Universal Periodic Review - 47th session

Joint Stakeholder Report

Human rights in the digital context and the state of civic space in the Democratic Republic of Congo (DRC)

Rudi International is a non-profit organisation based in the Democratic Republic of Congo (DRC). Since its incorporation in 2011, Rudi International has been working with programmes focusing on education and technology. For the latter, Rudi works at the intersection of technology and human rights, with projects focused on capacity building, research and advocacy.

Website: www.rudiinternational.org
Contact address: Av ESCO, Q. Lac Vert, Goma, DRC
Contact person: Arsène Tungali, Executive Director (arsenetungali@rudiinternational.org)

The Association for Progressive Communications (APC), an organisation in consultative status with ECOSOC, advocates the strategic use of information and communications technologies to advance human rights. The APC network has 67 organisational members and 41 associates active in 74 countries, including the DRC.

Website: www.apc.org
Contact address: PO Box 29755, Melville 2109, Johannesburg, South Africa
Contact person: Verónica Ferrari, Global Policy Advocacy Coordinator (veronica@apc.org)

April 2024

I. INTRODUCTION

1. This report focuses on human rights in the digital context and the state of civic space, including online, in the Democratic Republic of Congo (DRC). In particular, this report covers the following issues: disinformation; cybercrime, cybersecurity and data protection; and the situation of journalists and human rights defenders, with a particular focus on technology-facilitated gender-based violence targeting women journalists, politicians and rights defenders.

2. To produce this report, the relevant information and communications technology (ICT) legal framework in the DRC was analysed, and consultations and interviews with human rights defenders and civil society actors were carried out to complement this desk research. Insights from 10 non-governmental organisations focusing on women's rights online and offline in the DRC also informed our findings and recommendations on this topic.

II. NATIONAL CONTEXT

3. According to data from the International Telecommunication Union, the internet penetration rate in the DRC in 2021 was 23%.[1] The mobile internet penetration rate in the country was at 29.6% as of the first quarter of 2023 according to a report by the Regulatory Authority of Congo.[2] The number of internet users in the DRC is increasing each year, and as of January 2023 was estimated to be 23.04 million people.[3] However, reports indicate that the growth is slower than would be expected for a country that is the second largest in Africa.[4]

4. There are disparities in the access to and use of technologies in the country. For instance, as of January 2023, only 36.5% of women used

[1] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CD
[2] Autorité de Régulation de la Poste et des Télécommunications du Congo. (2023). *Observatoire du Marche de la Telephonie Mobile Rapport du 1er Trimestre 2023.* https://arptc.gouv.cd/app/uploads/2023/08/RAPPORT-OBSERVATOIRE-MARCHE-T1-2023.pdf
[3] Kemp, S. (2023, 13 February). Digital 2023: The Democratic Republic of the Congo. *DataReportal.* https://datareportal.com/reports/digital-2023-democratic-republic-of-the-congo
[4] Ryakitimbo, R., Nkhowani, B., & Mwimbi, J. (2023). *The holistic approach: Exploring women's online freedom of expression and freedom of assembly in the Democratic Republic of Congo*. Association for Progressive Communications. https://firn.genderit.org/sites/default/files/2023-09/The_holistic_approach_report.pdf

social media compared to 63.5% of men.[5] To address this and other barriers, a new telecommunications and ICT framework created a public body to take charge of managing a Universal Development Fund for ICT to guarantee populations living in remote areas access to the internet, as well as finance projects in favour of the development of the country's ICT sector.

5. Over the last five years, the political situation in the DRC has been marked by the first peaceful and democratic transition of power through the election of President Félix Tshisekedi in December 2018.

6. Although there is a decrease in human rights violations and restrictions on democratic space throughout Congolese territory, from January to June 2023 the United Nations Joint Human Rights Office in the DRC documented 116 violations of human rights.[6] Civil society groups have reported a trend of repression in the country, and human rights defenders, journalists and political opponents are exposed to arrest, intimidation, physical violence and murder.[7] In particular, human rights organisations have denounced the state of siege that has been in place in North Kivu and Ituri for more than two years as a measure that systematically restricts human rights and has led to the harassment and imprisonment of journalists, and killing of human rights defenders and political activists.[8]

[5] Kemp, S. (2023, 13 February). Op. cit.
[6] United Nations Joint Human Rights Office Democratic Republic of the Congo. (2023). *Communiqué de presse du BCNUDH sur les principales tendances des violations des droits de l'homme en juin 2023.* https://reliefweb.int/report/democratic-republic-congo/communique-de-presse-du-bcnudh-sur-les-principales-tendances-des-violations-des-droits-de-lhomme-en-juin-2023
[7] https://freedomhouse.org/country/democratic-republic-congo/freedom-world/2023
[8] Amnesty International. (2023, 6 May). RDC. Les autorités doivent lever l'« état de siège » sans plus attendre. https://www.amnesty.org/fr/latest/news/2023/05/drc-authorities-must-lift-state-of-siege-now/

III. UPR THIRD CYCLE RECOMMENDATIONS CONCERNING DIGITAL ISSUES

7. During the third cycle of the UPR, states included digital-related topics in their recommendations to the DRC for the first time.[9]

8. Rudi International and partner organisations advocated for states to include recommendations on guaranteeing the freedom of expression and assembly, both online and offline, and to cease internet disruptions. Additionally, they urged for the adoption of the Law on Telecommunications and ICT, under legislative review at the time. Strengthening citizens' rights to privacy through the establishment of a clear, comprehensive and up-to-date law on privacy and data protection was also emphasised in the recommendations. Furthermore, recommendations called for investments in ICT infrastructure development and skills education.

