du 25 novembre 20 relative aux telecommunications et aux technologies de l'information et de la communication • (Law no. 20/17 on telecommunications and information and communication technologies, which includes a cybercrime chapter)

[1] "Democratic Republic of Congo: Council of Ministers authorises ratification of Malabo Convention", alt.advisory, 27 January 2023.
[2] Loi n° 11/002 of 20 janvier 2011, amending Articles 71, 110, 126, 149, 197, 198, 218 and 226.

• **L'ordonnance-loi n°23/009 du 13 mars 2023**: Press Freedom Law • (this law could not be located online as of mid-2023, but a copy is on file with the authors) • L'ordonnance-loi n°23/010 du 13 mars 2023: Digital Code • Code Pénal Congolais (selected provisions)
CRIMINAL DEFAMATION: Yes[3]
DATA PROTECTION: DRC has provisions on personal data protection in a number of laws, including the recently-enacted Digital Code.[4]
ACCESS TO INFORMATION: DRC has a draft access to information law that has not yet been passed by both houses of Parliament.[5]

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

6.1 CONTEXT

The key media regulatory body is the **High Council for Broadcasting and Communication** ("Conseil Supérieur de l'Audiovisuel et de la Communication"- **CSAC),** which is established by Article 212 of the Constitution and Organic Law no. 11/001.[6]

CSAC's main functions are:

- guaranteeing freedom of the press, information and mass communication
- overseeing adherence to a code of conduct in respect of information provision
- overseeing equitable access to state media by all political parties and associations
- developing a code of conduct
- mediating in media-related disputes
- promoting excellence in media production

DEMOCRATIC REPUBLIC OF THE CONGO 2005 CONSTITUTION

Article 212
A High Council for Broadcasting and Communication with legal personality is established.

It has the mission to guarantee and ensure the liberty and protection of the press as well as of all means of mass communication in respect of the laws.

It supervises the respect for good practice standards with regard to the information and the equitable access of political parties, associations and citizens to the official means of information and communication.

The composition, competences, organization and operation of the High Council for Broadcasting and Communication are determined by organic law.

[3] Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, Article 74.
[4] Hogan Lovells, "DRC Overview: Guidance Note", Data Guidance, September 2022; "Recent developments in African data protection laws - Outlook for 2023", Lexology, [2022]; Jean-François Henrotte, "Protection des données en RDC", Lexing, [2023]. Other relevant laws on this topic are Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies") and L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Law no. 23/010 of 13 March 2023, the "Digital Code").
[5] Proposed Law on Access to Information (Proposition de Loi Relative a l'Access a l'Information). This law was passed by the Senate (the upper chamber of Parliament) in 2015, but not ratified by the National Assembly. See "Democratic Republic of Congo", PPLAAF, 2021; "Democratic Republic of Congo: High Commissioner update", UN High Commissioner for Human Rights, 30 March 2023.
[6] Loi organique n° 11/001 du 10 janvier 2011 portant composition, attribution et fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication ("Organic Law No. 11/001 of January 10, 2011 on the composition, attribution and functioning of the High Council for Broadcasting and Communication"). Note that Article 160 of the 2005 Constitution requires that all Organic Laws must be submitted to the

- promoting a culture of peace, democracy, human rights and fundamental freedoms
- promoting a national culture through the media
- protecting children
- filing reports to parliament
- providing advisory opinions on draft laws to Parliament or government.[7]

CSAC is governed by a Board of 15 members. They are all formally invested by the President, but the law requires that they represent a variety of stakeholders and the members appointed by government bodies are in the minority.[8]

CSAC has jurisdiction over "all means of mass communication", defined in the 2011 law as including "radio and/or television stations and/or television channels as well as print and electronic media outlets whose purpose is the collection, processing and dissemination of information or ideas".[9] It deals with media-related complaints from members of the public.[10] It is empowered to impose sanctions against journalists and media outlets for operating illegally, and it has unlimited discretionary powers to suspend a radio or television broadcasting service for up to three months, to suspend or cancel a specific programme, or to suspend or cancel a television channel or radio station or a section of a press organ. It can also seize media-related documents and materials.[11] CSAC can also approach the public prosecutor to institute criminal action.[12] Its powers to impose sanctions can respond to a complaint or be taken on its own initiative.[13]

The 2011 law prohibits the glorification of crime as well as incitement to violence, depravity of morals, xenophobia, tribal, ethnic, racial or religious hatred or any other form of discrimination;[14] there is no specific sanction for violating this stricture, but this could presumably support a finding of a violation of journalistic ethics or be used as a justification for imposing discretionary sanctions.

A recent case illustrates the powers that CSAC can wield. In May 2022, CSAC suspended journalist Louis-France Kuzikesa Ntotila of CML13 TV for 72 days for having "organized a media service whose content conveyed hate speech as well as remarks tending to incite violence against a tribe and to personal attacks". CSAC also cut off the CML13 television signal for 45 days and ordered that it could resume operations only on the presentation of all administrative documents, the program schedule and the specifications. Two elected officials who appeared as guests on the journalist's

Constitutional Court for a ruling on their conformity with the Constitution before they are promulgated. Internal regulations of the CSAC must also be submitted to the Court for a ruling on their constitutionality before they are applied.

[7] Loi organique n° 11/001, Articles 8-10, as translated and summarised in Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 206 (hereinafter "Limpitlaw").

[8] Loi organique n° 11/001, Articles 24 and 26.

[9] Id, Article 4.

[10] Id, Article 57.

[11] Id, Articles 58-59; Limpitlaw, pages 206-207.

[12] Id, Articles 68 and 74.

[13] See id, Article 62.

[14] id, Article 6.

show "Free Debate" were also sanctioned by being deprived of access to media broadcasting in the DRC for 90 days.[15]

CSAC operates alongside the independent statutory **Regulatory Authority for Posts, Telecommunications and Information Technologies of Congo** (*"L'Autorité de Régulation de la Poste et des Télécommunications du Congo"*) (**ARPTIC**).[16] ARPTIC is responsible for processing licence applications and permits and overseeing adherence to the laws and regulations relating to telecommunications.[17] Licencing and other basic conditions for telecommunications service providers are set out in **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies**[18] - which also contains the provisions on cybercrime discussed below. It should be noted that this law gives the Minister power, acting on a proposal from ARPTIC, to suspend or withdraw licences issued under the law for failure to comply with legal obligations; one additional ground for withdrawal of a licence is "endangering state security".[19]

One analysis notes that, despite the existence of these two regulatory bodies (CSAC and ARPTIC), the real power over the media remains concentrated in the executive.[20]

The **Broadcast Press Freedom and Professional Practice Decree**[21] sets out a number of content requirements for broadcasters. For example, broadcasters will be held responsible for all content broadcasts. They must be impartial and objective when broadcasting political content, and it is forbidden to broadcast "political propaganda", which is not defined. Further broadcasting content restrictions are contained in **The Broadcasting Press Freedom and Professional Practice Implementing Measures,**[22] which prohibits the broadcast of any content that contradicts Congolese laws, disturbs public order or infringes on good morals as well as any films, images or documentaries of a pornographic nature. There is also a **Radio and Television and Compliance Commission**,[23] that is charged with ensuring broadcasters' compliance with all applicable legal rules and making recommendations on sanctions in the case of breaches. [24]

[15] Oscar Bisimwa, "Urgent : le CSAC suspend le journaliste Louis-France Kuzikesa et sa chaîne CML13 TV", *Congo Reformes*, 22 mai 2023.
[16] This body was first created by Loi n°014/2002 du 16 octobre 2002, which was later replaced by Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies"). A table comparing the key points in these two laws can be found on the ARPTIC website here.
[17] Limpitlaw, page 209. Note that Limpitlaw's analysis does not cover the modifications made by the 2017 Telecommunications Law. Note also that the "Press Freedom Law" referred to in Limpitlaw is the 1996 version and not the one enacted in 2023.
[18] Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication ("Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies").
[19] Id, Article 52.
[20] Limpitlaw, page 208: "The DRC has more than one regulatory authority for broadcasting and signal distribution. While regulators are established in terms of a number of different statutes, it is clear that real power in respect of broadcasting resides in the executive branch of government and, in particular, with the Ministry of Press and Information. Despite being a constitutionally mandated body, the [CSAC] operates alongside a Regulatory Authority [ARPTIC], which deals with technical matters, and is overshadowed by the very real powers exercised by the executive".
[21] Ministerial Decree 04/MIP/020/96, dated 26 November 1996.
[22] Ministerial Decree 04/MCP/011/2002, dated 20 August 2002.
[23] Ministerial Decree 04/MIP/006/97 dated 28 February 1997.
[24] Limpitlaw, pages 226-229.

Even the content of music and entertainment is regulated. The **National Song and Entertainment Censorship Commission**, which is a body appointed by the Minister of Justice, reviews content to ensure it does not disturb public order or good morals and does not contain racial or tribal slurs, insults, slanderous language, or pornographic content. These requirements have been applied at times as the basis for the arrest of artists whose work was critical of the government.[25]

*In 2023, DRC enacted two new laws that are central to the topics under discussion: a **Press Freedom Law**[26] and a **Digital Code**.*[27]

*The new **Press Freedom Law** sets out* procedures for the exercise of freedom of the press and freedom of information in respect of radio and television broadcasting, the written press and any other means of communication in the DRC, including the online press.[28] It applies to public and private, community and religious media.[29] It also governs professional journalists and media professionals.[30] This law repeals "all previous provisions" contrary to it.[31]

The previous 1996 Press Freedom Law was revised in 2023 "on the basis of the recommendations of a national media convention held in January 2022, which called for a more up-to-date and protective legal framework for journalism and the media".[32] According to a government spokesperson: "This law makes it possible to solve a large number of problems which disturb this sector on a daily basis, among others, the slippages and the non-compliance of certain media, especially the online news media which, with technological evolution, are advancing with remarkable speed." This spokesperson also expressed particular concern about community radio stations which were not previously governed by any law.[33]

The new law defines "**freedom of the press**" as the right to inform, to be informed, to have one's opinions and convictions and to communicate them without any hindrance, whatever the medium used, subject to compliance with the law, the public order, the rights of others and of good morals – thus generally following the constitutional articulations of this right.[34]

---

[25] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[26] **L'Ordonnance-Loi n°23/009 du 13 mars 2023** fixant les modalites d'exercice de la liberté de presse, la liberté d'information et d'emission par la radio et la télévision, la presse écrite ou tout autre moyen de communication en République Démocratique du Congo ("Ordinance-Law N°23/009 of March 13, 2023 fixing the procedures for the exercise of freedom of the press, freedom of information and emission by radio and television, the written press or any other means of communication in Democratic Republic of Congo") ("Press Freedom Law"). This law could not be located online as of mid-2023, but a copy is on file with the authors. It replaces Law no. 96/002 of 22 June 1996.
[27] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
[28] **L'Ordonnance-Loi n°23/009**, Articles 1 and 82.
[29] Id, Article 15.
[30] Id, Article 2.
[31] Id, Article 140.
[32] "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders, "Legal Framework".
[33] Prince Mayiro, "RDC - Ass. Nat: Porté par Muyaya, le projet de loi de ratification de l'ordonnance-loi sur la liberté de la presse et la liberté d'information adopté",*7sur7.cd*, 5 avril 2023: "*Cette loi permet de résoudre un nombre important de problèmes qui dérangent ce secteur au quotidien, entre autres, les dérapages et la non-conformité de certains médias, surtout les médias d'informations en ligne qui, avec l'évolution technologique, avancent avec une rapidité remarquable.*" See also "Ordonnance loi fixant modalités de l'exercice de la liberté de la presse en RDC, Assemblée nationale : Patrick Muyaya explose et passe!", *Publié par La Prospérité*, 5 avril 2023.
[34] Compare Articles 23 and 24 of the Democratic Republic of the Congo 2005 Constitution quoted on the first page of this chapter.

