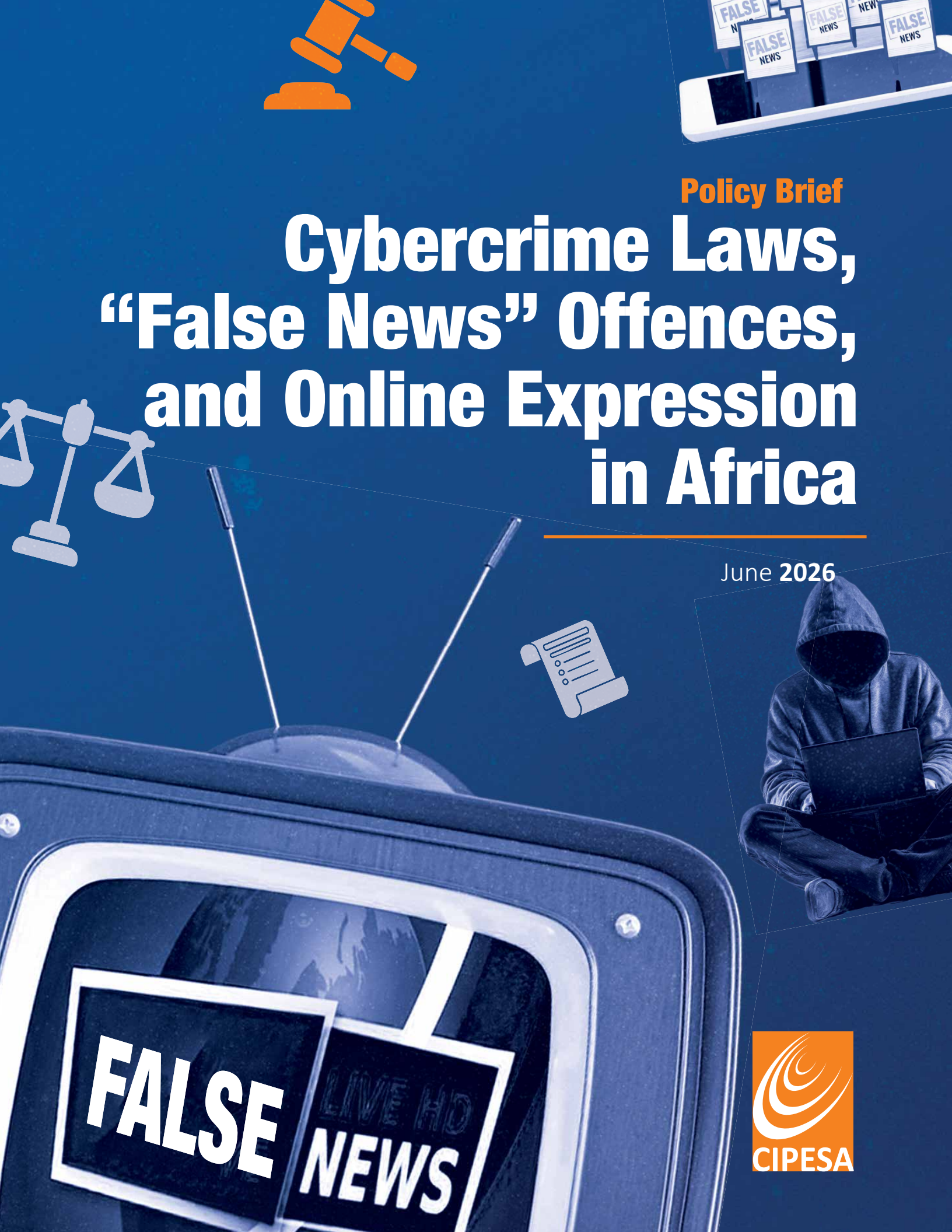
Policy Brief

Cybercrime Laws, "False News" Offences, and Online Expression in Africa

June **2026**



CIPESA

Background

Across Africa, governments are increasingly adopting cybercrime, misinformation, and "false news" laws to address growing digital harms, including disinformation, hate speech, online harassment, and cyber-enabled abuse. As internet access expands and digital platforms become central to civic participation, governments face legitimate pressures to protect citizens from digital harms and maintain public order.