9. In line with these recommendations, Belgium called on the Congolese government to: "Withdraw all media closure measures and no longer resort to the practice of limiting or cutting off communications systems (such as the internet and SMS), including during moments of tension or popular mobilization". (Recommendation 119.112, page 15.)[10]

10. Austria reiterated the need for the Congolese government to: "Ensure that perpetrators of violations of international humanitarian law and human rights violations, including against journalists, online media professionals, bloggers and human rights defenders, are brought to justice". (Recommendation 119.138, page 17.)[11]

11. Overall, the Congolese government has noted 28 and accepted 239 out of the 267 recommendations received. The recommendations from Belgium and Austria are among those accepted.[12]

[9] Tungali, A. (2019, 11 June). Hitting 'Refresh' on Digital Rights in the DRC — Livestreaming the UPR from Goma. *Medium.* https://medium.com/uproar/streaming-the-upr-from-goma-ff58d752cade
[10] Report of the Working Group on the Universal Periodic Review Democratic Republic of the Congo: https://www.upr-info.org/sites/default/files/documents/2019-09/a_hrc_42_5_drc_en.pdf
[11] Ibid.
[12] Responses to Recommendations, Democratic Republic of the Congo: https://www.upr-info.org/sites/default/files/documents/2019-12/2rps_drc.pdf

12. The Congolese government has taken steps in the direction of updating its ICT-related legal framework over the past five years. Laws were passed in Parliament, and entities and institutions such as the Digital Code, the Telecommunications and ICT Law, and the Agency for Digital Development were created. Strategic documents, including the National Digital Plan, were adopted and developed for the advancement of the technology sector and the promotion of digital rights. It is worth noting that some of these new elements and actions are the result of the recommendations made during the UPR's third cycle on the DRC.

13. There have been no shutdowns or restrictions placed on internet access in the DRC since President Tshisekedi took office in 2019. During the general elections in December 2023, after a commitment from the Ministry of Interior Affairs, internet and communication services remained operational across DRC territory.[13]

14. Nevertheless, Law No. 20/017 of November 2020 on Telecommunications and ICTs (Article 125)[14] stipulates that, for reasons of internal and/or external security, national defence, public order, the interests of the telecommunications service, or for any other reason deemed necessary, the state may suspend, restrict, filter, prohibit or close certain services and applications for a period of time it determines fit. This provision does not adhere to international standards, which state that measures to intentionally prevent or disrupt access to or the dissemination of information online are in violation of international human rights law.[15]

[13] Kinshasa, R. (2023, 19 December). RDC : Peter Kazadi dément la rumeur sur la coupure de la connexion internet le jour de vote. *Politico.* https://www.politico.cd/encontinu/2023/12/19/rdc-peter-kazadi-dement-la-rumeur-sur-la-coupure-de-la-connexion-internet-le-jour-de-vote.html/151567/

[14] Article 125.1. Without prejudice to the fundamental individual or collective rights and freedoms guaranteed by the Constitution and the procedures attached thereto, the state may, for the period 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 shut down certain services and applications, in whole or in part, including the use of the facilities.

[15] Resolution adopted by the Human Rights Council on 1 July 2016: https://digitallibrary.un.org/record/845727/files/A_HRC_RES_32_13-EN.pdf

15. Despite some positive efforts in line with the recommendations of the previous UPR cycle, such as the Law on the Protection of Human Rights Defenders,[16] the expected level of protection for defenders and journalists remains unrealised. As previously stated, there is a trend towards the repression of civic space in the DRC where human rights defenders and journalists are being targeted and exposed to arrest, intimidation, physical violence and murder.[17]

IV. UPR FOURTH CYCLE – HUMAN RIGHTS IN THE DIGITAL CONTEXT IN THE DEMOCRATIC REPUBLIC OF CONGO

Disinformation and hateful speech

1. Article 23 of the DRC Constitution guarantees the right to freedom of expression, information and the freedom of the press "subject to respect for the law, public order and morality". Although the internet is not specifically mentioned in the Constitution, it is understood that all platforms and means of communication are included.

2. In addition to the Constitution, Ordinance Law No. 23/009 of March 2023 sets out the terms and conditions for exercising freedom of the press, and covers freedom of information and broadcasting by radio and television, written press and any other means of communication. This law provides a framework for the exercise of the profession of a journalist or any other person who makes information available to the public online.

3. This ordinance law includes provisions that condemn the dissemination of content that "will likely shock the internet", relating to the glorification of violence among other things (Articles 87.4 and 90.1). Via the Congolese Penal Code of 1940, ordinance law also penalises the

[16] Article 3.1. of the Law on the Protection of Human Rights Defenders. The human rights defender shall freely carry out his activities throughout the national territory in compliance with the laws and regulations of the Republic. As such, he has the right to form and join organisations or associations with other persons.
[17] https://freedomhouse.org/country/democratic-republic-congo/freedom-world/2023

publication, dissemination or reproduction of “false news” (Article 123.1) by any means when carried out in bad faith, resulting in the disturbance of public peace. The Digital Code punishes the propagation (initiation or relaying) of false information pertaining to a person through social networks, computer systems, electronic communication networks or any form of electronic medium (Article 360).[18] However, the Penal Code does not specify how to determine what is considered a “false rumour” or “fake news”, or what the threshold is at which it can be decided that a piece of information is likely to alert, worry or provoke the public against “the established powers”, instead granting discretion to those responsible for enforcing this law.[19]

4. The Digital Code of 2023, among other issues, criminalises the propagation of speech that is likely to lead to or encourage hateful, tribal behaviour and behaviour that is contrary to good life and morals as well as patriotic values (Article 358).[20] Organisations warned that this framework contains sections that enable authorities to criminally prosecute journalists for their work, including for sharing “false news”. Under the Digital code,[21] authorities are granted the power to imprison journalists for sharing information electronically.[22] In April 2023, the Committee to Protect Journalists condemned the arrest and intimidation of journalists accused of spreading rumours. Gustave Bakuka, for example, was accused of “spreading false rumors” in an article he wrote and shared on a WhatsApp group discussing security issues in Kindu.[23]

[18] Article 360 of the Digital Code. Anyone who initiates or relays false information against a person through social networks, computer systems, electronic communication networks or any form of electronic medium shall be punished by penal servitude for a term of one to six months and a fine of 500,000 to one million Congolese francs, or by one of these penalties only.

