Summary of the submission by APC and CIPESA to the 51st session of the Universal Periodic Review at the UN Human Rights Council

Human rights in the digital context in Rwanda

The joint stakeholder report[1] by the Association for Progressive Communications (APC) and the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) focuses on key issues relating to human rights in the digital context in Rwanda, including digital connectivity and inclusion, freedom of expression online, surveillance and technology-facilitated gender-based violence, particularly its impact on human rights and women's rights defenders.

1. https://www.apc.org/en/node/40855/

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

CIPESA

I. Context of the human rights situation online in Rwanda

Since its Universal Periodic Review during the third cycle, Rwanda has made progress towards implementing some of the recommendations received. The digital infrastructure in Rwanda has expanded and access to information and communication technologies (ICTs) has improved significantly. However, there was heightened authoritarianism and censorship of online criticism in the lead-up to the 2024 general elections. Violations of user rights, strict censorship, increased surveillance and infrastructure limitations contributed to Freedom House lowering Rwanda's Freedom on the Net rating in 2024, rating it as "Not Free" with a score of 36/100.

II. Digital inclusion and connectivity

Rwanda's internet penetration rate was estimated to be 34.2% at the start of 2025. There is gender imbalance in internet access and use, with about 38.2% of active social media user identities estimated to be female in January 2025. Price and lack of appropriate devices – the main reasons for not accessing ICTs – affect women more due to fundamental gender disparities, particularly in education and income. There is a need for an effective framework to regulate Rwanda's national ID with a unique identifier number, which is becoming popular as a key to access services and conduct transactions electronically.

III. Freedom of speech and expression online

Rwandan laws still contain provisions that unduly restrict free speech and expression online, including provisions of the 2018 Penal Code relating to dissemination of edited words or images, spreading false information, causing hostile international opinion, humiliating national authorities and refusing to answer questions by intelligence officers. Meanwhile, troubling incidents of arrests, intimidation, abduction and killings of journalists and human rights defenders for exercising their rights to free speech continue to be reported. Self-censorship is widespread due to social pressure to support the government and fear of reprisals for criticising authorities. Restrictions on disinformation under the 2018 Cybercrime Law are characterised by vague definitions, with long periods of imprisonment prescribed. In June 2025, Rwanda's Supreme Court rejected a challenge to the 2018 Cybercrime Law for violating the constitutional guarantees of free speech.

IV. Online surveillance, transnational repression and right to privacy

The Law on Protection of Personal Data enacted by the Rwandan Government in October 2021 lacks a public-interest exception for digital and traditional media outlets and has very strict data localisation requirements. Mass surveillance is institutionalised within Rwanda, with Law 60/2013 requiring that service providers ensure their systems are technically capable of supporting interceptions at all times. 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.

V. Technology-facilitated gender-based violence (TFGBV) against women human rights defenders

Rwanda's 2018 Cybercrime Law aims to address some forms of TFGBV, but falls short in terms of implementation. There are concerns about the law being misused, for instance, to criminalise TFGBV survivors in cases where content is created and shared without consent. Gendered disinformation in Rwanda has been used to target women politicians and human rights defenders with image-based disinformation, sexualise them and create false narratives, shifting public focus from their main political discourse. Online and offline attacks based on gender identity and sexual orientation are prevalent in Rwanda, including online harassment, government surveillance and posting of images without consent.

VI. Key recommendations to the government of Rwanda

- Ensure that digital access is inclusive and equitable for all by removing access barriers for marginalised communities, including rural communities, women and persons with disabilities.
- Repeal provisions that unduly criminalise free speech, including articles 157, 164, 194, 233 and 253 of the 2018 Penal Code, and 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 of dissent against the government.
- Refrain from using or cease the use of artificial intelligence applications and spyware, in cases where it is impossible for them to operate in compliance with international human rights law or where they pose undue risks to the enjoyment of human rights, unless and until the adequate safeguards to protect human rights and fundamental freedoms are in place.
- Guarantee adequate independent oversight mechanisms to ensure state surveillance practices are limited and proportional in accordance with international human rights standards.
- Enhance measures and policies to prohibit, investigate and prosecute TFGBV 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, not overly broad or vague in terms of what speech is restricted and 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.
- 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 is appropriately addressed on their platforms.