However, many regulatory responses have introduced vague and broadly framed offences such as "false news", "false information", "offensive communication", "malicious communication", and "harmful content". These offences often lack clear legal definitions and grant authorities wide discretion to determine what speech is permissible. In practice, they have frequently been used against journalists, activists, opposition figures, bloggers, and ordinary citizens engaged in public debate.

The challenge facing African policymakers is therefore not whether online spaces should be regulated, but how the legal regulatory frameworks should address genuine digital harms without undermining constitutional freedoms and democratic participation.

This brief argues that while governments have legitimate interests in combating digital harms, which understandably the public needs to be protected from, many cybercrime and disinformation laws have evolved into instruments for stifling dissent rather than protecting citizens from digital harm. Combined with expanding surveillance powers, internet shutdowns, and weak accountability mechanisms, these laws and regulations are now part of a broader architecture of digital authoritarianism. At the same time, recent judicial decisions in countries such as Kenya, alongside legislative reforms in Nigeria, demonstrate that rights-respecting alternatives are both possible and necessary.

When Online Harm Regulation Becomes Speech Control

The proliferation of disinformation and digital manipulation presents genuine governance challenges. False information can undermine public health responses, inflame social tensions, distort electoral processes, and erode trust in public institutions. Governments, therefore, have a legitimate responsibility to develop legal frameworks capable of responding to these dynamic risks as well as safeguarding the integrity of democratic institutions and processes.

Yet many existing cybercrime and disinformation laws blur the distinction between harmful conduct and legitimate expression. Rather than targeting clearly defined forms of unlawful activity, such as coordinated disinformation campaigns, online fraud, or incitement to violence, they often criminalise vaguely defined categories of speech whose boundaries remain uncertain.

The consequence is a regulatory environment in several countries in which individuals cannot reasonably predict what forms of expression may attract criminal liability. Such uncertainty encourages self-censorship and creates opportunities for selective enforcement, mostly targeting critics of government, independent media, and civil society actors, with little attention paid to cybercriminals.

The problem is not merely poor legislative drafting. It reflects a broader tension between state interests in controlling information and democratic commitments to freedom of expression. In many contexts, cybercrime laws have become tools for managing political discourse rather than narrowly tailored mechanisms for addressing digital harms.

Emerging Patterns

Although national contexts differ, the implementation of cybercrime and disinformation laws across the continent reveals a recurring pattern of using broadly framed cybercrime, disinformation, and "false news" laws to regulate speech.[1] In countries such as Ethiopia, Kenya, Nigeria, and Uganda, these legal frameworks have been used as a basis to arrest, intimidate, detain and prosecute journalists, activists, and political commentators.

Ethiopia's 2020 Hate Speech and Disinformation Proclamation,[2] for example, has been invoked in cases involving journalists[3] and opposition-linked voices,[4] while Kenya's Computer Misuse and Cybercrimes Act (2018) has faced constitutional scrutiny for enabling selective enforcement during politically sensitive periods.[6] Similar concerns have been raised in Uganda[7] and Nigeria,[8] where prosecutions for "false information" have been challenged before national courts as incompatible with constitutional protections for expression.

A similar pattern is evident in Francophone West Africa, where cybercrime laws have increasingly been used to penalise criticism of state authorities and reporting on governance issues.