[19] Analyse du pays : République Démocratique du Congo: https://lj2026.n3cdn1.secureserver.net/wp-content/uploads/2023/04/ANALYSE-DU-PAYS_-Republique-Democratique-du-Congo_Jul22.pdf

[20] Article 358 of the Digital Code. Anyone who initiates an electronic communication that coerces, intimidates, harasses or causes emotional distress to a person, and/or uses a computer system with the aim of encouraging hateful, tribal behaviour and behaviour hostile to good morals and patriotic values shall be punished by penal servitude of one to two years and a fine of 500,000 to 10 million Congolese francs.

[21] Ordonnance- LOI N° 23/010 du 13 Mars 2023 Portant Code du Numerique: https://www.politico.cd/wp-content/uploads/2023/04/04042023-ORDONNANCE-LOI-23-010-DU-13-MARS-PORTANT-CODE-DU-NUMERIQUE-_compressed_compressed.pdf

[22] Committee to Protect Journalists. (2023, 23 May). DRC enacts press law and digital code that criminalize journalism. https://cpj.org/2023/05/drc-enacts-press-law-and-digital-code-that-criminalize-journalism/

[23] Committee to Protect Journalists. (2023, 14 April). DRC authorities detain 2 journalists, threaten another with arrest. https://cpj.org/2023/04/drc-authorities-detain-2-journalists-threaten-another-with-arrest/

5. Legislative responses that contain broad and vague terms are contrary to international human rights standards and the principles of legality, necessity and proportionality. These responses allow arbitrary or discretionary application, resulting in legal uncertainty, and pose serious challenges to the exercise of human rights due to their criminalising effects.[24]

6. For instance, “fake news” laws and provisions such as the ones in the DRC that restrict the media, criminalise and censor legitimate online content, or are used to prosecute journalists are disproportionate and incompatible with international human rights law, and counterproductive to tackling disinformation as they discourage diverse sources of information and undermine trust in public information.[25]

Cybersecurity, cybercrime and data protection

7. To date in the DRC, there is no specific law that deals with cyber-security and cybercrime issues. These areas are currently addressed by frameworks such as the 2020 Telecommunications and ICT framework[26] and the Digital Code of 2023.

8. The Digital Code created the National Cybersecurity Agency (Article 275), a public body placed under the Presidency of the Republic that takes care of all matters relating to cybersecurity and the security of information systems in the country. The Code grants prerogatives to this agency that include the authorisation of the interception and retention of personal data as well as the interception of corres-pondence sent by electronic means for several reasons, including the maintenance of national sovereignty, territorial integrity and national

[24] Lara-Castro, P. (2023). *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks.* Association for Progressive Communications. https://www.apc.org/sites/default/files/gender_considerations_on_cybercrime_0.pdf

[25] Khan, I. (2022, 4 April). In my view: To tackle disinformation, we must uphold freedom of opinion and expression. *The OECD Forum Network*. https://www.oecd-forum.org/posts/in-my-view-to-tackle-disinformation-we-must-uphold-freedom-of-opinion-and-expression-d5b370e1-e96c-4273-82b2-332548c38c9b

[26] LOI N° 20/017 du 25 Novembre 2020 Relative aux Telecommunications et aux Technologies de L'information et de la Communication: https://www.primature.cd/public/wp-content/uploads/2022/04/Loi-N%C2%B020-017-du-25-novembre-relative-aux-Te%CC%81le%CC%81com_08-12-020.pdf

defence, as well as the breach of public order (Articles 323[27] and 324[28]).

9. This agency, like the bodies connected with intelligence services, is under the direct authority of the Presidency of the Republic, and can become a tool of repression used by public authorities. For instance, this agency is not required to obtain judicial authorisation before intercepting data or communications.

10. This contradicts the international legal principles of proportionality, necessity and legality. For example, following the Necessary and Proportionate Principles,[29] national laws should only permit communication surveillance by specified state authorities for legitimate aims that correspond to a predominantly important legal interest necessary in a democratic society. In addition, communications surveillance can only be authorised by a competent, impartial and independent judicial authority.[30]

[27] Article 323 of the Digital Code. The National Cybersecurity Agency authorises: 1. The interception of correspondence sent by means of electronic communications, in accordance with the provisions of this Ordinance Law; 2. The preservation and protection of the integrity and collection, including in real time in accordance with the procedures provided for in Articles 25 *et seq.* of the Code of Criminal Procedure, of data and information on personal data and in Article 273 of this Ordinance Law. The detailed rules for implementing the provisions of this Article shall be specified by regulation.

[28] Article 324 of the Digital Code. The interception operations referred to in this Ordinance Law are authorised by the National Cybersecurity Agency when they are necessary for: 1. The maintenance of national sovereignty, territorial integrity or national defence; 2. The preservation of major foreign policy interests of the Democratic Republic of Congo; 3. The safeguarding of major economic, industrial and scientific interests of the Democratic Republic of Congo; 4. The prevention of terrorism, collective violence likely to seriously undermine public order, or organised crime and delinquency.