One positive element of the new law is that it gives journalists access to information of public interest that is not classified and does not involve state security or national defence. However, there are still weaknesses: the new press freedom law tightens the conditions for access to the profession of journalist and fails to explicitly abolish prison sentences for press offences – although it does at least add a "bad faith" element to the offences of publishing false information or allegations disturbing public order.[35] One online article describes it as "less repressive, but more restrictive" for journalists.[36]

The law defines a "**professional journalist**" as a person who graduated from a school of journalism recognized by the State and whose main, regular and remunerated activity consists in the collection, processing and dissemination of information, or a person holding a bachelor's degree or the equivalent who also has three years of professional practice in the collection, processing and dissemination of information within the editorial staff of a press company recognized by the State.[37] It also provides a broader definition of "**media professional**", which includes publishers, directors, editors, current affairs presenters, cartoonists, translator-editors, reporter-photographers, sound recording operators and others involved in media production.[38]

Media professionals must apply for a professional identity card and complete a probationary period of 12 to 24 months. At the end of the probationary period, the candidate must undertake to respect the code of ethics and professional conduct for journalists, by signing a written engagement with the body responsible for the self-regulation of the media profession. The training regime for media professionals and the other criteria for the granting, renewal and cancellation of the professional card, are set by the self-regulatory body of the profession.[39]

Foreign media professionals must be accredited by the minister in charge of communication and media, who sets the requirements, procedures, costs and duration of such accreditations.[40]

Different categories of press, including written press, broadcast media, religious media and online media, must submit applications to CSAC to operate, with specific requirements for information that must be provided in respect of each category of press. They are free to operate only after they have received a receipt, not from CSAC, but from the minister responsible for media and communications. The duration of the authorizations issued by the minister for the operation of the various categories of press enterprises cannot exceed a maximum of ten years.[41] In the case of written publications or broadcast media, the receipt must be provided within 30 days of the application, unless the application is incomplete; otherwise, the right to publish or broadcast is automatically acquired.[42] A similar rule applies to online press, with the

[35] Id; "DRC enacts press law and digital code that criminalize journalism", Committee to Protect Journalists, 23 May 2023.
[36] "La RDC se dote d'une nouvelle Loi sur la Presse, moins répressive, mais plus contraignante, à quelques mois des élections à hauts risques", statement by Journaliste en Danger (JED), *deskeco.*, 7 avril 2023.
[37] Id, Article 3 (item 11).
[38] Id (item 20).
[39] Id, Articles 8-12, 93
[40] Id, Article 94.
[41] Id, Article 59.
[42] Id, Article 6.

right to operate being automatically granted if there is no authority forthcoming after 90 days.[43]

Public radio and television stations are required to be "objective, impartial and pluralistic" and to broadcast programming based on the public's right to information, equal access, diversity of opinion and the values of democracy, tolerance, openness, dialogue and national cohesion.[44] **Community radio stations** must be administered and managed by bodies put in place by the local community or communities themselves, in compliance with the law on non-profit associations. They must be apolitical and they must promote peace, stability, cohesion, and the development of their respective communities but also of the whole nation.[45]

Any associative, community or religious media must have a Program Director who is a professional journalist.[46] (Associative media refers to a media outlet run by a non-profit association with a view to promoting its activities.[47]) The law also sets requirements for half of the content of such media, stipulating that they must fall within a range of categories devoted to the public good, such as the promotion of good governance or the promotion of traditional national cultural values.[48]

Online press organs must have a publication director and they must regularly employ at least two journalists. It must operate in a journalistic manner, by presenting regularly updated material and in respect of research, verification and formatting of its information. Its content must be of general public interest and must not be "likely to shock the Internet user by a representation of the human person undermining his dignity and decency or glorifying violence".[49] Online media must respect the law, public order, good morals and the rights of others.[50] This means that CSAC thus has the power to sanction online media for failing in these duties, either by withdrawing the notice of compliance or by temporarily banning their operation.[51]

Online press organs do not include personal websites and blogs published on a non-professional basis.[52]

On the **right of access to information**, media professionals have the right of access to all public and private sources of information "of public interest", and subject to the legal provisions in force, in particular on attacks on State security, national defence and professional secrecy, any holder of information has the obligation to provide media professionals with public interest information. Any unjustified retention of public interest information can be punished "in accordance with the law". **Media professionals are also explicitly protected against being required to divulge their sources of information**. Any person who delivers public information to a professional

[43] Id, Article 84.
[44] Id, Articles 64-66.
[45] Id, Articles 67-70.
[46] Id, Article 77.
[47] Id, Article 3 (item 14).
[48] Id, Article 80.
[49] Id, Articles 87- 88.
[50] Id, Article 92.
[51] "Les attributions du Conseil Supérieur de l'Audiovisuel et de la Communication, CSAC en sigle", Edmond Mbokolo Eilima, *LegaVox*, 11 mai 2023.
[52] **L'Ordonnance-Loi n°23/009**, Article 91.

journalist is also protected against prosecution if the information delivered falls within the competencies that the person has assumed.[53]

The Press Freedom Law also includes a **right of reply and rectification.** Any natural or legal person cited or implicated in a written or online press article or in a radio or television broadcast, either by name or indirectly, but in such a way that they can be identified, has the right to have a response or correction inserted in the columns of said publication or to access said program for the same purpose, free of charge. However, when charges concern persons taken individually, these rights apply only to the extent that the person's interests are called into question.[54] There are specific directions on timing, length, placement and presentation of the reply or correction.[55] The law stipulates that the publication of the right of reply or rectification constitutes compensation for the injured party; in the event of a refusal to publish the reply or rectification, the injured party has the right to approach the courts for compensation.[56]

The law also created a number of new **crimes** that can be applied to journalists, which are discussed below in section 6.4 of this chapter.

*The new **Digital Code** covers all digital activities and services, including* electronic commerce, electronic signatures, digital government services, the regulation of digital platforms, the protection of personal data, cybersecurity and cybercrime.[57] It creates a **Digital Regulatory Authority ("***l'Autorité de Régulation du Numérique***"-ARN)** that regulates digital activities and services,[58] in addition to several other bodies concerned with digital matters and cybersecurity. Its specifics on cybercrime are detailed in the cybercrime section of this chapter.

The state broadcast media, "**Radio Télévision Nationale Congolaise**" **(RTNC)**, is regulated by Ordinance 81/050 of 2 April 1981.[59] Its Board is appointed by the President, who also has the power to remove individual members during their terms of office.[60] The **Congolese Press Agency** ("Agence Ccongolaise Presse") **(ACP)**, which is the state newsgathering agency, is also regulated by law.[61]

Commenting for this study on the state's use of some of these laws for repressive purposes, Prof. Tresor Musole Maheshe, a law professor at the Catholic University of Bukavu, indicated that since its enactment, the **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** has been regularly deployed in a heavy-handed fashion to muzzle journalists and/or

[53] Id, Articles 95-97.
[54] Id, Article 104.
[55] Id, Articles 105-111.
[56] Id, Article 112.
[57] "The Democratic Republic of Congo takes a significant step in digital with the ratification of the Digital Code", *fatshimetrie*, 23 August 2023.
[58] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code"), Article 7
[59] L'Ordonnance n° 81/050 du 2 avril 1981 (not found online). See also Décret n°09/62 du 03 décembre 2009 fixant les statuts d'un établissement public dénommé Radio-Télévision Nationale Congolaise, en sigle « RTNC », which changed its name from "*L'Office Zaïrois de Radio diffusion et de television*" (OZRT) to "*Radio Télévision Nationale Congolaise"* (RTNC).
[60] Limpitlaw, page 216.
[61] It is currently regulated in terms of L'Ordonnance n° 81/052 du 2 avril 1981 (not found online).

media organizations.[62] He also pointed to the new ***Digital Code***, *despite it only being enacted in 2023, already having been used to censor some media outlets and journalists. Some of these examples are discussed in subsequent sections. He also expressed the opinion, based on anecdotal evidence, that the* ***Digital Code*** *has already created a "chilling effect" by contributing to journalists' self-censoring.*

6.2 CONSTITUTION

The DRC Constitution contains no general limitations clause. The rights to freedom of expression and freedom of information and the press are both made subject to respect for "the law, public order and morality".

In other words, these rights are subject to legislation. The Constitution articulates no limitations on the restrictions that can be imposed on these rights by legislation - such as requirements that such restrictions must be reasonable, proportional or necessary in an open and democratic society.

> The effect of this limitation formulation is the almost universal undermining of the very concept of constitutional supremacy. The protection given by a constitutional right is entirely subjugated to the content of legislation passed by parliament, and no special requirements in respect of such rights-limiting legislation are required.[63]

6.3 CASE STUDIES

This overview of the state of the media in DRC was published in 2021:

> *A number of laws limit the ability of the press to inform the public about matters of the day. All too often journalists are arrested and detained, and independent media houses are often raided and banned. In the case of broadcasters, many have had their broadcasting distribution signals suspended without notice. The DRC features regularly on international lists of poor media environments, and there is little doubt that the country is, sadly, not in line with international standards for democratic media regulation. Internet and social media shutdowns are frequent even though internet penetration is extremely low at approximately 6%.*[64]

[62] Tresor Musole Maheshe was interviewed via Zoom on 25 July 2023.
[63] Limpitlaw, page 187.
[64] Id, page 183 (footnotes omitted).

Reporters Without Borders makes the following observations in its 2023 World Press Freedom Index:

> *The Congolese media landscape is marked by the presence of politicians who own or launch media outlets intended to promote their influence and rise to power. The national radio and TV broadcaster is a state media outlet that lacks independence. It is very common for local authorities, militiamen, religious groups, and politicians to exert pressure on the journalists and media outlets present in their province. […]*
>
> *Congolese journalists and media outlets lead a very precarious existence. Employment contracts are rare and the practice of "coupage" – whereby journalists receive a cash payment for covering an event or reporting some information – is widespread. The funding that the state has to legally provide to media outlets has never been distributed in a transparent manner. Very few media outlets are viable and independent, and most are influenced by those who back them.*
>
> *Journalists are sometimes targeted on the basis of their ethnic or community affiliation, and they are exposed to reprisals in connection with their work, particularly in the east of the country, where there are many armed groups. The conflict in Nord-Kivu is off-limits for the media, which are caught between rebel violence and the army's response. Some radio stations or radio broadcasts were suspended in 2021 for "incitement to tribalism and violence". Many journalists routinely censor themselves. Corruption and certain mining contracts are among the subjects that are most likely to prompt self-censorship.*
> *The dangers to which journalists and media are exposed include arrest, intimidation, physical violence, media closures, media outlets getting ransacked, and murder. In Nord-Kivu, they have been threatened by a wave of harassment and reprisals since the start of 2023 despite a ceasefire. M23 rebels ordered some media outlets to change their editorial policies. Discouraging the armed forces via the media in wartime is punishable by death. The security forces have been implicated in many abuses but enjoy complete impunity.*[65]

A media rights watchdog in the DRC, Journalistes en Danger, reported in November 2022 that there had been 124 cases of **attacks against journalists and media organizations** that year alone, including one instance of a journalist being killed while two journalists were abducted. Another 37 journalists were arrested, 18 were physically assaulted and 17 media organizations or programmes were shut down or suspended.[66]

It has been reported that journalists are frequently subjected to **violence, harassment, intimidation and even murder** by the government armed forces due to their reporting. For instance, Radio Okapi alleged in 2022 that a FARDC officer had shot and killed journalist Chadrack Senghi in retaliation for his reporting on army officials' harassment of civilians and their failures in the struggle against ISIS-DRC. The FARDC officer in question was reportedly arrested and charged with "flagrancy". [67]

[65] "2023 World Press Freedom Index: Democratic Republic of Congo", Reporters Without Borders.
[66] "East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom", Amnesty International, 3 May 2023.
[67] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.

The Committee to Protect Journalists reports numerous 2023 incidents that appear to be aimed at the **intimidation** of individual journalists:

- In June 2023, three journalists – Jeef Ngoyi, Marie-Louise Malou Mbela, and Jiresse Nkelani – were **arrested and assaulted** by at least 12 soldiers from the Armed Forces of the DRC (FARDC). They had been covering a land dispute in Kinshasa. They were all released by the next day, after interventions by the United Nations mission to the DRC. None of them were charged with any crime. The Committee to Protect Journalists notes that "repeated arrests and attacks on Congolese journalists by security forces that are supposed to be protecting the public make for an alarming pattern that must be reversed."[68]

- In April 2023, Gustave Bakuka, a reporter with the privately owned broadcaster Radio Mushauri, was **arrested** by three members of the Congolese National Intelligence Agency (ANR). He was accused of "**spreading false rumours**" in an article he wrote and shared through a WhatsApp group discussing security issues in Kindu, the capital of the Maniema province.[69]

- In a separate incident in April 2023, Diègo Kayiba, a reporter with the privately owned broadcaster Kin Actu TV and news website Reportage.cd, was **summoned and detained** by a prosecutor in Kinshasa in connection to two tweets which alleged that the head of the General Inspectorate of Finance had not been transparent about his personal spending and that he had betrayed the President through his own presidential ambitions.[70]

- In a third incident, an elected municipal representative in the city of Tshikapa, sent an audio message to journalist Sylvain Kabongo, a reporter with the privately owned Netic-news.net, **threatening him with arrest** for publishing a "baseless article" on his relationship with the minister of finance. The elected official claims that the article **damaged his reputation**, and he told the Committee to Protect Journalists that he intends to "punish" Kabongo and force him not to publish similar reports.[71]

- Also in April 2023, journalist Mills Tshibangu, director of the privately owned online broadcaster Chat Television, was arrested by a group of about 12 police officers in response to a **criminal defamation** complaint filed by the Minister of Mines in respect of reporting on alleged corruption involving a lithium mine. Tshibangu was held in custody overnight.