1 *CIPESA, Africa's Digital Dilemma: Platform Regulation Vs Internet Freedom, May 2025, Africa's Digital Dilemma: Platform Regulation Vs Internet Freedom – Collaboration on International ICT Policy for East and Southern Africa (CIPESA)*

2 *Access Now, "Hate Speech and Disinformation Prevention and Suppression Proclamation", 2020, https://www.accessnow.org/wp-content/uploads/2020/05/Hate-Speech-and-Disinformation-Prevention-and-Suppression-Proclamation.pdf*

3 *HRW, "Ethiopia:Surge in Arrests of Journalists, Media Workers", September 2025, https://www.hrw.org/news/2025/09/22/ethiopia-surge-in-arrests-of-journalists-media-workers*

4 *Ethiopia Observer, "29 Activists Detained on Charges of Inciting Riots on Social Media Posts", January 2024, https://www.ethiopiaobserver.com/2024/01/22/29-activists-detained-on-charges-of-inciting-riots-on-social-media-posts/*

5 *IPKenya, "The Computer Misuse and Cybercrimes Act,2018, https://ipkenya.wordpress.com/wp-content/uploads/2018/05/the-computer-misuse-and-cybercrimes-act-2018.pdf*

6 *ICJ Kenya, "Court of Appeal Declares Sections of the Cybercrimes Act Unconstitutional", March 2026, https://icj-kenya.org/news/court-of-appeal-declares-sections-of-cybercrimes-act-unconstitutional/*

7 *CPJ, "Uganda Declares Criminal Defamation Unconstitutional, Strikes Down Cybercrime Law, March 2026, https://cpj.org/2026/03/uganda-declares-criminal-defamation-unconstitutional-strikes-down-cybercrime-law/*

8 *Columbia University, "Okedara v. Attorney General, February 2019, https://globalfreedomofexpression.columbia.edu/cases/okedara-v-attorney-general/*

Mali: Criminalisation of criticism of cybercrime law

In June 2026, two journalists in Mali, Abdrahamane Keïta and Chahana Takiou, were arrested under the country's cybercrime law for criticising the military government's record on press freedom. One of the journalists had previously spoken publicly about the misuse of the same law and was subsequently detained under its provisions. Mali's cybercrime framework operates under legislation introduced since 2022, which has replaced earlier press protections with significantly harsher penalties for online expression. The case illustrates how cybercrime frameworks can be used not only to regulate content but also to suppress criticism of the laws themselves. [9]

Niger cybercrime law used against journalists

In November 2025, six journalists in Niger, Moussa Kaka and Abdoul Aziz of Saraounia TV; Ibro Chaibou and Souleymane Brah from the online publication Voice of the People; Youssouf Seriba of Les Échos du Niger; and Oumarou Kané, founder of the magazine Le Hérisson, were arrested and detained after sharing a press conference invitation on social media. They were charged under a cybercrime law amended in 2024 to reinstate prison sentences of up to five years for content deemed to disturb public order. The case illustrates how vaguely worded cybercrime provisions can be applied to ordinary journalistic practice, turning routine information sharing into a criminal offence.[10]

Additionally, these laws are disproportionately enforced against individuals engaged in political expression rather than against coordinated disinformation networks. Journalists, opposition politicians, activists, satirists, and social media users have frequently been the primary targets of prosecution.[11]

Moreover, restrictions on online expression increasingly operate alongside broader systems of digital governance, including surveillance technologies, telecommunications interception frameworks, biometric identification systems, and internet shutdowns. Together, these measures create cumulative restrictions on civic space and democratic participation.

Judicial and Legislative Responses

Recent developments suggest that courts and reform processes are beginning to scrutinise the constitutionality and proportionality of the enforcement of these laws.

Uganda provides one of the clearest examples of both regulatory overreach and judicial correction. For several years, provisions of the Computer Misuse Act 2011 and related legislation were used to prosecute journalists, activists, lawyers, and government critics under offences such as offensive communication, cyber harassment, and criminal libel.

In 2026, the Constitutional Court struck down key provisions of the Computer Misuse (Amendment) Act, 2022, finding that offences criminalising communication that "ridicules", "demeans", or "promotes hostility" were impermissibly vague and susceptible to arbitrary enforcement. The Court also invalidated criminal libel provisions, emphasising that civil remedies provide a less restrictive means of protecting reputation.[12]

The decision represents an important reaffirmation of the principle that restrictions on expression must be clearly defined and proportionate to legitimate objectives.