[29] The International Principles on the Application of Human Rights to Communication Surveillance (or the 13 Necessary and Proportionate Principles) explain how international human rights law applies in the context of communication surveillance. The principles are firmly rooted in established international human rights law and jurisprudence. For more, see Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance: https://necessaryandproportionate.org/principles/

[30] Ibid.

11. The Digital Code also defines cybercrime offences as a set of specific criminal offences whose commission is facilitated or linked to the use of technologies. As stated above, the Code punishes the dissemination of tribalistic, racist and xenophobic content through an electronic system (Article 356),[31] harassment through an electronic system (Article 358),[32] or the propagation (initiation or relaying) of false information pertaining to a person through electronic means or social networks (Article 360).[33]

12. Section 360 of the Digital Code imposes penalties of up to six months in prison or a fine of one million francs (nearly USD 430) for journalists relaying false information electronically. Additionally, under Section 358, penalties of up to two years in prison and a fine of 10 million francs (nearly USD 4,330) apply to electronic communications deemed coercive, intimidating or provocative, thus potentially encouraging behaviour that is contrary to moral and patriotic values. These provisions also pose risks for human rights activists and defenders who may be unfairly targeted under ambiguous terms like the "disturbance of tranquillity".

13. A secure internet is best achieved through a rights-based approach and must be centred on the security of people. While both cyber-security and cybercrime pertain to the security of computer systems, cybersecurity provides a different approach to that of cybercrime and should be differentiated from it.[34]

14. Cybercrime legislation should be used solely to address offences that require the use of a computer system – so-called "cyber-dependent" crimes. The extension of cybercrime legislation to cover traditional offences committed using a computer or "cyber-enabled" crimes is unnecessary and risky for several human rights.[35]

---

[31] Article 356 of the Congolese Digital Code. Anyone who intentionally creates, downloads, disseminates or makes available to the public through a computer system writings, content, messages, photos, sounds, videos, drawings or any other representation of ideas or theories of a racist, tribalist or xenophobic nature within the meaning of this Ordinance Law, and whose actions come under the purview of Ordinance Law No. 66-342 of 7 June 1966 on the suppression of racism and tribalism, shall be punished by penal servitude from one month to two years and a fine of one million to 10 million Congolese francs, or by one of these penalties only.

[32] Article 358 of the Digital Code. Op. cit.

[33] Article 360 of the Digital Code. Op. cit.

[34] Knodel, M., Degezelle, W., & Kumar, S. (2023, 20 January). Mythbusting: Cybercrime versus Cybersecurity. *Tech Policy Press.* https://www.techpolicy.press/mythbusting-cybercrime-versus-cybersecurity/

[35] Lara-Castro, P. (2023). Op. cit.

15. Definitions of cybercrime should be in line with human rights standards. Cybercrime legislation characterised by broad and vague definitions not only ends up being ineffective and disproportionate, but violates human rights by criminalising the online activities of individuals and organisations and by being used as a legal tool to silence critical voices and restrict civic space.[36]

16. Organisations have been reporting a concerning trend wherein, for their critique of governmental actions, journalists and individuals are facing criminal charges of defamation, the dissemination of "false information" and the publication of rumours which, although unsubstantiated, have purportedly led to public alarm.[37]

17. Cybersecurity and cybercrime frameworks must encompass complementary initiatives and approaches such as comprehensive data protection laws. The Digital Code, which incorporates provisions on privacy and data protection in line with the recommendations of Rudi International and partner organisations in the previous UPR cycle, serves as a basis for specific legislation on personal data protection that is in line with international standards.

[36] Ibid.
[37] Hubbard, D. (2023). Democratic Republic of Congo (DRC). In *Impact of Cybercrime and Cyber Security Laws on Media Freedom and Digital Rights*. Advancing Rights in Southern Africa. https://internews.org/wp-content/uploads/2023/11/ARISA-IEA-CHAPTER-6-DRC.pdf

V. UPR FOURTH CYCLE – MEDIA FREEDOM AND CIVIC SPACE

18. Although media freedom is constitutionally guaranteed in the DRC, and despite improvements in the country's legal framework, journalists continue to face threats, intimidation, arrests, criminal defamation suits, detentions, arbitrary arrests and physical attacks in the course of their work.[38] Reporters Without Borders, for example, noted at least 123 cases of arbitrary arrest, three killings and two enforced disappearances of journalists in the last five years.[39]

19. The ordinance law governing the exercise of freedom of the press did not decriminalise press offences. As a result, it is still possible for any journalist to have to report before the courts for acts committed in the performance of their duties. These include acts punishable by deprivation of liberty, such as defamation or insult.

20. Civil society groups have reported a rising trend in repression in the country.[40] Many challenges endanger the work of human rights defenders. Killings, extrajudicial executions, enforced disappearances, torture, cruel, inhuman or degrading treatment, arbitrary detention, physical and digital threats, harassment, stigmatisation, restrictions on appearing before international bodies, and administrative restrictions

