DATA PRIVACY | REGULATORY

Cybercrime across borders: Navigating Africa's fragmented legislative landscape – Part 2

17 September 2026 *9 min read*

by Ahmore Burger-Smidt, Director and Head of Regulatory, and Boitumelo Khwene, Candidate Attorney

In Part one of this series, we detailed the disparity amongst the African countries in mainly Southern Africa and the various approaches to cybersecurity. Unfortunately, this creates a uncertainty for many multi-jurisdictional entities operating across the African continent on how to best approach the issue of cybersecurity when there are discrepancies in the promulgation of legislation targeted at addressing this very issue.

In the second and final part of this series, we focus specifically on East and West Africans countries. At first glance, it seems strides are being made particularly in East Africa to enact viable cybercrime laws which combat and adequately address the issue of cybersecurity, however, numerous constitutional challenges have impeded on this aspiration. With civil society organisations in some countries arguing that certain provisions in these laws infringe on the right to freedom of expression and the right of privacy. In essence, it seems some African countries have merely pledged to enacting laws addressing and aimed at curbing cybercrime but no progressive measures have been taken thereafter.

East Africa: Constitutional Volatility amid Evolving Frameworks

- **Kenya: A Moving Target**

Kenya's Computer Misuse and Cybercrimes Act of 2018[1] reaches a broad range of conduct: unauthorised interference with computer systems, interception, publication of false information, cyber harassment, cybersquatting and fraudulent use of electronic data. It also establishes the National Computer and Cybercrimes Co-ordination Committee. For basic offences, penalties can reach KES 200,000 or two years' imprisonment; for aiding and abetting, they rise to KES 7 million or four years.

Several provisions of the Act have faced constitutional challenge after its enactment including concerns that the provisions may possibly infringe on the right to freedom of expression which can have a dire impact on also the freedom of media. Nonetheless, the core Act has been upheld. The 2025 amendments, which sought higher penalties and broader content-takedown powers, now face a fresh constitutional challenge, with conservatory orders in place.[2] Kenya captures a pattern increasingly visible across the continent: cybercrime laws are enacted, challenged, partly struck down, re-enacted and challenged again, leaving compliance teams to work against a moving legal target.

- **Tanzania: Broad Powers, Narrow Oversight**

Tanzania's Cybercrimes Act of 2015[3] criminalises illegal access, interception, data interference, data espionage and computer-related forgery and fraud. It has nevertheless drawn criticism for giving law enforcement extensive search-and-seizure powers with limited judicial oversight and that the enactment fails to provide procedural safeguards for human rights protection which would uphold the right to freedom of expression and the right to privacy,[4] prompting concerns about misuse familiar from the wider African cybercrime debate.

- **Uganda: Constitutional Volatility**

Uganda offers perhaps the clearest example of constitutional volatility in this field. The Computer Misuse Act of 2011 was amended in 2022[5] to broaden the unauthorised-access offence and introduce new provisions on the unauthorised sharing of children's information and social media abuse. In March 2026, however, Uganda's Constitutional Court declared the 2022 amendment "null and void" because Parliament had not met the constitutionally required quorum when it was passed.[6] The Court also struck down the criminal defamation provisions. As a result, the pre-2022 principal Act currently governs, pending re-enactment.

- **Rwanda: A Proactive Framework**

Rwanda's Law on Prevention and Punishment of Cybercrimes, enacted in 2018,[7] places the country among East Africa's more proactive states in this field. Rwanda is both a Budapest Convention signatory and a Malabo Convention ratifier, reflecting a deliberate effort to align its domestic framework with international standards. That dual alignment remains relatively unusual on the continent and fits Rwanda's broader ambition to position itself as a technology and innovation hub.

West Africa: Diversity, Ambition and Contested Levies

- **Nigeria: Scale and Contested Reform**

Nigeria's Cybercrimes (Prohibition, Prevention, Etc) Act of 2015, significantly amended in 2024,[8] is West Africa's most consequential cybercrime statute, given the scale of the Nigerian financial services sector. It criminalises unauthorised and fraudulent access to computer systems to obtain data vital to national security and requires incidents to be reported to the National Computer Emergency Response Team within 72 hours; non-compliance is punishable by denial of internet services and be liable for paying a mandatory fine of N2,000,000 into the National Cyber Security Fund.[9]

The 2024 amendment matters for several reasons. It revised section 24 of the 2015 Act, a provision the ECOWAS Community Court of Justice condemned for its use against journalists.[10] It also broadened the coverage of payment-technology fraud. Most controversially, it introduced a 0.5 per cent National Cybersecurity Levy on banks and payment service providers, a provision that prompted significant industry opposition and was subsequently suspended by the House of Representatives.[11] The Central Bank of Nigeria regulates financial institutions' compliance, and the data protection regulator has sanctioned at least one bank for breach. Nigeria's framework is therefore both ambitious and contested, and it demands close monitoring.

- **Ghana: Institutional Regulation**

Ghana's Cybersecurity Act of 2020[12] takes an institutional and regulatory approach. It makes the Cyber Security Authority the primary regulator, with power to license cybersecurity service providers and to designate and audit critical information infrastructure, a category that expressly includes banking and financial services. The Act also creates a National Computer Emergency Response Team and a Cybersecurity Fund financed by levies on Bank of Ghana-licensed entities.[13] Alongside the Data Protection Act and the Electronic Transactions Act, it forms a layered regulatory architecture that must navigate carefully.

