Universal Periodic Review – 51st session

Joint stakeholder report: Human rights in the digital context in Rwanda

The Association for Progressive Communications (APC), an organisation in consultative status with ECOSOC, advocates the strategic use of information and communications technologies (ICTs) to advance human rights. The APC network has 73 organisational members and 44 associates active in 74 countries.

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

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, funded by the UK's Department for International Development (DfID). CIPESA focuses on decision making that facilitates the use of ICT in support of good governance, human rights and livelihoods. CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFiD, which cited the lack of easy, affordable and timely access to information about ICT-related issues and processes as a key barrier to effective and inclusive ICT policy making in Africa. As such, CIPESA's work responds to the shortage of information, resources and actors consistently working at the nexus of technology, human rights and society.

Website: https://cipesa.org

I. Introduction

1. This stakeholder report focuses on key issues relating to human rights in the digital context in Rwanda, including digital connectivity and inclusion, freedom of speech and expression online, online surveillance, transnational repression and right to privacy and technology-facilitated gender-based violence (TFGBV). This report draws on a desk review and on inputs received during a stakeholder consultation on digital rights in Rwanda. Another report by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) provides additional input on freedom of expression, information and content censorship, digital inclusion and privacy.
2. This review marks the fourth cycle for Rwanda in the Universal Periodic Review (UPR) mechanism. During the third cycle, Rwanda demonstrated the importance it places on issues relating to freedom of speech and expression and freedom of the press, receiving 32 recommendations related to these issues, including 24 relating to free speech and expression (with a focus on the need to revise legislative provisions that unduly restrict free speech) and 17 recommendations relating to the protection of journalists and human rights defenders from attacks and intimidation.[1]

II. CONTEXT OF THE SITUATION OF HUMAN RIGHTS ONLINE IN RWANDA

3. Rwanda has made progress in expanding its digital infrastructure. Access to information and communication technologies (ICTs) has improved significantly in recent years.[2] However, the situation of human rights online in Rwanda has deteriorated since the last UPR review in 2021, particularly in the lead-up to the general elections held in July 2024.[3] Incumbent President Paul Kagame's bid for re-election for a fourth term was accompanied by heightened government authoritarianism and censorship of online criticism.[4] The Rwandan Patriotic Front (RPF), led by President Kagame, which has been in power since ousting forces responsible for the 1994 genocide, was elected for a fourth term in July 2024 with 99.17% of the vote. While the RPF regime has provided stability and economic growth for Rwanda, it has suppressed political dissent through tactics such as arbitrary detention, torture and suspected assassinations of exiled dissidents.[5]
4. Violations of user rights, strict censorship, increased surveillance and infrastructure limitations have contributed to Rwanda still being declared as "Not Free" by Freedom House, which gave Rwanda a score of 36/100 in 2024,[6] two points down from its 2021 score of 38/100.[7]

---

1. Human Rights Council. (2021, 25 March). *Report of the Working Group on the Universal Periodic Review: Rwanda*. A/HRC/47/14. https://docs.un.org/en/A/HRC/47/14
2. Paradigm Initiative. (2025). *Digital Rights and Inclusion in Africa: LONDA 2024*. https://paradigmhq.org/wp-content/uploads/2025/06/Londa-2024-1.pdf
3. Freedom House. (2024). *Freedom on the Net 2024: Rwanda*. https://freedomhouse.org/country/rwanda/freedom-net/2024
4. Reporters Without Borders. (2025). *Rwanda*. https://rsf.org/en/country/rwanda
5. Freedom House. (2024). Op. cit.
6. Ibid.
7. Ibid.