Kenya's Court of Appeal[13] reached similar conclusions in its 2026 decision striking down provisions criminalising false publications under the Computer Misuse and Cybercrimes Act 2018.[14] The court recognised that attempts to criminalise "falsity" itself risked capturing innocent conduct, including the unintentional sharing of inaccurate information. More fundamentally, it acknowledged that truth is often contested and evolving, making broad criminal prohibitions incompatible with open democratic debate.

The ruling reinforced the principle that disinformation concerns cannot justify unrestricted state discretion over public discourse.

9 *CPJ, "In Mali, Two More Journalists Arrested Under Cybercrimes Law for Criticising Authorities", June 2026, https://cpj.org/2026/06/in-mali-2-more-journalists-arrested-under-cybercrime-law-for-criticizing-authorities/*

10 *HRW, "Journalists in Niger Arrested Under Cybercrimes Law", November 2025, https://www.hrw.org/news/2025/11/06/journalists-in-niger-arrested-under-cybercrime-law*

11 *The Conversation, "Punitive Laws are Failing to Curb Disinformation in Africa. Time for a Rethink", June 2021,https://theconversation.com/punitive-laws-are-failing-to-curb-misinformation-in-africa-time-for-a-rethink-162961*

12 *Cipesa, "CIPESA Welcomes the Annulment of Sections of Uganda's Computer Misuse Act", March 2026, https://cipesa.org/2026/03/cipesa-welcomes-the-annulment-of-sections-of-ugandas-computer-misuse-act/*

13 *Court of Appeal declares sections of Cybercrimes Act unconstitutional - ICJ Kenya*

14 *IPKenya, "The Computer Misuse and Cybercrimes Act,2018, https://ipkenya.wordpress.com/wp-content/uploads/2018/05/the-computer-misuse-and-cybercrimes-act-2018.pdf*

Nigeria demonstrates a different pathway toward accountability. Following sustained advocacy from civil society organisations, journalists, and digital rights groups, amendments adopted in 2024 narrowed the scope of Section 24 of the Cybercrime Act by requiring proof of intent to cause harm.

While implementation challenges remain, the reforms illustrate how civil society participation in legislative processes can reduce opportunities for arbitrary enforcement while preserving the state's ability to address genuinely harmful conduct. However, recent enforcement cases suggest that legal reform alone may be insufficient to shift entrenched practices of arrest and detention under cybercrime provisions.

Nigeria's post-reform enforcement gap

Nigeria's 2024 amendments to Section 24 of the Cybercrimes Act narrowed the scope of the offence by requiring proof of intent to cause harm, in an effort to reduce arbitrary prosecution for online expression. However, enforcement patterns in late 2025 indicate limited practical change. An investigative journalist, Daniel Ojukwu, was in May 2024 detained and transferred across state lines without access to legal counsel or formal charges.[15]

In separate incidents, a reporter was arrested on allegations of cyberbullying and criminal defamation, while two individuals in Kano were detained over Facebook posts criticising public infrastructure projects.[16] These cases highlight the gap between legislative reform and enforcement practice, underscoring that legal amendments alone do not automatically prevent the abusive application of cybercrime laws.

By contrast, Tanzania continues to maintain one of the continent's most restrictive digital governance environments. The Cyber Crimes Act 2015, Electronic and Postal Communications Act 2010, and Online Content (Amendment) Regulations 2020 collectively impose extensive controls on online expression through licensing requirements, content restrictions, and criminal penalties.

The limited success of judicial challenges has allowed these Tanzanian frameworks to remain largely intact, illustrating how restrictive models can become entrenched where institutional safeguards are weak.[17]

At the regional level, the African Commission on Human and Peoples' Rights (ACHPR) has received multiple complaints on internet shutdowns, surveillance, and digital repression, including complaints linked to election-related restrictions in Uganda and Chad.[18] Similarly, the Economic Community of West African States (ECOWAS) Court of Justice[19] has issued decisions affirming that internet shutdowns violate freedom of expression. However, these regional judicial processes are slow, often non-binding in practice, and dependent on state compliance, limiting their deterrent effect and leaving many violations unremedied.