[38] According to Journaliste en Danger, two journalists from Radio Canal Révélation based in Bunia, Ituri Province, were subjected to intimidation and death threats by individuals claiming to belong to the armed group Force Patriotique et Intégrationniste du Congo, also known as Chini ya Kilima. Since 8 January 2021, Freddy Upar and Nicolas Synthe Awacang'o have been receiving threatening text messages and telephone calls from armed militia members accusing the journalists of siding with the DRC's armed forces. Please see: CIVICUS. (2021, 10 February). Rights groups: Increase in violations in 2020. *CIVICUS Monitor*. https://monitor.civicus.org/explore/Rights-organisations-increase-human-rights-violations-in-2020/
On 14 February 2023, the armed rebel group M23, which controls parts of Rutshuru Territory, North Kivu Province, summoned the heads of broadcast media operating in the area, accusing them of "inciting hatred" and ordering them to change their editorial line. M23 ordered the media outlets to broadcast a weekly programme, led by an M23 member, and prohibited the retransmission of a popular radio station and programme produced in Goma by journalists who have fled the area. Please see: CIVICUS Monitor. (2023). *People Power Under Attack 2023.* https://civicusmonitor.contentfiles.net/media/documents/GlobalFindings2023.pdf
Another emblematic case was the arrest of journalist Stanis Bujakera in September 2023 against the backdrop of an article published in *Jeune Afrique* on the death of national member of parliament and opposition leader Chérubin Okende, incriminating the regime in power at the time. This arrest is considered arbitrary by human rights organisations.

[39] Reporters Sans Frontières. (2023, 20 December). RDC : Les journalistes doivent pouvoir couvrir l'élection présidentielle en sécurité et sans restriction. https://rsf.org/fr/rdc-les-journalistes-doivent-pouvoir-couvrir-l-élection-présidentielle-en-sécurité-et-sans

[40] https://freedomhouse.org/country/democratic-republic-congo/freedom-world/2023

on the holding of demonstrations are among the most widespread violations against human rights defenders.[41]

21. The Law on the Protection of Human Rights Defenders[42] is a framework that addresses the rights, duties and responsibilities of human rights defenders and the obligations of the state towards them, as well as the mechanisms for their protection. This framework is the result of a long and hard advocacy process undertaken by international and national civil society organisations in the DRC over the past decade.

22. While this law seeks to protect human rights defenders from arbitrary arrest during their activities or because of their opinions (Articles 19 and 20) and provides for a system of punishment for the perpetrators of violations against human rights defenders (Articles 21 to 28), according to several reports by civil society, the government uses arbitrary arrests and detentions to muzzle dissenting voices. Cases of arrest and pre-trial detention are rife in the DRC. Criminalisation is intended to put pressure on defenders and discourage them from carrying out activities to promote and protect fundamental rights and freedoms.[43]

23. For instance, this legal framework obliges individual workers to register with the National Human Rights Commission and to submit an annual report on their activities to the same.[44] Many activists are reluctant to register with the Commission to receive an identification number or complete the mandatory annual report submission for fear that they will

[41] Agir ensemble pour les droits humains. (2023). *RD-Congo : état des lieux de la criminalisation des défenseur·se·s des droits humains dans un pays en crise (2020-2022).* https://agir-ensemble-droits-humains.org/wp-content/uploads/2022/09/Rapport-RD-Congo-AEDH-web.pdf

[42] Article 3.1. of the Law on the Protection of Human Rights Defenders. Op. cit.

[43] Agir ensemble pour les droits humains. (2023). Op. cit.
In 2021, several human rights activists from the citizens' movement Lutte pour le Changement (LUCHA) were arrested and severely punished by the political and judicial authorities in the DRC following their activism against the establishment of a state of siege regime in North Kivu and Ituri. Very heavy sentences were handed down to some of them.
So-called "informal" organisations such as LUCHA and Filimbi have always endured harsh treatment from the authorities. They have been, in the past, labelled as terrorist groups by some. Only a few authorities have been able to approach the members of these organisations. Rudi International has conducted research on them in the past, resulting in recommendations to the Congolese government to review national legislation so that it expressly recognises the existence of informal organisations.

[44] Article 11. The human rights defender [...] submits an annual report on his activities to the National Human Rights Commission, with a copy for information to the Minister of Justice and the minister responsible for human rights, as well as to the General Secretariat attached to the latter. However, sending the report and the allocation of an identification number do not place the human rights defender under the supervision of the National Human Rights Commission.

be monitored. These provisions also restrict freedom of expression and association, as they implicitly deny activists working individually or in informal organisations the status of human rights defenders. This measure is contrary to the broad definition of human rights defenders in the United Nations Declaration on Human Rights Defenders, which recognises that a human rights defender is "anyone working for the protection of human rights, regardless of the duration of their work".[45] Under this framework, human rights defenders can face up to two years in prison if the information they publish is deemed defamatory, insulting or slanderous (Article 28).[46]

24. Human rights defenders are individuals or groups that engage in protecting and promoting human rights. The work of defenders is crucial to protecting rights and promoting gender inclusion, equality and diversity, as well as upholding democracy and the rule of law, which is essential to the flourishing of society.[47]

25. The DRC government should refrain from enacting laws and implementing policies that unduly restrict civic space, and has to make sure that these laws and policies are consistent with a state's obligations under international human rights law.

[45] Kame, A. E. (2023, 23 October). DRC adopts national law to protect, promote rights of defenders. *International Service for Human Rights.* https://ishr.ch/latest-updates/the-drc-adopts-a-national-law-to-protect-and-promote-the-rights-of-human-rights-defenders/

[46] Article 28 of the Law on the Protection and Accountability of Human Rights Defenders in the DRC. Without prejudice to the provisions of the Congolese Penal Code, a human rights defender who discloses defamatory, insulting or slanderous information shall be punished by penal servitude from six months to two years or a fine of 500,000 to two million Congolese francs, or by one of these penalties only.