III. DIGITAL CONNECTIVITY AND INCLUSION

5. Rwanda's digital infrastructure expansion in recent years has been impressive, but its internet penetration rate remains low, with 4.93 million internet users reported in January 2025, which translates to an internet penetration rate of 34.2% at the start of 2025.[8]
6. Relative to other African countries, Rwanda has strong foundations to make digital access affordable, but there is gender imbalance in internet access and use.[9] DataReportal figures indicate that of 1.3 million active social media user identities in January 2025, only 38.2% were female.[10] In a 2021 study commissioned by APC, women cited price and lack of appropriate devices as the main reasons for not using the internet.[11] These challenges affect women more due to fundamental gender disparities, particularly in education and income.[12]
7. Rwanda's national ID with a unique identifier number not only satisfies daily identification needs, it is also becoming popularly used as a key to access services and conduct transactions electronically. However, there is a need for an effective legal and institutional framework to regulate current and future uses of the national ID, especially online.[13]

IV. FREEDOM OF SPEECH AND EXPRESSION ONLINE

8. Despite constitutional protections for freedom of expression, there is a continued clampdown on real or perceived opposition to government policy.[14] Contrary to the recommendations received during the third cycle of the UPR, Rwandan laws still contain provisions that unduly restrict free speech and expression, including the following articles of the 2018 Penal Code, which stipulate both fines and imprisonment as sanctions:[15]
    - Article 157 prescribes up to one year in prison for dissemination of edited or modified words or images without indicating they have been modified.
    - Article 164 prescribes up to seven years imprisonment for using "speech, writing or any other act" to instigate divisions among people or cause civil unrest on the basis of discrimination.
    - Article 194 prescribes up to 10 years imprisonment for spreading false information or harmful propaganda with intent to cause hostile international opinion or "public disaffection" against the government.

---

8. Kemp, S. (2025, 3 March). Digital 2025: Rwanda. *DataReportal*. https://datareportal.com/reports/digital-2025-rwanda
9. Research ICT Africa. (2021). *Gender norms, gendered work and intersectional digital inequalities in Rwanda*. https://www.apc.org/en/pubs/gender-norms-gendered-work-and-intersectional-digital-inequalities-rwanda
10. Kemp, S. (2025, 3 March). Op. cit.
11. Research ICT Africa. (2021). Op. cit.
12. Ibid.
13. Binda, E. M. (2021). *Digital identity in Rwanda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa*. Research ICT Africa. https://researchictafrica.net/publication/digital-identity-in-rwanda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/
14. Paradigm Initiative. (2025). Op. cit.
15. Human Rights Council. (2021, 25 March). Op. cit., paras. 134.50, 134.53, 134.55, 134.57, 134.58, 135.40, 136.31, 136.32, 136.33, 136.34, 136.35, 136.37, 136.39, 136.41, 136.43, 136.44, 136.45.

- Article 233 prescribes up to two years imprisonment for humiliating "national authorities and persons in charge of public service" including through verbal gestures or threats, in writing or through cartoons. These penalties are doubled if the offence takes place during a parliamentary session or if it is directed at any top-ranking authorities.
- Article 253 criminalises the refusal to answer "questions by intelligence or security officers in the exercise of their duties" or deliberately providing false answers to such questions. It effectively forces journalists and bloggers to disclose their sources or face a penalty of up to six months imprisonment.

9. The government uses these laws to target journalists and human rights defenders. Political commentator Aimable Karasira was arrested in May 2021 for allegedly inciting division and public disorder through social media comments.[16] He remains in detention and his trial was still ongoing as of June 2025.[17] In September 2021, YouTuber Yvonne Idamange, who published content critical of the Kagame government, was convicted under article 194 and sentenced to 15 years imprisonment.[18] In late 2021, eight members of the opposition party Development and Liberty for All (DALFA-Umurinzi) were arrested for allegedly distributing a book promoting non-violent resistance against authoritarianism. Also arrested was journalist Théoneste Nsengimana, who was planning to cover the event. Their trial is ongoing.[19] In December 2022, Theophile Ntirutwa, spokesperson of the DALFA-Umurinzi, was sentenced to seven years in prison for allegedly tarnishing the country's image.[20]
10. Rwandan reporter John Williams Ntwali, a leading investigative journalist and editor of the newspaper The Chronicles, who was regularly threatened due to his work reporting human rights abuses in Rwanda, died in January 2023 under suspicious circumstances.[21] The matter was closed after a hasty trial behind closed doors[22] and no independent investigation was conducted despite appeals from civil society organisations and press