- **Francophone West Africa: A Distinctive Tradition**

Francophone West Africa has its own legislative character. The region often draws on French civil-law models and reflects the influence of regional harmonisation efforts.

Côte d'Ivoire enacted its cybercrime law in 2013 and amended it in 2023,[14] covering ICT-specific offences, online intellectual-property infringements and offences committed over electronic communications networks. The amendment revised several key provisions, showing a willingness to update the framework as threats evolve. A companion personal data protection law and an electronic transactions law complete the regulatory architecture.

Senegal's 2008 cybercrime law,[15] modelled on the Budapest Convention, ranks among the earliest francophone African cybercrime statutes. Senegal's accession to the Budapest Convention in December 2016 strengthened that alignment with the European standard and was followed by the creation of a dedicated cybercrime police division.

Benin may have the region's most ambitious approach. Its Code du numérique, adopted in 2017 and amended in 2021,[16] is a consolidated 647-article digital code; its sixth book is devoted to "Cybercriminalité et cybersécurité." The Code creates a national information systems security agency and a central office for the repression of cybercrime. What is even more impressive is that the Code places an obligation on network operators and trust-service services providers to prioritise cybersecurity within their respective organisations. Comprehensive, if complex, it reflects a civil-law preference for codification.

Togo enacted its cybersecurity and cybercrime law in 2018,[17] establishing a Computer Emergency Response Team, a Security Operating Centre and a National Cybersecurity Agency. It has ratified the Malabo Convention and hosted the Lomé Cybersecurity Summit, presenting itself as a continental advocate for cybersecurity governance.

Burkina Faso is an instructive transitional case. It has no standalone modern cybercrime act and instead relies on its Penal Code and institutional cybersecurity structures, including a Central Brigade for Combating Cybercrime, a national Computer Incident Response Team and the Agence Nationale de Sécurité des Systèmes d'Information. It adopted a National Cybersecurity Strategy from 2019 to 2023, and legislative revision is under way to align domestic law with both the Council of Europe's Convention 108[18] and the Malabo Convention.

Looking Forward: Harmonisation, Vigilance and Proactive Compliance

The adoption of the UN Convention Against Cybercrime in December 2024[19] could mark a turning point in the global governance of cybercrime. If the Convention secures broad ratification and, crucially, ratifying states enact robust, consistent domestic implementing legislation, it could provide the harmonising force the patchwork continental landscape so urgently needs.

Africa's digital transformation is accelerating, and the cybercrime threat is moving with it. The legislative response remains uneven, but momentum is building.

The organisations best placed to navigate this landscape will be those that treat cybercrime compliance not as a box-ticking exercise but rather as a strategic governance imperative, one demanding rigour, resources and board-level attention.

---

[1] Computer Misuse and Cybercrimes Act No 5 of 2018 (Kenya), assented 16 May 2018.

[2] The Computer Misuse and Cybercrimes (Amendment) Bill, 2025, which sought to expand penalties and introduce broader content takedown powers, was subject to conservatory orders by the High Court of Kenya as at mid-2025.

[3] Cybercrimes Act, 2015 (Tanzania), passed 1 April 2015.

[4] See, eg, Article 19 "Tanzania: Cybercrimes Act 2015 Undermines Free Expression" (2015).

[5] Computer Misuse Act, 2011 (Uganda), as amended by the Computer Misuse (Amendment) Act, 2022.

[6] The Constitutional Court of Uganda declared the Computer Misuse (Amendment) Act 2022 null and void in March 2026 on the ground that Parliament had lacked the constitutionally required quorum at the time of passage.

[7] Law No 60/2018 of 25 September 2018 on Prevention and Punishment of Cybercrimes (Rwanda).

[8] Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 (Nigeria), as amended by the Cybercrime (Prohibition, Prevention, Etc) (Amendment) Act, 2024, signed 28 February 2024.

[9] Section 21(3) of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 (as amended 2024).

[10] Section 24 of the 2015 Act was condemned by the ECOWAS Community Court of Justice for its deployment against journalists. The 2024 amendment revised the provision.

[11] The contested 0.5% National Cybersecurity Levy on banks and payment service providers was introduced by the 2024 amendment but subsequently suspended by the House of Representatives following industry opposition.

[12] Cybersecurity Act, 2020 (Act 1038) (Ghana).

[13] Ibid.

[14] Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité (Côte d'Ivoire), as amended by Loi n° 2023-593 of 7 June 2023.

[15] Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité (Senegal). Senegal acceded to the Budapest Convention in December 2016.

[16] Code du numérique, Loi n° 2017-20 (Benin), adopted 13 June 2017, as amended by Loi n° 2020-35 of 6 January 2021.

[17] Loi n° 2018-026 du 7 décembre 2018 relative à la cybersécurité et à la lutte contre la cybercriminalité (Togo).

[18] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), opened for signature 28 January 1981.

[19] United Nations Convention Against Cybercrime (n 3). The Convention enters into force 90 days after the fortieth ratification.

Ahmore Burger-Smidt

Head of Regulatory

View Profile