[47] Freedom Online Coalition. (2019). FOC Joint Statement on Defending Civic Space Online. https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-Defending-Civic-Space-Online.pdf

Technology-facilitated gender-based violence against women journalists, politicians and rights defenders

26. Despite the Constitution affirming the protection of women against all forms of violence, women, including journalists, face increasing intimidation and death threats for exercising their freedom of expression and airing their opinion publicly.[48] Although there is still limited research on the issue and these cases are often not reported due to the social norms still in place in Congolese society, gender-based violence (GBV) is, according to reports, a pressing problem in the DRC. In a workshop in December 2023, women journalists, media professionals and women human rights defenders expressed concern about the insecurity that women experience online, more specifically through social networks. Participants highlighted technology-facilitated gender-based violence (TFGBV) as a growing threat, including harassment, cyberbullying, blackmail, hacking and identity theft, among other types of violence.[49]

27. According to research, women journalists and rights defenders noted that what happens offline actually translates to the online world and vice versa, and that the offline abuse of women persists online, but the latter is not taken as seriously as the former.[50]

28. To address this, the government has put in place mechanisms such as accountability frameworks and national protocols for case management and a database of incidents. However, these protocols and mechanisms mainly respond to offline GBV.[51] Ordinance Law No. 23/023 of September 2023 amends and supplements the Congolese Penal Code and the Code of Criminal Procedure to address GBV perpetrated through communication or information networks, establishing penalties for these acts and making referral to the courts

[48] These are usually acts of gender-based intimidation and stigmatisation, such as: the harassment of victims or witnesses of rape as well as their relatives or family members; threatening to publish information on social media or other platforms on the internet that is likely to harm a person's honour or reputation because of their gender; acts of blackmail by threatening to reveal or impute facts likely to harm a person's honour or reputation, because of his or her sex, etc. For more, see: Ryakitimbo, R., Nkhowani, B., & Mwimbi, J. (2023). Op. cit.

[49] Ibandula, C. (2023, 14 December). RDC : Le gouvernement congolais appelé à mettre en place les mesures d'application de la loi portant le code numérique. *Digital Congo.* https://www.digitalcongo.net/article/rdc-le-gouvernement-congolais-appele-a-mettre-en-place-les-mesures-d-application-de-la-loi-portant-le-code-numerique/

[50] Ryakitimbo, R., Nkhowani, B., & Mwimbi, J. (2023). Op. cit.

[51] Ibid.

more accessible.[52] With the amendment of the Code, the state bears the cost of said referral through the national budget, and the right to free legal assistance at all levels is established (Article 7b).[53]

29. From conversations and consultations conducted by Rudi International in preparation of this submission, we learnt that cases of sextortion, harassment and other forms of online threats discourage many women human rights defenders (WHRDs) from continuing to use the internet in their daily work. These forms of attacks often result in the publication of intimate content with the aim of discrediting the victim or extorting them. Also, some women activists continue to suffer misogynistic attacks when they speak out on public platforms.

[52] Article 147 of the new penal code in its subparagraphs p, u and w provides for heavy and severe penalties for some offences committed online and based on the gender of the victims. These fines and prison sentences range from six months to 10 years and from 500,000 to 10 million Congolese francs.
Ordonnance-LOI N°23/023 du 11 Septembre 2023 Modifiant et Completant le Decret du 30 Janvier 1940 Portant Code Penal Congolais:Articles 147.p., u., and w., of the Ordinance-Law No. 23/023 of 11 September 2023 amending and supplementing the Decree of 30 January 1940 on the Criminal Code, available at https://usercontent.one/wp/www.sofepadirdc.org/wp-content/uploads/2023/09/ORDONNANCE-LOI-PORTANT-CODE-DE-PENAL-CONGOLAIS.pdf?media=1692206460: Article 147p. The offence of gender-based intimidation and stigmatisation covers any act of harassment, reprisal or threat of reprisal committed intentionally against a person, their relatives, witnesses or whistleblowers, with the aim of hindering the care of victims and the prosecution of perpetrators. Any person found guilty of the offence defined in the preceding paragraph shall be punished by imprisonment for a term of six to 24 months and a fine of 500,000 to one million Congolese francs.
- Article 174u. Anyone who obtains and/or maliciously publishes or threatens to publish, directly or through an intermediary, information, regardless of the process used, on communication or information networks and other internet platforms likely to harm the honour or reputation of a person because of his or her gender shall be punished by three to five years' penal servitude and a fine of five million to ten million Congolese francs or one of these penalties only. In the event of a repeat offence, the offender shall be punished by five to 10 years' imprisonment and a fine of ten million Congolese francs.
- Article 174w. Blackmail is the act of obtaining, against the will of a person, either a signature, an undertaking or a waiver, or the revelation of a secret, or the handing over of funds, securities or any other property, or a favour of a sexual nature, by threatening to reveal or impute facts likely to harm his or her honour or reputation on account of his or her sex. Whoever commits blackmail shall be punished by one to three years' imprisonment and a fine of 500,000 to one million Congolese francs.

The state bears the cost of the referral through the national budget. The right to free legal assistance at all levels is enshrined in Article 7b, and the payment of costs by the national budget is confirmed by Article 122 bis.

[53] Article 7b. Without prejudice to the right to legal aid by counsel of his/her choice, the victim of gender-based violence shall have the right to free assistance at all stages of the proceedings. Ordonnance-LOI N° 23/024 du 11 Septembre 2023 Modifiant et Completant le Decret du 06 Aout 1959 Portant Code de Procedure Penale: Ordinance-Law No. 23/023 of 11 September 2023 amending and supplementing the Decree of 6 August 1959 on the Code of Procedure, available at https://usercontent.one/wp/www.sofepadirdc.org/wp-content/uploads/2023/09/ORDONNANCE-LOI-PORTANT-CODE-DE-PROCEDURE-PENALE.pdf?media=1692206460 . Article 7b. Without prejudice to the right to legal aid by counsel of his/her choice, the victim of gender-based violence shall have the right to free assistance at all stages of the proceedings.