16. Voice of America. (2025, 13 January). Rwandan court orders Aimable Karasira to begin defense. *Voice of America*. https://www.radiyoyacuvoa.com/a/7934984.html
17. Committee to Protect Journalists. (2024). *Aimable Karasira Uzaramba*. https://cpj.org/data/people/aimable-karasira-uzaramba/; KT Press. (2025, 5 June). Aimable Karasira Defends Himself in Court: "I Was Just Expressing My Views." *KT Press*. https://www.ktpress.rw/2025/06/aimable-karasira-defends-himself-in-court-i-was-just-expressing-my-views/
18. AFP. (2021, 1 October). Rwandan YouTuber jailed for 15 years after anti-govt posts. *The East African*. https://www.theeastafrican.co.ke/tea/news/east-africa/rwandan-youtuber-jailed-for-15-years-3568970; Rédaction Africanews. (2021, 31 January). Rwandan govt critic on YouTube sentenced to 15 years. *Africanews*. https://www.africanews.com/2021/10/01/rwandan-govt-critic-on-youtube-sentenced-to-15-years/; The Coalition for Women in Journalism. (2021, 1 October). Rwanda: CFWIJ is Concerned At Yvonne Idamange's Conviction. https://www.womeninjournalism.org/threats-all/rwanda-yvonne-idamanges-conviction
19. Jimoh, A. .UN Special Rapporteur on Human Rights Defenders, et al. (2024, 3 April). Rwanda: criminal prosecution and detention of journalists and human rights defenders Théoneste Nsengimana and Dieudonné Niyonsenga (joint communication). https://srdefenders.org/rwanda-criminal-prosecution-and-detention-of-journalists-and-human-rights-defenders-theoneste-nsengimana-and-dieudonne-niyonsenga-joint-communication/; Amnesty International. (2024, 5 December). Rwanda: Authorities must immediately release detained journalist and members of political op-position. https://www.amnesty.org/en/latest/news/2024/12/rwanda-authorities-must-immediately-release-detained-journalist-and-members-of-political-opposition/; Paradigm Initiative. (2025). Op. cit.
20. Human Rights Watch. (2023, 18 January). Politician Convicted for Harming Rwanda's Image. https://www.hrw.org/news/2023/01/18/politician-convicted-harming-rwandas-image
21. Andrzejewski, C. (2024, 28 May). Collision course: An investigation into the death of a journalist hated by Rwandan authorities. *Forbidden Stories*. https://forbiddenstories.org/collision-course-an-investigation-into-the-death-of-a-journalist-hated-by-rwandan-authorities/; Human Rights Watch. (2023, 20 January). Rwanda: Suspicious Death of Investigative Journalist. https://www.hrw.org/news/2023/01/20/rwanda-suspicious-death-investigative-journalist
22. Mudge, L. (2023, 9 February). No Clarity Over Journalist's Death in Rwanda. *Human Rights Watch*. https://www.hrw.org/news/2023/02/09/no-clarity-over-journalists-death-rwanda; Mudge, L. (2023, 9 February). Questions Remain Over Rwandan Journalist's Suspicious Death. *Human Rights Watch*. https://www.hrw.org/news/2023/07/18/questions-remain-over-rwandan-journalists-suspicious-death

associations.[23] In March 2024, local administration officers assaulted Ndahiro Valens Pappy, a journalist with a private TV station, while he was reporting on the demolition of homes in the Kicukiro District.[24]