- In March 2023, journalist John Ngongo Lomango, director of the Radiotélévision Evangélique Phare (RTEP) broadcaster, was arrested by ANR agents in Kindu. He was accused of **distributing false information** in a news broadcast where he reported that Angolan soldiers had arrived in Kindu to assist the Congolese military

[68] "Congolese soldiers arrest, beat 3 journalists covering land dispute", Committee to Protect Journalists, 30 June 2023.
[69] "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
[70] Id
[71] Id.

in implementing a cease-fire with the M23 rebel group He was released two days later, but authorities confiscated his phone with the intention of searching it.[72]

- Also in March 2023, the Minister of Defense filed a criminal complaint against journalist Stanis Bujekera Tshamala, accusing him of **publishing false rumours that caused public alarm** in a tweet According to Bujekera, who is a correspondent for the France-based Jeune Afrique news website, the Reuters news agency, and the Congolese online new outlet Actualité.cd, the tweet had simply quoted from the official minutes of a Cabinet meeting in which the Minister of Defence had expressed surprise about the military advance by M23 rebels in the eastern part of the country. After intervention by the Minister of Communication, the Minister of Defence dropped the complaint.[73]

- In January 2023, the minister of communication and media for Lomami province ordered *Radio Tokomi Wapi* to suspend its operations and close its office in the provincial capital of Kabinda. Police were stationed at the broadcaster's offices to enforce the closure. Provincial officials alleged that the radio station had **incited the local population to tribalism, revolt, and disobedience of provincial authorities**, as well as failing to comply with journalistic ethics, after a guest on a call-in programme criticised the province's governor. The owner and the director of the radio station insisted that it had not broadcast anything that constituted incitement and considered the suspension to be politically motivated.[74]

- Also in January 2023, two journalists – Sylvain Kiomba, editor-in-chief of the privately owned radio station *Shilo FM*, and Joseph Ebondo, a reporter at the same station – were detained on suspicion of **criminal defamation** after they alleged that the ANR operated illegal secret holding cells in Lubao. They were questioned and then released without being charged two days later.[75]

The US State Department's 2022 Report on Human Rights Practices reports that there have been numerous cases where individuals have been charged with contempt, defamation, spreading false rumours, and public insult for criticizing the actions of government officials:

- In late July and early August 2022, several opposition party members and supporters were arrested in Kinshasa on separate charges of **defamation**, **public** insult, and **spreading false rumours**.

- In August 2022, the former head of the President's political party Union for Democracy and Social Progress, Jean-Marc Kabund, was arrested on the charges of **contempt of the head of state**, **defamation**, and **spreading false rumours.** The charges related to statements he made during a press conference, calling President Tshisekedi "irresponsible" and "a public danger" and accusing

[72] "Congolese journalist John Ngongo Lomango arrested over conflict reporting", Committee to Protect Journalists, 28 March 2023; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
[73] "DRC defence minister files, withdraws false news complaint against reporter Stanis Bujekera", Committee to Protect Journalists, 14 March 2023.
[74] "DRC broadcaster Radio Tokomi Wapi suspended, police shutter station", Committee to Protect Journalists, 18 January 2023.
[75] "DRC authorities detain 2 journalists for 48 hours over reporting on alleged secret jails", Committee to Protect Journalists, 12 January 2023.

government officials of lying, manipulation, embezzlement of public funds, and corruption. Kabund remained in detention in November 2022, despite an August 2022 court order that he should be remanded to house arrest.

- At least five provincial and national politicians were **arrested** in North Kivu and Ituri for criticizing the state of siege in the two provinces.

- In November 2021, Luc Malembe, a spokesperson for the opposition party *Engagement for Citizenship and Development* (ECIDe), was arrested on charges of **spreading false rumours** after he criticized the state of siege in the eastern provinces in a social media post. He was acquitted after spending seven months in detention.[76]

In January 2022, freelance reporter Patrick Lola and Christian Bofaya, a reporter for the privately owned *E Radio*, were **arrested for allegedly disturbing public order** after they covered a public protest about a dispute concerning the election of three provincial deputies. They remained in detention until August 2022, when the Court of Cassation in Kinshasa granted bail. After the court decision, demonstrations broke out at Mbandaka Central Prison, where the journalists were held (along with the provincial deputies who had been arrested for organising the protests). Bofaya escaped from prison during the aftermath of this incident, but Lola remained in custody because he was unable to pay the 2 million Congolese francs set as bail. As of April 2023, Lola was still in custody.[77]

In February 2022, National Deputy Josue Mufula was arrested at the airport in Goma, on charges of **contempt of the army**, **flagrancy**, and **provocation and incitement to breaches of public authority** because he passed out leaflets criticizing the state of siege.[78]

In June 2022, President Tshisekedi granted presidential amnesty to Jacky Ndala, a member of the opposition party *Ensemble pour la Republique*, who was sentenced to two years in prison on charges of **incitement to civil disobedience** for allegedly encouraging *Ensemble* party members to protest a draft law that would bar citizens with one non-Congolese parent from holding presidential office.[79]

In August 2022, officials arrested Marie Masemi, a social media star on charges of **defamation** and **public insult** after she posted a video on social media criticizing the First Lady and alleging that she was not Congolese. She was released Masemi after three days in custody, and the charges were dropped. Masemi posted a video to social media apologizing for her comments, but some wondered if the apology had been coerced as a condition of her release.[80]

[76] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 1E. The report views these persons as political prisoners and detainees.
[77] "Patrick Lola Imprisoned", Committee to Protect Journalists, 10 January 2022; "DRC authorities detain 2 journalists, threaten another with arrest", Committee to Protect Journalists, 14 April 2023.
[78] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[79] Id, section 1E
[80] Id, section 2A.

In November 2022, Olivier Makambu of the community broadcaster *Radio Communautaire pour le Renouveau du Kwango (RCRK)* was detained after a Member of Parliament filed a **criminal defamation** complaint against him.[81]

In November 2021, the minister of communication and media in the Equateur province of DRC suspended *Radio Télévision Sarah (RTS)* for 60 days, accusing it of **insulting government authorities** and "**calling on the population to revolt,**" after it aired programmes critical of Equateur Governor Bobo Boloko Bolumbu. In January 2022, the Equateur government **extended the suspension indefinitely**. The media outlet filed a lawsuit against the Equateur government, and a local court of appeal in the provincial capital declared the closure to be illegal and ordered that the station must be permitted to reopen. The next day, when journalists arrived at the office, they found that all of the broadcasting equipment was missing. Armed police officers then arrived and blocked access to the broadcaster's office over the next several days. In 2022, a court in the provincial capital convicted *RTS* reporter Chilassy Bofumbo on charges of "**prejudicial accusations, contempt for authority, public insult, and inciting hatred and rebellion**" in connection with his coverage of a street protest against the governor. He was released after being held for seven months. In 2019, the director of RTS, Steve Mwanyo Iwewe, was sentenced to 12 months imprisonment on a charge of **insulting the governor**, tied to his coverage of a protest on the eve of elections. He was released after two months of incarceration.[82]

In March 2021, the Mayor of Kolwezi filed a complaint of **criminal defamation under Article 74 of the Penal Code** against Donat Kambola, the Coordinator of the *Initiative Bonne Gouvernance et Droits Humains* (IBGDH) ("Good Governance and Human Rights Initiative"). IBGDH is a member of the umbrella NGO body *La Synergie des Organizations de la Société Civile de Lualaba Œuvrant dans le secteur des Ressources Naturelles* (SOLORN) ("The Coalition of Civil Society Organizations in Lualaba working in the Natural Resources Sector"), and Kambola is the coordinator of that coalition. The charges appear to stem from a letter by SOLORN to the Provincial Government of Lualaba denouncing the poor state of the roads in some parts of Kolwezi and calling for an investigation into conflicts of interest and alleged irregularities in the sale of government land. SOLORN also filed a criminal complaint with the public prosecutor related to conflicts of interest in public office and embezzlement of public property.[83]

These are just a few of many more cases that could be cited. The US State Department reported in 2022 that provincial governments sometimes prevented journalists from filming or covering certain protests or pressured the media not to cover certain events – including those organized by opposition parties or local activists. [84]

Multiple sources indicated that many journalists exercise self-censorship due to concerns of harassment, intimidation, or arrest.

[81] Joel Simon, Carlos Lauría and Ona Flores,"Weaponizing the Law: Attacks on Media Freedom", Thompson Reuters Foundation and Tow Centre for Digital Journalism, April 2023, page 18.
[82] "Governor of DRC's Equateur province defies court order allowing Radio Télévision Sarah to reopen", Committee to Protect Journalists, 13 June 2023; "In DRC, provincial governor blocks radio station's bid to resume broadcasting", Reporters Without Borders, 20 June 2023.
[83] "DRC: Drop Defamation Charges Against Human Rights Defender", Amnesty International Public Statement, AFR 62/3924/2021, 30 March 2021.
[84] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.

A 2021 report states that the government limits access to the Internet in several ways:

- Total shutdowns
- Targeted shutdowns, where only particular sites are blocked.
- Throttled internet, where the speed of the internet is deliberately slowed so as to render it effectively unusable.[85]

This is authorised by Article 125 of **Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies**.[86]

Loi n° 20/17 du 25 novembre 20 relative aux telecommunications et aux technologies de l'information et de la communication

ARTICLE 125:
Sans préjudice des droits et libertés fondamentaux individuels ou collectifs garantis par la Constitution et des procédures y attachées, l'Etat peut, durant le temps qu'il détermine, soit pour des raisons de sécurité intérieure et/ou extérieure, de défense nationale ou d'ordre public, soit dans l'intérêt du service public de télécommunications, soit pour tout autre motif jugé nécessaire, suspendre, restreindre, filtrer, interdire ou fermer certains services et applications, en tout ou en partie, y compris l'usage des installations.

Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies

ARTICLE 125:
Without prejudice to the fundamental individual or collective rights and freedoms guaranteed by the Constitution and the procedures attached thereto, the State may, during the time it determines, either for reasons of internal and/or external security, national defence or public order, or in the interest of the public telecommunications service, or for any other reason deemed necessary, suspend, restrict, filter, prohibit or close certain services and applications, in whole or in part, including the use of installations.

This is an overview of internet shutdowns between 2015 and 2019:

[85] Limpitlaw, page 221.
[86] Such moves could also have been implemented by ARPTIC under Article 3(i) of Loi n° 014-2002 du 16 octobre 2002 portant création de l'Autorité de régularisation de la poste et des télécommunications which empowers it to protect the public interest. Limpitlaw, page 221. (Limpitlaw also mentions the Telecommunications Act 13-2002 of 16 October 2002 as possible authority, but this law was repealed by Article 202 of Law 20/17.)

The Democratic Republic of Congo has experienced many internet shutdowns over the past several years. These have ranged from complete country wide shutdowns to targeted regional shutdowns of social media platforms. […] The internet shutdowns are often accompanied by outages of SMS services, cuts to radio and television signals for independent broadcasters, and the implementation of roadblocks in population centres such as Kinshasa.

The first reported internet shutdown occurred in January 2015. This followed an earlier 25 day cut to SMS services in December of 2011. Again, on 19 December 2016, the government ordered the internet to be shut down on the day Joseph Kabila was set to step down as head of State. On 30 December 2017, the Democratic Republic of Congo's Telecommunications Minister, Emery Okundji, ordered the country's telecommunications providers to shutdown internet and SMS services across the country. There was another three-day internet blockage beginning 21 January 2018. Then on 25 February 2018 there was a ten-hour blockage. From 31 December 2018 to 6 January 2019, during the election count, internet users in the Democratic Republic of Congo were again shut off from the internet.[87]

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

DRC does not have a single dedicated cybercrime law. Instead, **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** contains chapters on cybersecurity, cryptology and cybercrime.[88] In addition, **Ordinance-Law no, 23/010 of 13 March 2023**, the Digital Code, contains provisions on cybersecurity, cryptology and cybercrime.[89] The Digital Code states that it repeals all previous provisions contrary to it,[90] but it generally appears to supplement **Law no. 20/17** rather than to supersede it.

A) CYBERCRIME PROVISIONS IN LAW NO. 20/17 ON TELECOMMUNICATIONS AND INFORMATION AND COMMUNICATION TECHNOLOGIES

Article 153 of Law no. 20/17 provides an overview of the acts that constitute cybercrime:

1. child pornography;
2. racism;
3. xenophobia
4. infringements, in particular those involving:

[87] "Navigating Litigation during Internet Shutdowns in Southern Africa", Southern Africa Litigation Centre, June 2019, page 9 (footnote omitted).
[88] Loi n° 20/17 du 25 novembre 2020 relative aux telecommunications et aux technologies de l'information et de la communication (Law No. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies). This law is administered by ARPTIC, under the supervision of the relevant minister. Id, Articles 12-13.
[89] L'Ordonnance-Loi n°23/010 du 13 mars 2023 portent Code du Numerique ("Digital Code")
[90] Id, Article 389.

a. the activities of providers of electronic communication services for the public;
b. electronic advertising,
c. direct marketing;

5. damage to property related to information and communication technologies
6. attacks by any means of public dissemination;
7. attacks on national defence;
8. breaches of the confidentiality of computer systems;
9. breaches of the integrity of computer systems;
10. damage to the availability of computer systems;
11. computer data breaches in general;
12. specific breaches of the law relating to personal data.