30. WHRDs from Congo use social media, in particular Facebook, for advocacy and to engage in collective activism on GBV and sexual reproductive health issues for women. However, research and interviews carried out in the context of this submission point out that WHRDs suffer from a lack of training on how to use digital platforms. A lack of digital knowledge and skills among some defenders makes their work difficult and renders them more vulnerable than men defenders.[54]

31. For women politicians in the DRC, social media platforms are not only a means to share their work but are also avenues to advocate for pertinent issues and push for greater women's participation in politics.[55] However, cases of harassment, hate speech, targeted comments, abusive content and trolling, and other forms of online violence against women politicians or aspiring politicians are also rife in the country, especially during election periods.[56]

32. Similarly, women journalists revealed during our research that they do not often use online platforms because of the misogynistic attacks they experience online. One key challenge faced by respondents in a study focused on Congo and other African francophone countries (both WHRDs and women journalists) was the use of gender and sexuality stereotypes to harm them online.[57]

33. The aforementioned study, focused on women journalists and WHRDs, revealed that there is a lack of awareness in the DRC of the laws in Congo that protect individuals against TFGBV. Congolese journalists and WHRDs that participated in this study said that they do not know how to apply these laws and policies when they are harassed online. For instance, there is no clear indication of where one can report cases and to whom. They further mentioned the lack of enforcement of these frameworks and the need for WHRDs and journalists to increase their knowledge of these laws and policies.[58]

[54] Nyamwire, B., Metial, K., & Siba Yahaya, M. (2022). *A Dark Place for Women Journalists and Women Human Rights Defenders: Documenting the Experiences of Online Violence in Anglo and Francophone Countries.* Pollicy. https://pollicy.org/resource/a-dark-place-for-women-journalists/
[55] Ryakitimbo, R., Nkhowani, B., & Mwimbi, J. (2023). Op. cit.
[56] Zigbia Tayoro, A. (2023, 23 August). La MONUSCO forme les femmes politiques à la sécurité numérique pour faire face au cyber-harcèlement en période électorale. *MONUSCO.* https://monusco.unmissions.org/la-monusco-forme-les-femmes-politiques-à-la-sécurité-numérique-pour-faire-face-au-cyber-harcèlement
[57] Nyamwire, B., Metial, K., & Siba Yahaya, M. (2022). Op. cit.
[58] Nyamwire, B., Metial, K., & Siba Yahaya, M. (2022). Op. cit.

34. Women journalists and rights defenders who work in conflict areas find that their jobs make them a target for abuse both online and offline. They also face digital gap challenges such as unreliable power and connection, which hinder their right to fully utilise digital platforms. This gap is more pronounced for LGBTQIA+ communities, who are not only stigmatised but are also easily victimised on various platforms. These communities are not exempt from GBV, both online and offline, being forced to hide from harassment, attacks and hatred.[59]

VII. FOURTH CYCLE RECOMMENDATIONS TO THE CONGOLESE GOVERNMENT

35. Over the past five years, the Congolese Government has made progress in its ICT-related legislation. However, more efforts need to be made through a holistic approach to ensure the protection of media freedom and civic space, in particular for journalists, women and human rights defenders.

36. Hence, we recommend that the Government of DRC take the following measures.

Disinformation and hateful speech

37. Any measure to address disinformation and hateful speech must be in accordance with international law, including human rights law and the principles of lawfulness, legitimacy, necessity and proportionality.

38. In line with the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019,[60] the government should amend laws addressing “fake news” and hateful speech to bring them in line with international human rights standards. The government should ensure that they do not pose risks to the exercise of human rights, do not restrict the media and criminalise legitimate content, and are not used to prosecute journalists.

[59] Ryakitimbo, R., Nkhowani, B., & Mwimbi, J. (2023). Op. cit.
[60] See Principle 22 on Criminal Measures: https://achpr.au.int/en/node/902

39. The government should refrain from stifling freedom of opinion and expression under the guise of countering disinformation or “fake news”, including intimidating journalists and interfering with their ability to operate freely.[61]

40. The government should promote a healthy information system that includes robust access to public information, plural, accessible and diverse media contexts, independent journalism and the possibility of expressing ideas safely.

41. We also encourage the government to implement holistic approaches to tackle disinformation and hateful speech online, such as implementing digital and media literacy programmes. These programmes could be embedded in the regular education system curricula.[62]

42. Along with digital literacy, the government should enhance efforts towards digital inclusion. We call on the DRC government to accelerate the rollout of the Universal Service Fund to ensure access to the internet in remote regions and work towards addressing existing digital gaps in the country, including through the adoption of community-centred responses to digital inclusion, such as community networks.

Cybersecurity, cybercrime and data protection

43. Communications surveillance should adhere to international human rights law and standards. Following the Necessary and Proportionate Principles, national laws should only permit communications surveillance by specified state authorities to achieve a legitimate aim that is necessary in a democratic society. Determinations related to communications surveillance must be made by a competent and independent judicial authority.[63]

44. The extension of cybercrime legislation to cover “cyber-enabled” crimes is unnecessary and risky for human rights. The government should actively narrow the range of issues covered under cybercrime

[61] Freedom Online Coalition. (2019). Op. cit.
[62] Association for Progressive Communications. (2021). *APC policy explainer: Disinformation*. https://www.apc.org/en/pubs/apc-policy-explainer-disinformation
[63] Necessary & Proportionate. Op. cit.

in accordance with human rights standards.[64] Cybercrime legislation should be used only for addressing "cyber-dependent" crimes.