11. Self-censorship is widespread among journalists as well as non-journalists due to social pressure to support the government and fear of reprisals against those who criticise authorities.[25]
12. Rwanda has not implemented recommendations received during the third cycle of the UPR aimed at guaranteeing independence from government interference for the Rwanda Media Commission (RMC) or broadening the definition of journalist in its 2013 Media Law.[26] Protections under the law are not extended to citizen journalists, freelance journalists and bloggers.[27]
13. Disinformation is a multifaceted and complex issue. Policy and regulatory responses should pass the three-part test of legality, necessity and proportionality, considering that attempts to curtail information disorders may significantly impact freedom of expression and opinion.[28] Rwanda lacks specific legislation against online disinformation, but the 2018 Cybercrime Law contains restrictions on disinformation. The provisions are characterised by vague definitions and prescribe long periods of imprisonment as sanctions.[29] This violates the principles of legality, necessity and proportionality, enabling arbitrary application and legal uncertainty, which threaten the exercise of fundamental rights and deepen inequalities.[30] In June 2025, Rwanda's Supreme Court rejected a challenge to the 2018 Cybercrime Law for violating the constitutional guarantees of free speech.[31]

V. ONLINE SURVEILLANCE, TRANSNATIONAL REPRESSION AND RIGHT TO PRIVACY

14. Rwanda has signed and ratified the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, which also recognises the right to privacy and requires that countries establish data protection authorities to ensure secure collection, processing and storage of personal data. However, Rwanda still needs

23. Human Rights Watch. (2023, 31 January). Rwanda: Ensure Independent Investigation into John Williams Ntwali's Death. https://www.hrw.org/news/2023/01/31/rwanda-ensure-independent-investigation-john-williams-ntwalis-death; UNESCO. (2023, 30 January). Director-General urges investigation into the death of journalist John Williams Ntwali in Rwanda. https://www.unesco.org/en/articles/director-general-urges-investigation-death-journalist-john-williams-ntwali-rwanda
24. Tuyishimire, R. (2024, 12 March). Kigali: Dasso iravugwaho gukomeretsa umunyamakuru. *Umuseke*. https://umuseke.rw/2024/03/kigali-dasso-iravugwaho-gukomeretsa-umunyamakuru/
25. Freedom House. (2024). Op. cit.; Paradigm Initiative. (2025). Op. cit.
26. Human Rights Council. (2021, 25 March). Op. cit., paras. 136.29, 136.30, 136.36, 136.38.
27. Human Rights Watch. (2021, 30 March). Rwanda: Arrests, Prosecutions over YouTube Posts. https://www.hrw.org/news/2021/03/30/rwanda-arrests-prosecutions-over-youtube-posts
28. Association for Progressive Communications. (2021). *APC Policy Explainer: Disinformation*. https://www.apc.org/en/pubs/apc-policy-explainer-disinformation
29. Lexota. (2022). *Country Analysis: Rwanda*. https://lexota.org/country/rwanda/
30. Derechos Digitales, & Association for Progressive Communications. (2023). *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks*. https://www.apc.org/sites/default/files/gender_considerations_on_cybercrime_0.pdf
31. KT Press. (2025, 7 June). Supreme Court Upholds Law Which Petitioners Said Violates Free Speech. *KT Press*. https://www.ktpress.rw/2025/06/supreme-court-upholds-law-which-petitioners-said-violates-free-speech/
32. Freedom House. (2024). Op. cit.; ARTICLE 19. (2021, 15 June). Rwanda: Draft data protection bill must incorporate freedom of expression and information safeguards. https://www.article19.org/resources/rwanda-data-protection-bill-must-incorporate-free-speech-safeguards/; Shao, D., Ishengoma, F., Nikiforova, A., & Swetu, M. (2025). Comparative analysis of data protection

to align its domestic laws and policy with the Malabo Convention and international human rights standards.