Specific offences in these categories are set out in another part of the same law,[91] as summarised in the tables below. Titles have been added to the tables for ease of reference, but there are no titles in the law itself. The French text of some of the technical offences is provided in footnotes, where the translation may have misinterpreted what is prohibited.

LAW NO. 20/17 - TECHNICAL OFFENCES	
Article 179: Violating secrecy of correspondence or manipulating personal data	Without prejudice to the payment of damages to the victim, it is an offence to violate the secrecy of correspondence or to manipulate personal data without prior authorization. The penalty is penal servitude for the individual who acted in this manner, and a fine for that individual's employer. o Note that Article 126 lifts the secrecy of correspondence – * At the request of the public prosecutor * With the authorization of the Courts and Tribunals within the framework of a judicial investigation of a crime; * By competent public authorities, for reasons of internal and/or external security of the State, national defence or public order.
Article 180: Intercepting private communications or correspondence	It is an offence to intercept, listen to, record or transcribe by means of any device a communication or private correspondence. The penalty is 1 to 3 years of primary penal servitude and/or a fine.[92]
Article 182: Disrupting the Hertzian emissions of an authorized service	It is an offence to disrupt the Hertzian emissions of an authorized service using, without right, a frequency or a radio installation. The punishment is primary penal servitude for one month to one year and/or a fine.[93]

[91] Loi n° 20/17, Article 154.
[92] "Est punie de un à trois ans de servitude pénale principale et/ou d'une amende de 1.000.000 à 10.000.000 de francs congolais, toute interception, écoute, enregistrement, transcription au moyen d'un quelconque dispositif pour divulgation d'une communication ou correspondance privée."
[93] "Est puni d'une peine de servitude pénale principale d'un mois à un an et/ou d'une amende de 50.000.000 à 100.000.000 de Francs congolais, toute personne qui perturbe, en utilisant, sans titre, une fréquence ou une installation radioélectrique, les émissions hertziennes d'un service autorisé."

Article 184: Interrupting electronic communications	It is an offence to intentionally interrupt electronic communications by any means. The penalty is penal servitude for 2 to 5 years and/or a fine.
Article 185: Unauthorized use of frequencies or numbers	It is an offence to use or transfer frequencies, numbers or blocks of numbers that have not been allocated. The penalty is a fine.
Article 186: Fraudulent access or remaining	It is an offence to fraudulently access, or remain in, all or part of an electronic communication system. The penalty is penal servitude of six months to three years and a fine, or one of these penalities only.[94] It is also an offence to obtain any advantage whatsoever, for oneself or others, by fraudulently accessing. or remaining in. all or part of an electronic communication system. The penalty is the same as above.[95] o The offences of fraudulent access and remaining, which are separated in some SADC countries, are combined into one here. Some say that both are forms of unauthorized access.[96] o There appears to be no defense of justified access for a purpose that is in the public interest, such as security testing or gaining information for use in whistleblowing.
Article 187: Fraudulent data interference	It is an offence to fraudulently introduce data into an electronic communication system that obstructs or distorts its operation. The penalty is primary penal servitude of one to five years and/or a fine.
Article 188: Computer-related forgery by changing data	It is an offence to damage, erase, deteriorate, alter or fraudulently modify the data in an electronic communication system. The penalty is the same as provided in the Penal Code for forgery in writing.
Article 189: Computer-related forgery by producing or manufacturing data & using unlawful data	It is an offence to produce or manufacture a set of digitized data by fraudulently entering, erasing or deleting data from an electronic communication system. The penalty is the same as provided in the Penal Code for forgery in writing. The same penalties apply to knowingly making use of the data obtained under the conditions provided for in Articles 185 to 187 of this law. o The prohibition on the use of data that was obtained in violation of Article 186 (Fraudulent access or remaining) could affect the ability of journalists to use whistleblower data or data in a cache such as Wikileaks.
Article 190:	It is an offence to process personal data (or to cause it to be processed) without the prior authorization required by Article 126. The penalty is

[94] "*Quiconque accède ou se maintient frauduleusement dans tout ou partie d'un système de communication électronique est puni d'une servitude pénale de six mois à trois ans et d'une amende 1.000.000 à 10.000.000 de francs congolais ou de l'une de ces peines seulement*".
[95] "*Est également puni des mêmes peines, celui qui se procure poir soi-même ou pour autrui, un avantage quelconque, en s'introduisant ou se maintenant frauduleusement dans tout ou partie d'un système de communication électronique.*"
[96] *Assessing Cybercrime Laws from a Human Rights Perspective*, Global Partners Digital, [2022], page 14.

Unauthorised processing of personal data	penal servitude for an unspecified time for the individual who committed the offence, and a fine for that individual's employer. o "Personal data" is defined in Article 4 (item 37) as "any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social or economic identity". o "Processing of personal data" is defined in Article 4 (item 95) as "any operation or set of operations carried out using automated or non-automated processes and applied to the data, such as the collection, processing, recording, organization, storage, adaptation, modification, extraction, saving, copying, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, as well as the blocking, encryption, erasure or destruction of personal data". o These definitions are based on the Malabo Convention. o The authorization referred to in Article 126 is authorization by Courts and Tribunals within the framework of a judicial investigation of a crime. o It is unusual in the region for illegal personal data processing to be classified as a cybercrime.
Article 191: Devices for unlawful use	It is an offence to produce, sell, import, hold, distribute, offer, assign or make available equipment, a computer program, a device or data designed or specially adapted to commit one or more of the offences provided for in Articles 186 to 189 of this law. It is also an offence to do the same acts with a password, an access code or similar computerized data allowing access to all or part of the electronic communication system. The penalty in either case is the same as for the underlying offence, or the most severely sanctioned underlying offence. o Similar provisions in many other SADC countries refer to devices *primarily* designed or adapted for illegal purposes, because of the existence of dual-use devices.
Article 196: Theft of information	The fraudulent embezzlement of information to the detriment of others through a system of electronic communication is a form of theft. The penalty is the same as provided in the Penal Code for theft.

With respect to the **penalties** for technical offences, all are punishable by a term of imprisonment or a fine, or both.

LAW NO. 20/17 – CONTENT-BASED OFFENCES	
Article 181: Obscene, racist or xenophobic material or false distress calls	It is an offence to transmit or put into circulation – • obscene, racist or xenophobic signals, images and messages; or • false or misleading distress calls by means of telecommunications or ICT. The penalty is primary penal servitude for 6 months to a year and/or a fine.

	○ There is no definition of the key terms "obscene", "racist" or "xenophobic", which opens the door to subjective enforcement and self-censorship.
Article 193: Child pornography	It is an offence to produce, record, offer, make available, distribute, transmit, import or export an image or representation containing child pornography through an electronic communication system. The penalty is primary penal servitude for five to ten years and/or a fine. ○ "Child pornography" is defined in Article 4 (item 76) as "any data of whatever nature or form visually depicting a minor engaging in sexually explicit conduct or realistic images depicting a minor engaging in sexually explicit conduct. ○ This offence overlaps with Article 174m of the Penal Code which contains a broader definition of "child pornography".[97]
Article 194: Ideas or theories of a racist or xenophobic nature	It is an offence to create, download, distribute or make available in any form whatsoever writings, messages, photos, drawings or any other representation of ideas or theories of a racist or xenophobic nature through an electronic communication system. The penalty is a primary penal servitude of five to ten years and/or a fine. ○ There is no definition of the "ideas or theories of a racist or xenophobic nature", which opens the door to subjective enforcement and self-censorship. ○ Similar provisions in other SADC countries do not criminalize the mere *download* of such material where it is not further disseminated. This could, for instance, hinder a journalistic investigation into racist or xenophobic groups. It is also unusual to prohibit the creation of such material where it is not publicly shared.
Article 194: Discriminatory threats	Any threat, by means of an electronic communication system, to commit an offence against a person because of his membership of a group which is characterized by race, descent or national or ethnic origin, or religion where this serves as a pretext for one of the other elements. The penalty is penal servitude of 5 to 10 years and a fine. ○ This is one of the few offences that imposes a mandatory prison sentence, without the option of a fine instead of imprisonment.
Article 197: Treason	It is treason through an electronic communications system to – • deliver to a foreign power or its agents, in whatever form or by any means whatsoever, any information, object, document, procedure, digitized data or computerized file that must be kept secret in the interest of the national defence; • secure any of these items for the purpose of delivering them to a foreign power or its agents; • destroys such items, or allows them to be destroyed, in order to favour a foreign country. The penalty is the same as provided in the Penal Code for treason.

[97] Code pénal congolais, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006. Article 174 applies to "any representation by any means whatsoever, of a child engaging in sexual activities explicit, real or simulated, or any representation of the sexual organs of a child, for primarily sexual purposes".

	○ This offence overlaps with Articles 184-185 of the Penal Code.[98] The penalty is death.
Article 198: Failure to safeguard information related to national defence	It is an offence for any guardian or custodian of any information, object, document, process, digitized data or computerized file which must be kept secret in the interest of national defence – without any intention of treason or espionage – to, through an electronic communication system, destroy, remove, reproduce, withdraw, transfer or reproduce the item, or allow it to be brought to the attention of an unqualified person or the public. The penalty is penal servitude for 5 to 10 years.

With respect to the **penalties** for content-based offences, only the offence of discriminatory threats makes no provision for a fine to be imposed as an alternative to imprisonment (instead of imposing the two kinds of penalties in conjunction). The logic behind treating this offence differently from the others on the list is unclear.

Across the board, it is an offence to **participate in an association or an agreement** established with a view to preparing for or committing a cybercrime. The penalty is the same as any other kind of criminal association.[99]

Law no. 20/17 imposes a range of duties on telecommunications and internet service providers.

SIM card registration: Telecommunications service providers are required by Article 92 to collect and store identifying information in respect of all their subscribers, and to keep "identification cards containing the minimum essential information". The specific conditions and procedures for identifying subscribers are set out in orders issued by the relevant minister.[100] The sale of SIM cards to unidentified users, the provision of access to unidentified users, or providing or allowing clandestine avenues for accessing telecommunications services are criminal offences.[101] According to Privacy International, the ministerial order on SIM card registration "requires telecom operators to respect the secrecy of information collected from their subscribers except for compelling reasons related to internal and external security or in the event of legal proceedings".[102]

Cybercafés: Article 58 requires that the intention to offer cybercafés or "hot spots" must be declared to ARPTIC, which will issue a certificate of approval and inform the relevant minister. The terms and conditions for granting approval are set by ministerial order.

Preservation of connection and traffic data: In terms of Article 143, network operators and service providers are required to retain connection and traffic data for 12 months and to install data traffic monitoring mechanisms on their networks. The stored data

[98] Code pénal congolais, Articles 184-185. The Penal Code provides separate offences for Congolese citizens (treason) and for foreigners (espionage). The cybercrime offence applies to "any person".
[99] Loi n° 20/17, Article 192.
[100] Id, Articles 92-95.
[101] Id, Articles 156-157 and 172-173.
[102] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 26. The ministerial order referenced in this source could not be located online.

must be accessible during legal investigations, under the conditions set by laws and regulations relevant to such investigations.

Prohibition on undermining State security: A provision unusual in the region is Article 176, which makes it an offence for any network operator or service provider to undermine the security of the State, or to facilitate this.

Filters: Under Article 139, network content providers are required to set up filters to deal with harmful attacks on the personal data and privacy of users. Article 140 requires operators that provide access to information systems to inform users of the need to install parental control devices and the existence of filtering devices, as well as offering at least one filtering tool.

Warnings about risks: Article 140 requires operators that provide access to information systems to warn users of the dangers of insecure information systems and the risks of security breaches and computer viruses. They must also provide information about tools to protect against viruses, spyware and misleading software, the activation of personal firewalls, intrusion detection systems and the activation of automatic updates. in terms of Article 141, they must also inform users that is it illegal to use the network to disseminate illegal content, and that it is illegal to design and distribute spyware or other tools that can be used for fraudulent behaviour.