In 2023, the ECOWAS Court held, in Association des Blogueurs de Guinée and Others v The State of Guinea,[20] that states have an obligation not only to refrain from interfering with freedom of expression, but also to take all necessary measures to give it (freedom of expression) effect. The court determined that, by shutting down the internet amidst protests against the president of Guinea's amendment of the constitution, the state infringed upon citizens' rights to freedom of expression.

In cybercrime regulation, regional efforts aim at harmonisation but tend to prioritise security over rights.[21] Broad surveillance powers with limited judicial oversight raise concerns regarding privacy and freedom of expression. This tension highlights the persistent imbalance between security and public safety objectives, on the one hand, and human rights protections, on the other.

15 *Foundation for Investigative Journalism, "Police Move Abducted FIJ Reporter Daniel Ojukwu to Abuja, May 2024, https://fij.ng/article/police-move-abducted-fij-reporter-daniel-ojukwu-to-abuja/*

16 *CPJ, "Three Nigerian Journalists Detained on Cybercrimes Allegations, Despite Reform, November 2025, https://cpj.org/2025/11/3-nigerian-journalists-detained-on-cybercrime-allegations-despite-reform/*

17 *Cipesa, "Tanzania's Digital Rights Record Faces Fresh Scrutiny at the UPR, May 2026, https://cipesa.org/2026/05/tanzanias-digital-rights-record-faces-fresh-scrutiny-at-the-upr/*

18 *Cipesa, Advancing Strategic Litigation on Internet Shutdown Cases in Africa: Promises and Pitfalls, https://cipesa.org/wp-content/files/Advancing-Strategic-Litigation-on-Internet-Shutdowns-cases-in-Africa-Promises-and-Pitfalls.pdf*

19 *Ibid*

20 *Cyrilla Collaborative, "Association des Blogueurs de Guinée", October 2023, https://cyrilla.org/en/entity/pz0x57ngpz9?page=2*

21 *EU Cyber Direct, "Shaping the UNCybercrime Convention: Human Rights at a Crossroads", February 2026, https://eucyberdirect.eu/blog/shaping-the-un-cybercrime-convention-human-rights-at-a-crossroads*

Beyond Speech Regulation: Surveillance and Digital Control

Cybercrime and disinformation laws do not operate in isolation. Across the continent, restrictions on expression increasingly intersect with surveillance and information control measures that expand state influence over digital spaces.

Internet shutdowns during elections, protests, and periods of political unrest have become recurring features in several countries. Governments have also expanded interception of communication powers, strengthened monitoring obligations for telecommunications providers, and invested in mass biometric identification systems that centralise sensitive personal information.

Legal frameworks in Benin, Cameroon, Chad, Côte d'Ivoire, Malawi, Mali, Niger, Nigeria, Rwanda, Senegal, Tanzania, Togo, Tunisia, Uganda, Zambia, and Zimbabwe commonly require telecommunications providers to facilitate interception of communications.[22]

These laws often mandate the installation of surveillance infrastructure and the provision of real-time access to user data, frequently without strong judicial oversight. In Uganda, for instance, legislation compels telecom companies to enable interception systems, while Zambia's Cyber Security and Cyber Crimes Act (2021) requires service providers to support real-time monitoring and data disclosure. Zimbabwe's interception laws similarly obligate providers to maintain constant surveillance capabilities.[23]

In Central Africa, countries including Cameroon, Chad, the Democratic Republic of the Congo, Equatorial Guinea, and Gabon have expanded surveillance practices, often with limited privacy and data protection safeguards. In East Africa, surveillance has been linked to violations of multiple rights, including the rights to privacy, freedom of expression, access to information, and freedom of assembly and association.