15. In October 2021 the Rwandan Government enacted a Law on Protection of Personal Data. This law lacks a public interest exception for digital and traditional media outlets and has very strict data localisation requirements that are of particular concern. Further, the National Cyber Security Authority tasked with overseeing implementation of the law is not an independent body.[32]
16. Mass surveillance is institutionalised within Rwanda, with article 7 of Law 60/2013, the Law Regulating the Interception of Communications, requiring that service providers ensure that systems are technically capable of supporting interceptions at all times.
17. Digital technologies have enabled unprecedented mass and individualised surveillance. Despite constitutional privacy protections for Rwandan citizens, credible reports indicate that the government has acquired Pegasus (a powerful spyware) and deploys it against political opponents and human rights defenders, including members of the diaspora.[33] In July 2021, an international investigative media consortium revealed that Rwandan authorities had potentially targeted over 3,500 activists, journalists and political dissidents with NSO Group spyware.[34] An October 2023 report highlighted patterns of extra-national control, surveillance and intimidation of Rwandan refugee and diaspora communities.[35]

VI. TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE AGAINST WOMEN HUMAN RIGHTS DEFENDERS

18. Technology-facilitated gender-based violence (TFGBV)[36] – such as cyberstalking, online harassment and doxxing – involves acts of gender-based violence that are committed, abetted or aggravated, partly or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms and email. TFGBV has the same roots as other forms of gender-based violence and is part of the same continuum. Online and offline gender-based violence do not happen in vacuums separate from each other, as women and gender-diverse people's lives online intersect frequently and in various complex ways with other areas of their lives, and violence in any one domain can often produce harm across other domains.[37]

---

regulations in East African countries. *Digital Policy, Regulation and Governance, 27*(4), 486-501. https://doi.org/10.1108/DPRG-06-2024-0120

33. Freedom House. (2024). Op. cit.
34. Amnesty International. (2021, 19 July). Pegasus Project: Rwandan authorities chose thousands of activists, jour-nalists and politicians to target with NSO spyware. https://www.amnesty.org/en/latest/press-release/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/
35. Human Rights Watch. (2023). *"Join Us or Die": Rwanda's Extraterritorial Repression*. https://www.hrw.org/report/2023/10/10/join-us-or-die/rwandas-extraterritorial-repression
36. In this submission, we primarily use the term "technology-facilitated gender-based violence" (TFGBV), while many other terms, such as "online gender-based violence" (OGBV), are in use in international human rights spaces. Since our early research in this area, we have understood that technology-related GBV includes a broader scope of harms to be addressed, including violence facilitated by technology in so-called offline or on-ground lives, rather than just violence that happens in an online space.
37. Association for Progressive Communications. (2017). *Online gender-based violence: A submission from the Asso-ciation for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*. https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf; Association for Progressive Communications. (2023). *Feminist principles of the internet: Advocacy brief on violence*. https://genderit.org/FPI-paper-on-violence#sdfootnote1sym
38. Rutgers International. (2024). *Decoding Technology-Facilitated Gender-Based Violence: A Reality Check from Seven Countries*. https://rutgers.international/resources/decoding-technology-facilitated-gender-based-violence-a-reality-check-from-seven-countries/
39. Association for Progressive Communications. (2023). *Placing the gendered in disinformation*. https://www.apc.org/en/project/plac-

19. Rwanda's 2018 Cybercrime Law aims to address some forms of TFGBV, but falls short in terms of implementation. Additionally, there are concerns about the law being misused, for instance, to criminalise TFGBV survivors themselves in cases of content created and shared without consent.[38]
20. Gendered disinformation is a subset of TFGBV that uses false or misleading gender and sex-based narratives against women aimed at deterring them from participating in the public sphere. It combines three defining characteristics of online disinformation: falsity, malign intent and coordination. Gendered disinformation targets not only women and LGBTQ+ people, but also feminist struggles and gendered discourse. In practice, it is used to silence women, to push them to self-censorship and to restrict their civic space.[39] The content represents direct attacks on women or gender-diverse individuals, generally based on gender bias, stereotypes and expectations.[40]
21. Gendered disinformation in Rwanda has been used to deter young women from a political career, by targeting women politicians with image-based disinformation to sexualise them and create false narratives, shifting public focus from their main political discourse. In May 2024, opposition leader Victoire Ingabire Umuhoza faced aggressive online harassment following public disclosure of her intended presidential candidacy.[41] Similar tactics[42] are observed in attacks against women human rights defenders.[43]
22. Rwanda does not criminalise consensual same-sex relations, but Rwandan society is still conservative and online and offline attacks based on gender identity and sexual orientation are prevalent. Online harassment, government surveillance and posting of images without consent are widespread concerns.[44] For instance, Rwandan designer Moses Turahirwa was targeted with homophobic comments and arrested for suspected forgery after sharing a photo on Instagram to show that a passport reflected Turahirwa's new gender.[45]