Cryptology: Article 146 requires service providers to declare any intention to offer encryption services to ARPTIC, which will issue a certificate of approval and inform the relevant minister. The declaration by the service provider must include a description of the technical characteristics of the cryptology means, as well as the source code of the software used. Article 145 exempts consular or diplomatic missions and the use of encryption related to state security agencies from the declaration requirements.[103]

Enforcement: Under Article 168, government officials may carry out unannounced checks for telecommunications and ICT offences, and at the request of the public prosecutor – and in accordance with the provisions of the Code of Criminal Procedure - carry out searches and seizures for this purpose.

B) CYBERCRIME PROVISIONS IN LAW NO. 23/010, DIGITAL CODE

The Digital Code, like the law on telecommunications and information and communication technologies, contains both technical and content-based offences. It also establishes the principle that existing common law offences can be committed by means of an electronic communication network or a computer system.[104]

As in the case of the law on telecommunications and information and communication technologies, titles have been added to the tables for ease of reference, but are not provided in the law itself, except in some cases as paragraph

[103] See id, page 25 for more details.
[104] L'Ordonnance-Loi n°23/010, Article 331: "*Les infractions de droit commun commises au moyen d'un ou sur un reseau de communication electronlque ou un svsterne informatique sont reprirnees conforrnernent au Code penal congolais et aux dispositions penales particulleres en vigueur.*"

headings for one or more articles. Also, here again, the French text of some of the technical offences is provided in footnotes for precision.

LAW NO. 23/010 (DIGITAL CODE) - TECHNICAL OFFENCES	
Article 332: Unlawful access or remaining	It is an offence, intentionally and without right, to access, or remain in, all or part of an electronic communication system with a fraudulent intention. The penalty is penal servitude of three to five years and a fine, or one of these penalties only.[105] It is also an offence to exceed one's power of legal access to a computer system with fraudulent intent or with intent to harm. The penalty is penal servitude for two to five years and a fine, or one of these penalties only.[106] o "Access" is defined in Article 2 (item 1) as direct or indirect connection to all or any part of a computer system or an electronic communication network. o The offences of fraudulent access and remaining, which are separated in some SADC countries, are combined into one here. Some say that both are forms of unauthorized access.[107] o These offences overlap with Article 186 of *Law no. 20/17* discussed above.
Article 333: Unlawful access or remaining that affects computer data or the operation of the computer system.	When the illegal access or remaining described in Article 332 results in deleting, obtaining or modifying data contained in the computer system, or an altering of the operation of the computer system, the penalties are increased. The penalties are increased still further if the acts referred to are committed in violation of security measures.
Article 334: Interception or other technical interference with non-public transmission of data	It is an offence, intentionally and without right, and by technical means, to intercept, disclose, use, alter or misappropriate data during non-public transmission to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such data. The penalty is penal servitude of five to ten years and a fine. o This offence overlaps with Articles 180 and 182 of *Law no. 20/17* discussed above.
Article 335: Unauthorised transfer of personal data	It is an offence to transfer, without the authorization of the person concerned, that person's personal data from one information system or means of data storage to another. The penalty is penal servitude for six months to three years and a fine.[108]

[105] Id, Article 332: "*Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un svsteme informatique, avec une intention frauduleuse est puni dune peine de servitude penale de trois a cinq ans et d'une amende de clnquante millions a cent rnlllions de francs Congolais ou de l'une de ces peines seulement.*"

[106] Id: "*Quiconque, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'acces legal a un svsterne informatique, est puni d'une peine de servitude penale de deux a cinq ans et d'une amende de cinquante millions a cent millions de francs congolais ou de l'une de ces peines seulement*."

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

[108] L'Ordonnance-Loi n°23/010, Article 332: "*Est puni d'une servitude penale de six moi à trois ans et d'une amende de cinq millions a cent millions de francs conqolals, celui qui transfère, sans autorisation de la personne concernée, des données à caractère personnel de cette dernière d'un systerne informatlque ou d'un moyen de stockage de données vers un autre.*"

	There are enhanced penalties if this offence is committed with fraudulent intent, in connection with a computer system connected to another computer system, or by means of bypassing protective measures put in place to prevent access to the content of a non-public transmission. This offence does not apply in the following cases: • an interception carried out in accordance with a judicial warrant; • communication sent by or intended for a person who has consented to the interception; • interception carried out by a legal person authorized to do this for the purposes of public safety or national defence; • interception carried out by a legal or natural person legally authorized to do this under the legal provisions and regulations in force in the DRC.
Article 336: Data breach	It is an offence, intentionally and without right, to directly or indirectly damage, erase, deteriorate, alter or delete data. The penalty is penal servitude for six months to five years and a fine, or one of these penalties only. There is an enhnaced penalty if the offence is committed with fraudulent intent or intent to harm.
Article 337: Interruption of normal operaton of computer system	It is an offence, intentionally and without right, to directly or indirectly cause by any technological means an interruption of the normal operation of a computer system. The penalty is penal servitude for one to ten years and a fine, or one of these penalties only. There is an enhanced penalty where the offence causes damage to data in the affected computer system or in any other computer system. There is also an enhanced penalty where the offence causes a serious disturbance or prevents, totally or partially, the normal functioning of the computer system concerned or any other computer system. There is an enhanced penalty where the offence affects one or more sensitive or critical infrastructures. It is irrelevant whether the impact of the offence is temporary or permanent. o There is no definition of sensitive or critical infrastructure ("*infrastructures sensibles ou critiques*"),. However, Article 2 (item 43) defines critical or essential infrastructure ("*infrastructure critique· ou essentielle*") as facilities, resources, equipment and/or services, non-interchangeable and with particular characteristics where it would be impossible for potential competitors to reproduce them by reasonable means because of the prohibitive cost of their reproduction.
Article 338: Devices for unlawful use	It is an offence, intentionally and without right, to produce, sell, import, export, distribute or make available in another form, any electronic device or equipment including data or computer programs, primarily designed or adapted for the commission of one or more offences provided for in the Digital Code. The penalty is penal servitude for two to five years and a fine, or one of these penalties only.

	It is an offence, intentionally and without right, to possess any device, including data, primarily designed or adapted to enable the commission of one or more offences provided for in the Digital Code. The penalty is penal servitude for six months to five years and a fine, or one of these penalties only. It is an offence for any officer, public official or law enforcement office, in the exercise of his duties - except in the cases provided for by law – to unduly possess, produce, sell, obtain with a view to its use, import, distribute or make available in other forms a device, including data, primarily designed or adapted to enable the commission of one or more offences referred to in the Digital Code. The penalty is penal servitude for two to five years and a fine, or one of these penalties only. o This provision overlaps with Article 191 of *Law no. 20/17* discussed above. This formulation is an improvement over Article 191 because it refers to devices *primarily* designed or adapted for illegal purposes, and thus avoids criminalization of dual-use devices.
Article 339: Falsification of data or forgery	It is an offence to commit forgery by introducing, intentionally and without right, modified, altered or erased data into a computer system, so that they are stored, processed or transmitted by a computer system or electronic communication network, or by modifying data by any other technological means, for possible use of such data or modification of their legal scope. The penalty is penal servitude for three to five years and a fine, or one of these penalties only.[109] Anyone who makes use of such data, while knowing that the data are false; is punished with penal servitude of five to ten years and a fine of twenty to fifty million Congolese francs, or one of these penalties only. o This provision overlaps with Articles 188 and 189 of *Law no. 20/17* discussed above.
Article 340: Computer fraud	It is an offence, intentionally and without right, to cause or seek to cause harm to another with intent to gain an illegal economic advantage for oneself or a third party, by - • introducing into a computer system, modified, altered or erased data that is stored, processed or transmitted by a computer system; • interfering with the normal operation of a computer system or data contained therein. The penalty is penal servitude for five to ten years and a fine.
Article 348: Sending unsolicited messages	It is an offence to send any unsolicited electronic message based on the collection of personal data without a link that allows recipients to unsubscribe. Failure to comply with this provision exposes the offender to a fine.

[109] Id, Article 339: "*Quiconque commet un faux en introduisant, intentionnellement et sans droit, dans un système informatique ou un réseau de communication électronique, en modifiant, en altérant ou en effaçant des données qui sont stockées, traitées ou transmises par un système informatique ou un réseau de communication électronique ou en modifiant par tout autre moyen technologique, l'utilisation possible des données dans un système informatique ou un réseau de communication électronique, et par la modifie là portée juridique de telles données, est puni d'une servitude penale de trois a cinq ans et d'une amende de·vingt millions a cinquante millions de francs congolais, ou l;une de ces peines seulement.*"

Article 349: Deception	It is an offence to use elements of identification of a natural or legal person with the aim of tricking the recipients of an electronic message or the users of a website into communicating personal data or confidential information. The penalty is penal servitude for six months to two years and a fine, or one of these penalties only.
Article 350: Unauthorised processing or personal data	It is an offence to process personal data without having previously informed the person concerned of their right of appeal, rectification or opposition, the nature of the data transmitted and the destination of the data, or despite the opposition of the person concerned. The penalty is penal servitude of six months to two years and a fine, or one of these penalties only.
Article 351: Identity theft	It is an offence, intentionally and without right, to usurp another's identity through a computer system, by phishing or any other means, by using one or more forms of data that make it possible to attribute oneself falsely and to assume the identity of others in order to disturb their peace or to attack their honour, their reputation or their interests. The penalty is penal servitude for one to five years and a fine. It is an offence to intentionally and wrongfully avail oneself of a reason or legitimate justification, using a computer system at any stage of the offence, to transfer, possess or use a means of identifying oneself as another person with the intention of committing, aiding or encouraging an illegal activity. The penalty is penal servitude for two to five years and a fine, or one of these penalties only. It is an offence to pretend through a computer system to be a third party (institutional, trust or otherwise) with the aim of inciting or compelling the victim to communicate personal data. The penalty is penal servitude for five to ten years and a fine, or one of these penalties only.
Article 352: Misuse of personal data or confidential information for misappropriation of funds	It is an offence to use personal data or confidential information for the purpose of misappropriating public or private funds. The penalty is penal servitude for one to ten years and a fine.
Article 353: Bank card fraud	It is an offence to - • counterfeit or tamper with a payment or withdrawal card by means of or on an electronic communication network or a computer system; • knowingly use a counterfeit or falslfied payment or withdrawal card by means of or on an electronic communication network or computer system; • knowingly accept or agree to receive payment by means of a counterfeit or falsified payment card by means of or on an electronic communication network or a computer system. The penalty is penal servitude for two to five years and a fine, or one of these penalties only.
Article 354: Facilitating bank card fraud	It is an offence to manufacture, acquire, hold, transfer, offer or provide equipment, instruments, computer programs or any data, designed or specially adapted, to carry out the offences provided for in Article 353. The

	penalty is penal servitude for five to ten years and a fine, or one of these penalties only. Counterfeit or falisified cards must be confiscated for the purpose of destruction, as well as any items intended or used for bank card offences except where they were used without the knowledge of the owner. In cases of recidivism, a judicial authority may interdict the perpetrator's civil rights and prohibit professional or social activity for one to two years.
Article 363: Junk mail and spam	It is an offence to do any of the following, intentionally and without legitimate cause or justification, or where the perpetrator has wrongly availed himself of a motive or a justification: • trigger the transmission of erroneous, unwanted or unlawful messages from multiple emails or by an intermediate computer system; • use a computer system or a protected electronic communications network for relaying or retransmitting messages from multiple emails for the purpose of spoofing or to mislead users or the electronic or internet service provider as to the origin of these messages; • severely falsify header information in messages from multiple emails and intentionally trigger the transmission of these messages.
Article 380: Damage to an effective technical measure	It is an offence to use or to provide various listed means to circumvent, neutralize, suppress or undermine a protection or control mechanism (otherwise than for the purposes of IT security).