Although many states have enacted data protection legislation, enforcement remains uneven, and the data protection authorities, where established, often lack independence, resources, or enforcement authority, especially over state security agencies. The result is a growing imbalance between state surveillance capabilities and mechanisms designed to protect citizens' rights.

Taken together, these developments contribute to a broader environment of self-censorship, reduced civic participation, and weakened democratic accountability.

22 *Paradigm Initiative, The State of Deployment of Surveillance Technologies in Africa, May 2024, https://cipesa.org/wp-content/files/documents/Our_Work_on_Surveillance_Concerns_In_Africa.pdf*

23 *Cipesa, "Digital Authoritarianism and Democratic Participation in Africa", June 2022, https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief-.pdf*

Implications

The cases documented in this brief point to consequences that extend well beyond individual prosecutions. They reveal a pattern in which legal frameworks designed to address digital harms are being applied in ways that weaken the institutions and practices on which democratic governance depends.

When journalists face criminal liability for reporting on matters of public interest, public oversight of the government is weakened, and accountability gaps widen. If citizens self-censor online, civic participation declines, and the plurality and diversity of voices shaping public debate narrows. Once internet shutdowns disrupt communication during elections or protests, they effectively close the public square, thus undermining the conditions for informed democratic choice. And when surveillance powers expand without adequate judicial oversight, the chilling effect extends beyond targeted individuals to broader communities of journalists, activists, and civic actors. Also, when the law is brutally developed and enforced against legitimate non-state actors, public confidence and trust in state institutions wane, thereby amplifying the cycle of pushback and criticism the state wanted to muzzle in the first place.

These effects accumulate over time. Vague criminal offences, expansive surveillance powers, and platform restrictions reinforce one another, gradually narrowing the space for legitimate expression. The result is a system of digital control that emerges through the interaction of multiple measures that, individually, are often presented as lawful or necessary, but in reality, they represent a growing culture of digital authoritarianism.

Conclusion

Governments face legitimate pressures to address disinformation and other emerging digital harms. However, regulatory approaches that rely on vaguely defined criminal offences and expansive state powers often undermine the rights and democratic values they are intended to protect.

The persistence of restrictive frameworks in countries such as Uganda and Tanzania underscores these risks, even as other jurisdictions pursue reform. At the same time, some recent judicial decisions and legislative changes demonstrate that alternative, rights-respecting approaches are possible.

The central challenge is not whether digital spaces should be regulated, but how to ensure that regulation addresses online harms while protecting freedom of expression, privacy, and democratic participation. The future of online freedom in Africa will depend on how governments, courts, regional institutions, and technology companies navigate this balance.

Policy Recommendations

For Governments

- Repeal or amend vague offences criminalising “false information”, “offensive communication”, and similarly broad categories of speech.
- Prioritise civil remedies over criminal sanctions for defamation and reputation-related disputes.
- Desist from instituting internet shutdowns and ensure that any restrictions to freedom of expression comply with international human rights standards.
- Strengthen judicial authorisation and oversight mechanisms for surveillance and interception of communication.
- Accelerate ratification and implementation of the Malabo Convention.

For Legislators and Regulators

- Ensure that digital governance laws comply with the principles of legality, necessity, and proportionality.
- Conduct mandatory human rights impact assessments before adopting new cybercrime or disinformation legislation.
- Institutionalise meaningful public participation in the development of digital governance frameworks.
- Enhance the independence, capacity and resources of oversight bodies such as the data protection and communications regulatory authorities.

For Regional Institutions

- Strengthen monitoring and implementation mechanisms under the African Charter on Human and Peoples’ Rights.
- Promote regional standards on digital rights and accountable governance.

For Technology Platforms

- Invest in African-language moderation capacity and local contextual expertise.
- Increase transparency regarding content moderation decisions and algorithmic amplification.
- Strengthen grievance and appeal mechanisms for users in African jurisdictions.

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug facebook.com/cipesaug Linkedin/cipesa

www.cipesa.org