---

ing-gendered-disinformation

40. Martins, P. (2024). *Placing "gender" in disinformation*. Association for Progressive Communications. https://www.apc.org/en/pubs/placing-gender-disinformation
41. Umuhoza, V. (2024, 22 May). Rwanda's Undemocratic Election. *Foreign Policy*. https://foreignpolicy.com/2024/05/22/rwanda-kagame-undemocratic-election-victoire-ingabire/
42. Jin., X. (2025, 3 April). ASCL Seminar: Neoliberal Authoritarianism in Rwanda: A Feminist Analysis. *The African Studies Centre, Leiden University*.
43. These findings are based on discussions from the validation workshop with stakeholders organised on 20 June 2025.
44. McLean, N., & Cicero, T. (2023). *The Left Out Project report: The case for an online gender-based violence frame-work inclusive of trans-gender, non-binary and gender-diverse experiences*. Association for Progressive Communica-tions. https://www.apc.org/sites/default/files/the-left-out-project-report.pdf
45. Iriza, J. N. (2023, 27 April). Moshions' Turahirwa under probe for forging document. *The New Times*. https://www.newtimes.co.rw/article/7023/news/crime/moshions-moses-under-investigation-for-document-forgery; Africa News. (2023). Rwanda: LGBTQ fashion designer charged with passport forgery. *Africa News*. https://www.africanews.com/2023/04/28/rwanda-lgbtq-fashion-designer-charged-with-passport-forgery/
46. Association for Progressive Communications. (2021). Op. cit.
47. UN Human Rights Council. (2025). *Human rights defenders and new and emerging technologies: protecting hu-man rights defenders, including women human rights defenders, in the digital age*. https://documents.un.org/doc/undoc/ltd/g25/048/80/pdf/g2504880.

VII. RECOMMENDATIONS

23. We recommend that the Government of Rwanda take the following measures to uphold human rights in the digital context:

Digital connectivity and inclusion

- Invest in infrastructure to extend broadband internet access to rural areas, including through partnerships with private sector providers and community-based networks.
- Sustain efforts to create enabling policy and regulatory environments for the development and sustainability of community-led networks.
- Ensure transparency of the Universal Service Access Fund, especially in regard to allocation of funds, disbursements and operations. Expand the pool of potential beneficiaries and invest in projects addressing the gender digital divide.
- Implement programmes on early digital rights education and awareness activities, including prioritising digital literacy education in public junior and secondary schools to empower people with skills to navigate the digital space safely and critically.
- Offer targeted training programmes for adults, especially women, to equip them with the necessary digital skills for employment and participation in society. Implement mentorship programmes to increase the number of girls taking up ICT-related courses in school.
- Implement subsidy programmes or partnerships with service providers to improve access to devices for low-income households.
- Conduct regular assessments of connectivity availability and usage patterns to identify underserved areas and inform targeted interventions.
- Ensure that digital access is inclusive and equitable for all. Address barriers to accessing technology and the internet for marginalised communities, including rural communities, women and persons with disabilities. For this, the government should establish institutionalised bottom-up participation and multistakeholder decision-making processes to promote inclusive participation of communities in policy making concerning access and digital inclusion.

Freedom of speech and expression online

- Repeal provisions that unduly criminalise free speech, including articles 157, 164, 194, 233 and 253 of the 2018 Penal Code;
- Amend the 2018 Cybercrime Law to ensure that all provisions comply with international human rights standards relating to free speech and expression.
- Withdraw all cases against individuals facing harassment, intimidation and prosecution from state authorities for legitimate expression and dissent against the government.
- Conduct robust independent investigations into attacks targeting journalists and human rights defenders.
- Promote healthy information systems that include robust access to public information, plural, accessible and diverse media contexts, independent and qualified journalism

and the possibility of safely expressing ideas to counter disinformation.[46] This includes encouraging social media platforms to take proactive measures to address disinformation and provide transparency on their algorithms and content moderation policies.