There are additional offences relating to **cryptology** which are not listed in the table above. In brief, cryptology services or the supply, import or export of certain means of cryptology, must be declared to and approved by the National Agency of Cybersecurity. It is a criminal offence to violate these rules. It is also an offence to sell or rent to others a means of cryptology which has been the subject of an administrative ban on use and circulation or to obstruct a criminal investigation a means of cryptology or refuse to provide related information or documents. Furthermore, using cryptology to facilitate or commit a crime can result in a doubled penalty. It is an offence to refuse to provide a cryptology key where cryptology has been utilised in an offence – and the penally is enhanced if the refusal results in a failure to prevent the commission of an offence or to limit its effects. [110]

LAW NO. 23/010 (DIGITAL CODE) – CONTENT-BASED OFFENCES	
Article 355: Online gambling	Online gambling is prohibited, and it is an offence to advertise unauthorized gambling by means of or on an electronic communications network or a computer system. The penalty is a fine. The competent court may increase the amount of the fine to quadruple the amount of advertising expenditure devoted to the illegal operation.
Article 356: Dissemination of tribalist, racist and xenophobic material through	It is an offence to intentionally create, upload, distribute or make available to the public through a computer system, writings, content, messages, photos, sounds, videos, drawings or any other representation of ideas or theories of racist, tribalist or xenophobic nature or in any form whatsoever in the sense of the present ordinance-law and in accordance with the

[110] Id, Articles 341-347.

an electronic system	provisions of ordinance-law no. 66-342 of 07 June 1966 on the repression of racism and tribalism. The punishment is penal servitude for one month to two years and a fine, or one of these penalties only.[111] o The Digital Code does not define ideas or theories of racist, tribalist or xenophobic nature. It is broader than some offences of this nature in the SADC region since it does not require that the material in question incite hatred or discrimination. Also, it appears to outlaw the creation of material of this nature by means of a computer system even if the material is not shared.
Article 357: Child pornography	It is an offence to produce, distribute, broadcast, import, export, offer, make available, sell, procure for oneself or others or possess any pornographic material featuring a child through a computer system or an electronic communications network. The penalty is penal servitude for five to fifteen years and a fine. o The Digital Code contains no definition of "pornographic material".
Article 358: Harassment through electronic communication (with intent)	It is an offence to initiate electronic communication that coerces, intimidates, harasses or causes emotional distress in a person, using a computer system, for the purpose of encouraging hateful, tribal and hostile behaviour towards good morals and patriotic values. The penalty is penal servitude for one month to two years and a fine. "Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement haineux, tribal et hostile aux bonnes moeurs et aux valeurs patriotiques est puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais." o The Digital Code contains no definition of any of the key terms concerning content, making this provision very broad and vague - which opens the door to subjective application and abuse.
Article 359: Harassment through electronic communication (with knowledge)	It is an offence to harass a person through a computer system or electronic communication network, while the harasser knew or should have known that he would seriously affect the tranquillity of the person targeted by this behaviour. The penalty is penal servitude for one month to two years and a fine, or only one of these penalties. "Quiconque aura harcèle, par le biais d'un système informatique ou d'un réseau de communication électronique, une personne alors qu'il savait ou aurait du savoir qu'il affecterait gravement a ce comportement la tranquillité de la personne visée, sera puni d'une servitude pénale d'un mois à deux ans et d'une amende de cinq cent mille à dix millions de Francs congolais ou de l'une de ces deux peines seulement." o The Digital Code contains no definition of harassment, making this provision very broad and vague.

[111] Id, Article 356: "*Quiconque aura, intentionnellement, créé, téléchargé, diffusé ou mis à la disposition du public par le biais d'un systems informatique des écrlts, contenus, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idees ou de théories, de idées raciste, tribaliste ou xénophobe ou sous quelque-forme que ce soit […]*":

	○ In contrast to the provision above, this crime does not require an intention to harm the targeted person, but only that the harasser knew (or should have known) the likely effect of the behaviour. ○ The offence above, where there is purpose, results in a prison sentence *and* a fine. The penalty for this offence includes the option of a prison sentence *and/or* a fine.
Article 360: False information	It is an offence to initiate or relay false information against a person through social networks, computer systems, electronic communication networks or any form of electronic medium. The penalty is penal servitude for one to six months and a fine, or one of these penalties only. "Quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sodaux, des systèmes informatiques, des réseaux de communication électronique de ou toute forme de support électronique, est puni d'une servitude pénale d'un à six mois et d'une amende de cinq cent mille à un million de Francs congolais ou de l'une de ces peines seulement." ○ This offence has the potential to chill free speech severely, since it would be difficult if not entirely impossible to know if each and every aspect of a communication was true. Note that there is no requirement that the "false information" initiated or relayed must have caused any actual harm. ○ This is one of the few offences that specifically mentions social networks
Article 361: Negation, gross minimization, approval or justification of international crimes or sexual violence	It is an offence to broadcast or make available through a computer system or an electronic communications network data which denies, minimises, endorses or justifies acts constituting the crime of genocide, war crimes, crimes against humanity, crimes of aggression and/or sexual violence as defined by international instruments and the Congolese Penal Code and recognized as such by a final decision by a national or international court. The penalty is penal servitude for 10 to 20 years and a fine of one to six Congolese francs. ○ This offence is broader than many similar offences in the SADC region and has the potential to undermine political debate on some issues – such as whether a particular prison sentence was justified in a case of sexual violence. The reference to "crimes of aggression" is also very wide. ○ Although the paragraph heading above this provision refers to "gross minimisation" ("*minimisation grossière*"), the text of the provision refers only to "minimising" ("*minimisent*"). ○ The *minimum* penalty for this offence is very high: imprisonment for 10 years and a fine of one million Congolese francs.
Article 362: Incitement or provocation to commission of terrorist acts and apology for terrorist acts	It is an offence, by means of a computer system or an electronic communications network to incite or directly provoke acts of terrorism. The punishment will be in conformity with Articles 157 to 160 of the Congolese Military Penal Code. ○ The paragraph heading above this provision refers to "apology for terrorist acts" ("*apologie des actes terroristes*"), but the text of the provision covers only incitement and provocation.

Article 371: Cyberespionage	It is an offence to do any of the following acts by or through a computer system, intending or knowing that the offence will benefit a foreign government, a foreign company, a foreign intermediary or a foreign agent qualified as a spy: • to steal or, without authorization, to appropriate, take, carry, hide or obtain fraudulently, artificially or by trickery, information likely to undermine the State security and safety or a commercial or industrial secret; • without permission, to copy, duplicate, illustrate, draw, photograph, download, modify, destroy, photocopy, reproduce, transmit, send, address by mail, communicate or cede a commercial secret; • to collect, purchase, or possess a trade secret, knowing that it was stolen or appropriated, obtained or transformed without authorization; • to attempt or conspire to commit any of these offences. The penalty for a natural person is penal servitude of five to fifteen years and a fine from five billion to ten billion Congolese Francs, or one of these penalties only. The penalty for an organization is a fine of fifteen to twenty billion Congolese Francs.
Article 372: Recording of images relating to the commission of offences	It is an act of complicity in willful attacks on the integrity of the person, to knowingly record by any means on any medium whatsoever, images relating to the commission of offences. It is an offence to knowingly distribute such images. The penalty for distribution is penal servitude for one to five years and a fine. However, this does not apply in the case of the normal exercise of a profession whose purpose is to inform the public, or when it is carried out in order to prove the offence in court.[112] o Although professional journalists appear to be excluded, this offence could inhibit the role of ordinary citizens in exposing crime, particularly crimes committed by law enforcement or government officials.
Article 373: Distribution of instructions for manufacturing destructive devices	It is an offence to broadcast, by means of an electronic communications network or a computer system, methods for the manufacture of destructive devices made from gunpowder or explosive substances, nuclear, biological or chemical materials, or from any other product intended for domestic, industrial or agricultural use. The penalty is penal servitude of five to ten years and a fine. There is an enhanced penalty where the offence has resulted in murder or assassination.
Articles 375, 377-378, 381-382: Infringement of copyright intellectual and industrial property rights or neighbouring rights	There are various offences relating to infringements of copyright and similar rights by means of a computer system or an electronic communications network, or technological applications or devices.
Articles 375-376, 379:	There are several offences relating to infringement of the copyright of computer programmes and counterfeiting or piracy of computer software and hardware.

[112] Id, Article 372: "*Le présent article n'est pas applicable lorsque l'enregistrement soit la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public soit lorsqu'il est réalisé afin de servir de preuve en justice*."

Copyright infringement, counterfeiting or piracy of computer programmes, software or hardware	

With respect to **penalties** for both technical and content-based offences, conviction for some of the offences results in a minimum term of imprisonment along with a fine – with no option for imposing only one of these penalties. Significantly, one such offence is the vaguely defined crime of online harassment, where this crime is committed with the intent to encourage hateful, tribal and hostile behaviour towards good morals and patriotic values.

Filters: The Digital Code requires internet service providers to inform subscribers of the existence of filtering mechanisms, with failure to do so being a criminal offence.[113]

Identity of subscribers and content creators: Online service providers are required to hold and maintain data likely to allow identification of anyone who controls the creation of any content of the services they provide. They must also obtain guarantees from the editors of online public communications services that the identity of the content creators can be provided. The Public Prosecutor or the Data Protection Authority may require online service providers to preserve or produce this information in accordance with applicable laws.[114]

Persons who edit online public communication services must make available to the subscribers of such services the names of the publication's director and editor, company name, address, email and telephone number.[115]

Take-down provisions: Online service providers are not responsible for the content of information they transmit and to which they give access, if they meet the following conditions:

1. they have not originated the transmission;
2. they have not selected the recipients of the transmission;
3. they have not modified the information in the transmission; and
4. they have informed their subscribers of the existence of technical means making it possible to restrict access to certain services, or selected and offered one such means. (art 283)

[113] Id, Article 364.
[114] Id, Article 282: "*Le fournisseur des services en ligne est tenu détenir et de conserver les données de nature à permettre l'identification de quiconque aura contrlbué à la création du contenu ou de l'un des·contenus des services dont ils sont prestataires.*
Il est éqalement tenu de fournir aux personnes qui éditent un service de communication au public en ligne des garanties permettant à celles-ci de satisfaire aux conditions d'identification prévues à la présente ordonnance-loi.
L'Officier du Ministère Public ou l'Autorité protection des données peut requerir aupres des fournlsseurs de services en ligne, conformément à la loi en la rnatiere, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées à alinéa 1 du présent article."
[115] Id, Article 288..

Internet access providers and online service providers do not incur civil or criminal liability for the activities or information stored at the request of a recipient of their services, if they were unaware of their illegal character, or if they acted promptly to remove the data or to make access to it impossible as soon as they became aware of its illegal nature (art 284).[116]

Internet access providers and online service providers must contribute to the fight against the offences provided for in this ordinance-law by putting in place an easily accessible and visible device allowing anyone to bring to their attention the facts of an infraction of the law.[117]

Knowledge of disputed facts is presumed to have been acquired by a supplier of online services when notified of the following:

1. the date of the notification;
2. if the notifier is a natural person: his name, occupation, residence, birth date, date and place of birth;
3. if the notifier is a legal person: its legal form, its company denomination and its seat of operation;
4. the addressee's name and address or, if it is a legal person, its corporate name and head office;
5. a description of the disputed facts and, if possible, their precise location;
6. the reasons why the content should be removed;
7. a copy of the correspondence addressed to the author or publisher of the contentious information or activities requesting their discontinuation. withdrawal or modification, or any explanation of why the justification author or publisher could not be contacted.[118]

The person who knowingly reports inaccurate information about illegal content or activities to an online service provider, with the aim of obtaining the withdrawal or stopping the dissemination of such content or activities, commits a criminal offence.[119]

Internet access providers and online service providers do not have a general duty to monitor the information they transmit or store, unless requested to do so temporarily by an officer of the Ministry of Public Affairs, the National Agency for Cybersecurity, or an agency responsible for security and maintenance of public order.[120]

Internet access providers and online service providers are required to promptly inform competent authorities of all illegal activities reported to them.[121] They also have a duty to suspend any content likely to infringe morality *("tout contenu sussceptible de porter*

[116] Id..Similar rules apply to caching and linking to illegal information. Id, Articles 290-291.
[117] Id, Article 287.
[118] Id, Article 285. The statute refers to notification of *one* of the listed elements ("*La connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il·lui est notifié l'un des elements suivants…*"), but it appears to be intended to refer to a notification containing the listed elements.
[119] Id, Article 365.
[120] Id, Article 286.
[121] Id, Article 287.

atteinte à la moralité").[122] This broad authority is particularly worrying, particularly in the absence of any further details or definitions as to what this might encompass.

A judicial authority may order any online service provider, and failing that, any internet access provider, to apply specific measures to prevent damage or stop damage caused by the content of an online service, in accordance with applicable laws.[123]

Criminal sanctions: It is a crime for internet service providers to fail to meet any of the obligations placed on them by the Digital Code– with this rule applying to a legal person, as well as to any natural person or any manager of a legal person, that is by law or *de facto* carrying out the activities of an online communication services provider.[124]

C) PENAL CODE OFFENCES RELATED TO FREEDOM OF EXPRESSION

The Penal Code contains a number of content-based offences which seem to be frequently applied in practice to limit freedom of speech. The key provisions of this nature are summarised here.[125]

Criminal defamation is covered by Article 74. It applies to anyone who maliciously and publicly imputes a specific fact to a person that is likely to undermine their honour or reputation, or to expose them to public contempt. The punishment is penal servitude of eight days to one year, and a fine of twenty-five to one thousand zaires, or one of these penalties only. The requirement of malicious intent narrows the offence, in theory, but note that there is no explicit mention of truth or fair comment as defences.

CODE PENAL CONGOLAIS

Article 74: Celui qui a méchamment et publiquement imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur ou à la considération de cette personne, ou à l'exposer au mépris public, sera puni d'une servitude pénale de huit jours à un an et d'une amende de vingt-cinq à mille zaïres ou d'une de ces peines seulement.