45. Cybersecurity policies should aim to establish a framework rather than isolated laws, and should be responsive to the complex, differentiated and intersectional needs of people based on gender, sexual orientation, race, religion, among other factors. For this, both cybersecurity and cybercrime frameworks should consider the views of and impacts on historically excluded communities and groups.

46. Cybersecurity and cybercrime frameworks must encompass complementary initiatives and approaches such as implementing a comprehensive data protection law. The Congolese government should establish safeguards that apply to the collection, handling and disclosure of personal information obtained using communication technologies to uphold universal human rights and the rule of law.[65]

47. The government must implement awareness-raising and training programmes in cybersecurity for the public, private, academic and civil society sectors to equip them with the skills and knowledge necessary to respond to cybersecurity threats.[66]

Media freedom and civic space

48. In line with the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa,[67] the Congolese government should "review all criminal restrictions of content to ensure that they are justifiable and compatible with international human rights law and standards".[68]

49. The government should refrain from restricting freedom of expression online or offline except in accordance with the requirements of Articles 19.3 and 20.2 of the International Covenant on Civil and Political

[64] Lara-Castro, P. (2023). Op. cit.
[65] Joint Statement Presented at the 54th Session of the UN Human Rights Council on the Heightened Risks Associated with Surveillance Technologies and the Importance of Safeguards in the Use of these Tools: https://freedomonlinecoalition.com/joint-statement-heightened-risks-associated-with-surveillance-technologies-and-the-importance-of-safeguards-in-the-use-of-these-tools/
[66] Nyamwire, B., Metial, K., & Siba Yahaya, M. (2022). Op. cit.
[67] Declaration of Principles on Freedom of Expression and Access to Information in Africa, Principle 22: https://achpr.au.int/en/node/902
[68] Ibid.

Rights, strictly and narrowly construed. Criminal law should be used only in very exceptional and the most egregious circumstances of incitement to violence, hatred or discrimination.

50. The government should ensure the safety of journalists online and offline. Ending impunity for threats, intimidation, harassment, attacks and killings of journalists, including women journalists, bloggers, cartoonists and human rights defenders, is key to restoring confidence in the public sphere as a safe place for democratic deliberations.

51. Current legislation should evolve in this direction, to protect all human rights defenders online and offline, in addition to granting special protection to WHRDs.

52. The government should adopt a clear and public stance condemning the regressive nature of the use of internet restrictions and other forms of censorship and surveillance. Exceptions contained in laws and other government measures should be clear and unambiguous and in accordance with international human rights standards.

53. The government should avoid an overreliance on criminal law solutions and refrain from using national security, cybercrime, cybersecurity and related laws to unduly limit the ability of human rights defenders to exercise their human rights. Any such legislation, new or existing, should be evaluated against potential adverse effects on human rights.[69]

54. The government should stop criminalising human rights activists and journalists as a way to discourage them from doing their jobs. To encourage their work and the promotion of civil liberties, the arbitrary detention of human rights defenders in the DRC should cease.

55. Authorities should make more efforts to set up law enforcement mechanisms and finalise institutional reforms to protect civic space and guarantee freedom of association.

[69] Freedom Online Coalition. (2019). Op. cit.

Technology-facilitated gender-based-violence, women journalists and defenders

56. We encourage the government to take a holistic approach when developing solutions that address online and TFGBV by factoring in cultural practices and structural and systemic causes.

57. The Congolese government should adopt measures and policies to prohibit, investigate and prosecute online GBV. It should ensure that existing laws on GBV include aspects of technology-facilitated violence, and should engage with specialists in TFGBV for this purpose, including civil society organisations, survivors and academics.

58. Any legislative responses to tackle this issue should be in line with international human rights standards. Legal frameworks should adequately protect women's freedom of expression, privacy and freedom from violence. Any restrictions to freedom of expression as a response to GBV must be necessary and proportionate, should not be overly broad or vague in terms of what speech is restricted and should not over penalise.

59. The government should create awareness on existing legal frameworks that protect women from online GBV. Raising awareness on existing laws and policies will educate women about these laws, and encourage them to use and advocate for the use of them to combat online and TFGBV.

60. The government should implement regular public campaigns to raise awareness of TFGBV by ensuring a broader understanding of TFGBV and its impact while highlighting key issues around digital security and safety. For this, the government can collaborate with academia and civil society organisations.[70]

61. The government should work with civil society organisations to deepen the attention law enforcement authorities pay to TFGBV through gender-sensitive awareness initiatives. It should educate public

[70] Suzie Dunn, Tracy Vaillancourt, and Heather Brittain, "Supporting Safer Digital Spaces," The Centre for International Governance Innovation (CIGI), 2023. https://www.cigionline.org/static/documents/SaferInternet_Special_Report.pdf

officials, including security forces and law enforcement personnel, on women journalists' and WHRDs' right to carry out their work free of TFGBV.

62. The government should provide measures for redress and reparation for survivors of online and technology-facilitated violence. Such measures should include forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic and material, individual and collective, depending on the circumstances and the preferences of the victim.[71]

63. The government should condemn attacks on WHRDs and acknowledge their work as legitimate and essential for democratic societies, and refrain from using language that stigmatises, abuses, disparages or discriminates against them. It should ensure that law enforcement personnel, government officials and the judiciary receive appropriate training relating to the work and legitimacy of WHRDs and the gendered impact of violations against them. It should also increase or commence awareness raising programmes on the rights and roles of WHRDs.

[71] Feminist Internet Research Network. (2023, 24 August). Policy Recommendations from FIRN Research. *GenderIT*. https://www.genderit.org/articles/policy-recommendations-firn-research