- Lift the ban on foreign radio services such as the BBC Kinyarwanda service.
- Work with civil society organisations and community leaders on public awareness campaigns to promote tolerance, inclusivity and respect for diversity.
- Ensure independence of the RMC from government interference.
- Amend the 2013 Media Law to broaden the definition of journalist to extend protection to citizen journalists, freelance journalists and bloggers.

Online surveillance, transnational repression and right to privacy

- Ensure that the National Cyber Security Authority can act with complete independence in accordance with standards in the Malabo Convention.
- Encourage companies operating in Rwanda to implement robust cybersecurity measures to protect personal data and prevent cyberattacks, in line with the government's obligations under the United Nations Guiding Principles on Business and Human Rights (UNGP-BHR).
- Refrain from or cease the use or transfer of new and emerging technologies, including artificial intelligence applications and spyware, where they are impossible to operate in compliance with international human rights law or pose undue risks to the enjoyment of human rights, unless and until adequate safeguards to protect human rights and fundamental freedoms are in place.[47] Set up an adequately resourced independent judicial mechanism with oversight of the state surveillance apparatus.
- Refrain from using cybersecurity-related laws, policies and practices as a pretext to violate human rights and fundamental freedoms. Cybersecurity-related policies must provide security in a way that reinforces human rights.[48] Amend regulatory provisions such as Law 60/2013 that enable state surveillance of content without adequate safeguards.
- Guarantee adequate independent oversight mechanisms that operate on principles of transparency and accountability, provide redress mechanisms to victims and control state surveillance practices to ensure they are limited and proportional in accordance with international human rights standards.
- Strengthen the independence and accountability of the Rwanda Data Protection Office.

pdf; Baltazar, F., & Martins. P. (2025, 23 April). A digital milestone: New resolution on human rights defenders and new technologies adopted by the UN Human Rights Council. *Association for Progressive Communications*. https://www.apc.org/en/news/digital-milestone-new-resolution-human-rights-defenders-and-new-technologies-adopted-un-human

48. Association for Progressive Communications. (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity

Technology-facilitated gender-based violence against women public figures, including human rights defenders

- Enhance measures and policies to prohibit, investigate and prosecute TFGBV. Engage with specialists in TFGBV, including civil society organisations, survivors and academics to reform laws in this sense. Ensure that legislative responses aimed at tackling TFGBV are gender-responsive and in line with international human rights standards.
- Amend the 2018 Cybercrime Law to ensure that restrictions to freedom of expression as a response to TFGBV are necessary and proportionate and not overly broad or vague in terms of what speech is restricted and that they do not over penalise.
- Provide redress and reparation as an effective, efficient and meaningful way of aiding victims of TFGBV and ensuring that justice is achieved. Such measures should include forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic, material, individual and collective, depending on the circumstances and the preferences of the victim.
- Train judiciary personnel, lawyers, police and law enforcement officials and frontline workers to ensure their ability to investigate and prosecute perpetrators, and foster public trust in obtaining justice for cases of TFGBV, in conjunction with broader sensitisation in addressing gender-based violence.
- Ensure that online platforms comply with their responsibilities under the UNGP-BHR. Develop appropriate and effective accountability mechanisms for social media platforms and other technology companies, with a focus on ensuring company transparency and remediation to ensure that hate speech and TFGBV are addressed on their platforms, there is appropriate response to such instances and safeguards and redress mechanisms are available for those affected.
- Promote the development of TFGBV lexicons in different local languages to be used in training AI algorithms and individuals for effective content moderation to curb TFGBV.
- Proactively facilitate collaboration between various stakeholders, including technology companies, women's rights organisations, researchers and civil society, to strengthen policy making and implementation aimed at preventing and addressing TFGBV.