Under Article 75, **public insult** can be punished with penal servitude from eight days to two months and a fine of up to five hundred zaires, or one of these penalties only. This is a shocking broad and vague offence that has been frequently applied in practice, as the case studies provided in this chapter illustrate.

CODE PENAL CONGOLAIS

Article 75: Quiconque aura publiquement injurié une personne sera puni d'une servitude pénale de huit jours à deux mois et d'une amende n'excédant pas cinq cents zaïres ou d'une de ces peines seulement.

[122] Id, Article 287: *Ils sont également tenus, d;une part,d'informer et promptement les autorités compétentes de toutes activités illicites mentionnées qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part suspendre tout contenu sussceptible de porter atteinte à la moralité*".

[123] Id.

[124] Id, Articles 366-368.

[125] Code pénal congolais, Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004, as amended in 2006 in respect of sexual offences by Loi n° 06/018 du 20 juillet 2006 modifiant et complétant le Décret du 30 janvier 1940 portant Code pénal congolais.

Article 77 appears to criminalise **insults directed at a person** even if they are not made publically. The penalty is relatively minor, constituting penal servitude of eight days and a fine of a maximum of two hundred zaires, or one of these penalties only.

CODE PENAL CONGOLAIS

Article 77: Sera puni d'une servitude pénale de huit jours et d'une amende de deux cents zaïres au maximum ou d'une de ces peines seulement celui qui aura dirigé contre une personne des injures autres que celles prévues dans les dispositions précédentes de la présente section.

There are also a number of offences that on speech relating to **public authorities**:

- Article 76 punishes **slanderous denunciation** ("*une dénonciation calomnieuse*") **of a judicial authority, a public official or a subordinate**, made verbally or in writing.
- Article 135*bis* makes it an offence to directly **instigate disobedience to the laws**.
- Article 135*ter* makes it an offence **to provoke soldiers to turn away from their military duties and from the obedience they owe to their leaders**, in any way whatsoever.
- Article 136 makes it an offence to **insult**, through words, deeds, gestures or threats, certain **public functionaries in the exercise of their mandate or functions**. The steepest punishment is for insulting a member of the Political Bureau, the National Assembly, the Government, or the Constitutional Court. It is a somewhat lesser offence to insult a member of the courts and tribunals, an officer of a public ministry, a senior officer of the Armed Forces or the gendarmerie, or a governor in this manner. It is a still lesser offence to insult other agents of a public authority. **Insults against government bodies** is a similar crime, under Article 137. However, Article 138*ter* provides that prosecutions for these offences can be initiated only on a complaint from the injured person or the body to which the person belongs.

There are several offences that apply to the dissemination of **false information**:

- Article 199*bis* makes it an offence to knowingly spread false rumours that are likely to alarm the public, worry them, or incite them against "the established powers", where this is done with the intention of bringing trouble to the State. The penalty is imprisonment and a fine, or one of these penalties only.
- Article 199*ter* covers the same acts where they are knowingly committed without the intention of bringing trouble to the State. The penalty is imprisonment and a fine, or one of these penalties only – within a slightly lower range of time or money given the absence of the indicated intention.

- Article 211 makes it an offence to knowingly contribute to the publication, dissemination or reproduction, by any means whatsoever, of false news, fabricated or falsified material or material falsely attributed to third parties where this is done with the intention of disturbing the public peace. It is also an offence to exhibit in public any drawings, posters, engravings, paintings, photographs, objects or images that are likely to disturb the public peace, regardless of intention. The penalty is imprisonment or a fine, or both.

The law is not clear on how to determine what is considered a "false rumour" or "false news" or what the threshold is for deciding that information is likely to alarm or worry the public or incite them against "established powers". Thus, they provide an overly wide degree of discretion to those who enforce the law.[126]

CODE PENAL CONGOLAIS

Article 199*bis*: Quiconque, en répandant sciemment de faux bruits de nature à alarmer les populations, à les inquiéter ou les exciter contre les pouvoirs établis, aura porté ou aura cherché à porter le trouble dans l'Etat, sera puni d'une servitude pénale de deux mois à trois ans et d'une amende de cent à cinq cents zaïres, ou d'une de ces peines seulement.

Article 199*ter*:
Sera puni de un mois à un an de servitude pénale et d'une amende de vingt à cent zaïres ou de l'une de ces peines seulement, celui qui, sans intention de porter le trouble dans l'Etat, aura néanmoins sciemment répandu de faux bruits de nature à alarmer les populations, à les inquiéter ou à les exciter contre les pouvoirs établis.

Article 211: Sera puni d'une servitude pénale de deux mois à trois ans et d'une amende de mille à dix mille zaïres, ou d'une de ces peines seulement:
- celui qui, en vue de troubler la paix publique, aura sciemment contribué à la publication, à la diffusion ou à la reproduction, par quelque moyen que ce soit, de nouvelles fausses ou de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers;
- celui qui aura exposé ou fait exposer, dans les lieux publics ou ouverts au public, des dessins, affiches, gravures, peintures, photographies, tous objets ou images de nature à troubler la paix publique.

Anonymous publications are prohibited.[127]

D) PRESS FREEDOM LAW OFFENCES RELATED TO FREEDOM OF EXPRESSION

The Press Freedom Law enacted in 2023 states that it is considered an "**attack through the press**" ("*atteinte par voie de presse*") for a *media professional* to engage in any act or behaviour during the exercise of his profession that undermines public order, the rights of others or good morals and causes harm. It is also an "**attack**" ("*atteinte*") for a *media user* to violate and damage public order, the rights of others and good morals. Offences by the online press are punished in accordance with the legislation in force in criminal matters. [128] Sanctions for other types of media or for media users are not discussed in this provision, but presumably also fall under the criminal law.

It is an offence for anyone **acting in bad faith** to publish, disseminate or transmit **false news or allegations, or inaccurate facts**, by way of written press, online press, broadcast media or any other medium, where this has disturbed public order, aroused

[126] "LEXOTA Country Analysis: Democratic Republic of Congo", last updated July 2022.
[127] Code pénal congolais, Article 150h-150i.
[128] **L'ordonnance-loi n°23/009**, Article 113.

fear among the population, or caused the destruction of public property.[129] This also applies to false information against magistrates, civil servants or agents invested with the public authority in respect of the exercise of their functions.[130] It is similarly an offence, acting in bad faith, to publish, distribute or reproduce false news, fabricated or falsified material or material falsely attributed to third parties where this has disturbed the public peace.[131] These acts will be "punished according to law" - – which seemingly refers to the Penal Code provisions on false information discussed above, with the addition of a bad faith requirement and a requirement that actual harm must result in respect of the press. The publication, distribution or reproduction of false information in bad faith will be punished in accordance with the code of military justice when it has shaken the discipline or morale of the armies or hindered a war effort of the nation.[132]

It is an offence to **falsely claim to be a media professional**, punishable under the relevant provisions of the Penal Code.[133]

There are several points on **legal proceedings** and **information about crimes committed**. It is also punishable under the Penal Code for the press to violate the secrecy of a criminal investigation, to undermine the presumption of innocence in respect of a criminal proceeding, It is also prohibited to publish by any means photographs or portraits of people with the aim of thus disclosing all or part of the circumstances of a murder, an assassination, a suicide, a poisoning, threats, blows and injuries, attacks on morality and public morals or kidnapping. A further offence is the publication of information about the trial of a minor child or any trial in which a minor child is involved.[134]

It is also forbidden to offer, give or sell to **minor children** publications of any kind inciting to debauchery, prostitution, crime or the consumption or trafficking of drugs, alcohol or tobacco.[135]

It will also be punished according to the Penal Code -

- to directly provoke attacks on persons, in particular murder, assassination, theft, rape, violence, destruction and terrorism
- to apologise for war crimes, crimes against humanity, crimes of genocide or crimes of terrorism;
- to directly incite hatred, in particular religious, ethnic, tribal, regional or racial hatred.[136]

The Press Freedom Law also contains provisions concerning which specific media professionals have criminal, civil and professional liability for wrongs committed by the press.[137]

[129] Id, Article 120
[130] Id, Article 124.
[131] Id, Article 123.
[132] Id.
[133] Id, Article 124.
[134] Id, Articles 125-126.
[135] Id, Article 126.
[136] Id, Article 136.
[137] Id, Articles 127-128.

E) STATE SURVEILLANCE

The provisions of **Law no. 20/17 of 25 November 2020 governing telecommunications and information and communication technologies** that justify interference with information privacy, have been analysed as follows:

> *These exceptions include the lifting of the secrecy of correspondence at the request of the public prosecutor's office or with the authorisation of the courts and tribunals in the context of a judicial investigation, and derogation from this secrecy by the competent services – including the ANR – for reasons of internal and/or external state security, national defence or public order (Article 126). Next, Article 127 provides that "only the needs of information motivated by the requirements of the ultimate demonstration of the truth in a judicial case may authorise the Public Prosecutor's Office at the Court of Cassation to prescribe the interception, recording and transcription of correspondence emitted by means of telecommunications and information and communication technologies". Article 129 goes further by empowering the public prosecutor's office at the Court of Cassation to request any agent of a service or body to install a device necessary to carry out the operations indicated in the previous Article 127(1), while Article 128 provides that this decision may last for three months, renewable for the purposes of the investigation. The vagueness of these exceptions leads to disproportionate infringements of these rights in the Democratic Republic of Congo, which can be extended for as long as the person making the decision invokes the need for the investigation, as the number of renewals is not limited.*[138]

Decree-Law No. 003-2003 on the creation and organization of the National Intelligence Agency authorises state surveillance of any persons or groups suspected of carrying out an activity that could undermine state security, while **Decree-Law 1-61 of 25 February 1961 on State security measures** allows the Minister of the Interior to place persons who undermine state security under surveillance by a simple written decision. The broad justification of "state security" is reportedly abused as a means of stifling political opponents.[139]

In addition, **Ministerial Order No. CAB/MIN/PT&NTIC/AKIM/KL/Kbs/002 of 10 June 2020** has authorised the establishment of a Central Electric Identity Register (CEIR), as well as allowing the government to monitor mobile telephone subscribers. Through this registry, the government has access to information about millions of mobile phones that can facilitate State surveillance.[140]

In general, the legal criteria used to justify violations of privacy are based on national defence, national security, criminal investigations, the protection of public order and the prevention of crime, without much detail.[141] Yet, even though many of the laws

[138] Trésor Maheshe Musole and Jean-Paul Mushagalusa Rwabashi, "Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection", Media Policy and Democracy Project, December 2021, page 20.
[139] Id, page 21.
[140] Id, page 20.
[141] "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA (Collaboration on International ICT Policy for East and Southern Africa), February 2022, page 24.

relied upon to authorise state surveillance are broad and vague, there were reports that the government monitored private online communications without appropriate legal authority.[142]

At the same time, there are limits on citizen surveillance. Article 58 of **Law no. 20/17** requires that remote surveillance and video surveillance systems, in both closed private spaces and spaces open to the public, are permitted only after being declared to ARPTIC, which will provide a certificate and inform the Minister of the declaration. The terms and conditions for granting approval are set by ministerial order.

F) SIM CARD REGISTRATION

SIM card registration is mandatory and has been discussed above in the section on obligations of service provers in connection with cybercrime.

G) TAKE-DOWN NOTIFICATIONS

There are several provisions of the Digital Code which, taken together, constitute the equivalent of a take-down procedure. These have been discussed above.

6.5 ELECTION LAW AND FREEDOM OF EXPRESSION

DRC's next general election (which will include a presidential election) is scheduled for 20 December 2023.

Elections in DRC are regulated by the **Independent National Electoral Commission** ("*Commission Électorale Nationale Indépendante*") **(CENI),** which is established by the Constitution.[143] According to Freedom House, CENI is viewed by opposition parties and civil society as lacking independence and supporting the president. Freedom House also reports that President Tshisekedi reformed the CENI in July 2021, allocating seats for civil society groups, the ruling coalition, and the opposition. This move was criticised because the balance of the body tilts towards the government, which gives Tshisekedi control over future elections.[144]

[142] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 2A.
[143] Democratic Republic of the Congo 2005 Constitution, Article 211. CENI is governed by the Loi organique n° 10/013 du 28 juillet 2010 portant organisation et fonctionnement de la Commission Électorale Nationale Indépendante telle que modifiée et complétée par la Loi organique n° 13/012 du 19 avril 2013 et la Loi organique n° 21/012 du 03 juillet 2021 (Textes coordonnés et mis à jour) ("Organic Law No. 10/013 of 28 July 2010 on the organization and functioning of the Independent National Electoral Commission as amended and supplemented by Organic Law No. 13/012 of 19 April 2013 and Organic Law No. 21/012 of 03 July 2021 (Coordinated and updated texts)"). The CENI website can be found here.
[144] "Freedom in the World 2022: Democratic Republic of the Congo", Freedom House, section A3; Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).

DEMOCRATIC REPUBLIC OF THE CONGO 2005 CONSTITUTION

Article 211
An Independent National Electoral Commission with legal personality is established.
The Independent National Electoral Commission is charged with the organization of the electoral process, in particular the registration of voters, the maintenance of the electoral roll, voting operations, the counting of votes and any referendum.
It ensures the regularity of the electoral and referendum process.
An organic law establishes the organization and the operation of the Independent National Electoral Commission.

This brief overview of past election controversies provides context for the forthcoming elections:

The DRC gained independence from Belgium in 1960. Its post-independence history is bloody: the first post-independence leader, Patrice Lumumba, was assassinated in 1961. In 1965, military officer Mobutu Sese Seko assumed power after a period of civil war. Mobutu ruled his one-party state (which he renamed Zaire) until 1996, when he was ousted by an armed coalition led by Laurent Kabila. However, the country remained dangerously unstable and effectively in a state of civil war. In 2001, Laurent Kabila was assassinated by his bodyguard and was succeeded by his son, Joseph Kabila. Although Joseph Kabila is credited with introducing a number of important reforms, most notably a new constitution, his democratic credentials remained extremely poor. The last election which he won (in 2011) is disputed and lacked credibility due to widespread irregularities. President Kabila's second five-year term of office ended in December 2016, but the DRC failed to hold elections and he ruled without an electoral mandate, albeit with the backing of the Constitutional Court. In May 2016, the Constitutional Court, in a heavily criticised judgment, interpreted section 70 of the constitution, which provides that the president continues in office until the assumption of office of his successor, as entitling President Kabila to remain in office without an election having taken place. Critics argue that the Constitutional Court should have found section 75 of the constitution applicable — this provides for the Head of the Senate to assume office temporarily in the case of a presidential vacancy.

In August 2018, President Kabila announced he would not be running for a third term and the ruling party chose Emmanuel Shadari, seen as a Kabila loyalist, as its candidate for the presidential elections. The presidential elections were held on 30 December 2018. The outcome of the election was extremely controversial. The Electoral Commission and the Constitutional Court certified that Felix Tshisekedi, an opposition figure, won the election. However, powerful institutions, such as the Catholic Church, disputed this, and it, and the international press, reported that another opposition leader, Martin Fayulu, had, in fact, won by a landslide as evidenced by leaked election data.

At the time, the African Union called for the DRC to delay announcing the election results due to serious discrepancies between the provisional results announced by the Electoral Commission and the actual ballots cast. This was ignored and, on 24 January 2019, Mr Tshisekedi (apparently with former-President Kabila's backing) was sworn in as

the country's new president. Mr Tshisekedi's election has since been accepted by the European Union and the United States of America. The AU also backtracked on its objections to the election results as it elected Mr Tshisekedi the second vice-president of the AU on 16 February 2019.[145]

Looking at some of the freedom of expression issues in the last general election, CENI's decision to **refuse accreditation** to several international election observers and **media representatives** in the 2018 elections was internationally criticised. Another criticism of the 2018 election process was that Government authorities and the State Security Forces **prevented opposition parties from holding public meetings, assemblies, and peaceful protests**, or used force to prevent or disrupt their events. There were also reports that the government exercised **political influence in the distribution of media content during the election campaign**.[146]

RTNC, the **national broadcaster**, reportedly committed over 40% of its campaign airtime to the ruling party candidate and **failed to grant all candidates equal access**, while the CSAC did not enforce its decision to allocate equal airtime to all candidates, with no sanctions being imposed on RTNC or other media for their unequal coverage.[147]

During the 2018 campaign period, some candidates conducted digital campaigns on **social media platforms** even though internet reach in DRC is not widespread. It is reported that fake news and misinformation was rife on social media platforms at key stages of the process. [148]

Right after the general elections were held on 30 December 2018, the **government shut down all primary telecommunications**. A senior government official said that internet and SMS services were cut to preserve public order after "fictitious results" began circulating on social media, and that the communications services would be restored only after the publication of election results on 6 January. This step reportedly hindered the ability of electoral observers and witnesses to relay information from rural polling stations. The UN Special Rapporteur on freedom of expression at the time stated that this shutdown was in clear violation of international law and could not be justified by any means, urging government authorities to restore internet services as a matter of urgency.[149]

Despite the election controversies, the US State Department notes that "the 2019 inauguration of President Tshisekedi was the first peaceful transfer of power in the country's history".[150]

[145] Justine Limpitlaw, *Media Law Handbook for Southern Africa – Volume 1*, "Chapter 5: Democratic Republic of Congo", Konrad Adenauer Stiftung, 2021, page 182 (footnotes omitted).
[146] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, section 3.
[147] "Democratic Republic of the Congo 2018 Harmonized Presidential, Parliamentary and Provincial Elections: Expert Mission Report", The Carter Center, undated.
[148] Id.
[149] "UN expert urges DRC to restore internet services", UN Office of the High Commissioner on Human Rights, 7 January 2019.
[150] "2022 Country Reports on Human Rights Practices: Democratic Republic of the Congo", US State Department, "Executive Summary".

One recent analysis referred to the forthcoming 2023 elections as "the most unpredictable on the continent in 2023" and provides the following overview of the political environment:

> *The elections in the Democratic Republic of the Congo (DRC) mark another important inflection point in this country's long and elusive quest for democracy. To make progress, this country of more than 100 million people must overcome its deep-seated legacies of fraudulent, patronage-based, and opaque electoral practices institutionalized over the decades by the regimes of Mobutu Sese Seko and Laurent and Joseph Kabila.*
>
> *The incumbent, President Felix Tshisekedi, is seeking a second 5-year term. Son of the esteemed democracy champion, Etienne Tshisekedi, Felix Tshisekedi had an ignoble start to his presidency. In the view of many, he cut a power-sharing deal with the outgoing president, Joseph Kabila, to be declared the victor of the December 2018 elections. Independent analysts, including the respected election monitoring group, the National Episcopal Conference of Congo (CENCO), indicated that the genuine winner by a commanding margin was the leading opposition candidate, Martin Fayulu.*
>
> *Bowing to pressure from Kabila, the African Union and international democratic actors declined to demand a recount as called for by CENCO and many governments. A challenge of Tshisekedi's first term, thus, has been to overcome weak legitimacy in the eyes of his compatriots.*
>
> *Once in office, Tshisekedi has been able to claw away some influence from Kabila's entrenched grip on the institutions of power. This includes replacing the Kabila-backed speaker of the National Assembly as well as the influential prime minister. Tshisekedi has also made some progress on reforms. Perhaps most notable has been his reducing the repressiveness of the security services by replacing certain senior intelligence and internal security officials who had been sanctioned for human rights violations. Tshisekedi has also made headway in replacing some Kabila loyalists within senior ranks of the judiciary.*
>
> *This progress is noteworthy in that, upon stepping down, Kabila continued to exert great influence over the machinery of government in the DRC. Kabila's Common Front for Congo (FCC) alliance controlled 350 of the 500 seats in the National Assembly as well as a majority of ministries, judicial appointments, and senior officials throughout the security sector. Many observers expected Tshisekedi to be little more than a front man for Kabila's continued wielding of power behind the scenes.*
>
> *Tshisekedi was also a prominent defender of democratic norms on the continent during his 1-year tenure as African Union Chairman in 2021-2022.*
>
> *Nonetheless, in the process of winning over Kabila allies in government, democracy activists worry that Tshisekedi has adopted some of [the] same tactics as his predecessor. This includes the reliance on patronage to direct the unwieldy bureaucracy of the Congolese state.*
>
> *Finance Minister Nicolas Kazadi noted, for example, that the budget for exceptional security expenses had increased tenfold, though with little transparency over how*

these resources were improving security given the country's notoriously corrupt and abusive security sector.

Tshisekedi and his family have been linked to opaque deals with Chinese businesses for access to artisanal copper, cobalt, and diamonds. Tshisekedi has also been criticized for not doing enough to rein in the mechanisms of state capture employed by Kabila. This includes a $6-billion infrastructure-for-resources swap with Chinese state-owned firms dubbed the "deal of the century" and the embezzlement of $3.7 billion in state funds by internationally sanctioned mining magnate, Dan Gertler, through Kabila-endorsed contracts.

Tshisekedi controversially appointed close ally Denis Kadima as the new commissioner of the Independent National Election Commission (CENI) in 2021. Tshisekedi also modified the allocation of seats within CENI. While opposition parties and civil society are represented, critics feel the distribution still favours the ruling party.

Many democracy advocates, moreover, are critical that the Tshisekedi-led National Assembly failed to pass an amendment that would require CENI to adopt electoral best practices such as announcing electoral results at each polling center. Tallying and reporting of aggregate results from a central location is less transparent and more prone to rigging. In Kenya, for example, results announced at polling stations are final and cannot be altered. Additionally, the DRC relies on candidates gaining a plurality of votes rather than an absolute majority, making it easier for a candidate to win by solely appealing to their base rather than building a more inclusive coalition.

Tshisekedi faces credible opposition from numerous quarters. Most prominent among these is Martin Fayulu, the former ExxonMobil executive widely perceived to have won the 2018 election. Born in Kinshasa, Fayulu commands a broad following across the DRC's highly diverse constituencies. Moïse Katumbi, a former governor from the southeastern region of Katanga, is another popular rival. He was seen as such a threat by Kabila that the former leader launched several gratuitous court cases against him, forcing Katumbi into exile. Former Kabila Prime Minister Augustin Matata Ponyo Mapon is another prominent entrant to the presidential race. In 2018, there were nearly two dozen presidential contenders. The presence of so many candidates introduce considerable unpredictability given the DRC's single-round plurality system.

While the DRC's electoral institutions and oversight mechanisms may be weak, the country has a vibrant and organized civil society committed to a democratic system of government. These groups continue to demand transparency and popular participation in elections and holding leaders accountable to citizen interests. Among the most prominent, CENCO deployed over 40,000 election monitors in 2018. Through the experience gained from multiple cycles of parallel vote counting processes, it is increasingly difficult for candidates to credibly claim outcomes that deviate significantly from independent tallies.

Another wild card in the 2023 election is the ongoing instability in the east of the country. This is a multilayered conflict involving rivalries between Rwanda and Uganda, access to and trafficking of the DRC's vast and unregulated mineral deposits, 140 local armed groups, ethnic rivalries, and legacies of previous conflicts in the Great Lakes region. Prospects of Chinese and Russian interests joining the competition for resources in the region adds another level of complexity. Perceptions that Tshisekedi may have made opaque deals for DRC's resources also sets off a strong nationalist resentment that may have political consequences.

The resurgence of the threat from the armed group M23 in late 2021 has heightened tensions among all parties and added to the displacement of more than 5.5 million people from Ituri, North and South Kivu, and Tanganyika Provinces. The deployment of the East African Standby Force at the end of 2022 has helped tamp down tensions, though this will need to be translated into longer-term mediated solutions.

Ongoing instability may affect the ability of these eastern provinces to vote—an issue also faced in 2018. A full-blown regional conflict would clearly scramble the entire electoral process. Tshisekedi advisors have suggested that the elections may need to be delayed due to the unrest. This is fueling concerns that the instability in the east may be used as a pretext for Tshisekedi to prolong his tenure—harkening back to Kabila's 2-year delay before holding elections after his second term had expired.

The 2023 elections will say much about the trajectory of the Tshisekedi presidency. Will it hold to his stated democratic and reformist aspirations? Or will it fall into the well-worn governance norms in DRC—building exclusive patronage networks at the expense of public goods and services?

With so many uncertainties, the DRC polls may be the most unpredictable on the continent in 2023. While the DRC does not have a strong track record of transparent and credible elections, this remains the aspiration of millions of Congolese citizens. Experience has also shown that civil society will not blithely accept a fabricated outcome. Much may once again come down to the courts—and how regional and international actors respond.[151]

The CSAC adopted a new **directive on media regulation during the electoral campaign** on 21 June 2023.[152] However, this directive could not be located online as of August 2023.[153]

[151] Joseph Siegle and Candace Cook, "Africa's 2023 Elections: Democratic Resiliency in the Face of Trials: Democratic Republic of the Congo", Africa Centre for Strategic Studies, 31 January 2023 (updated on 10 July 2023).
[152] Christel Insiwe "Élections: Le CSAC adopte la directive de réglementation de la campagne électorale dans les medias", *7sur7.cd*, 22 juin 2023; Emille Kayomba, "Processus électoral : le CSAC et la CENI en concertation pour des bonnes élections", *b-onetv*, 14 juillet 2023.
[153] As a point of comparison, the previous "Directive du Conseil Supérieur de l'Audiovisuel et de la Communication n°CSAC/AP/001/2015 du 05 mars 2015 relative à la campagne électorale à travers les medias" is available here.