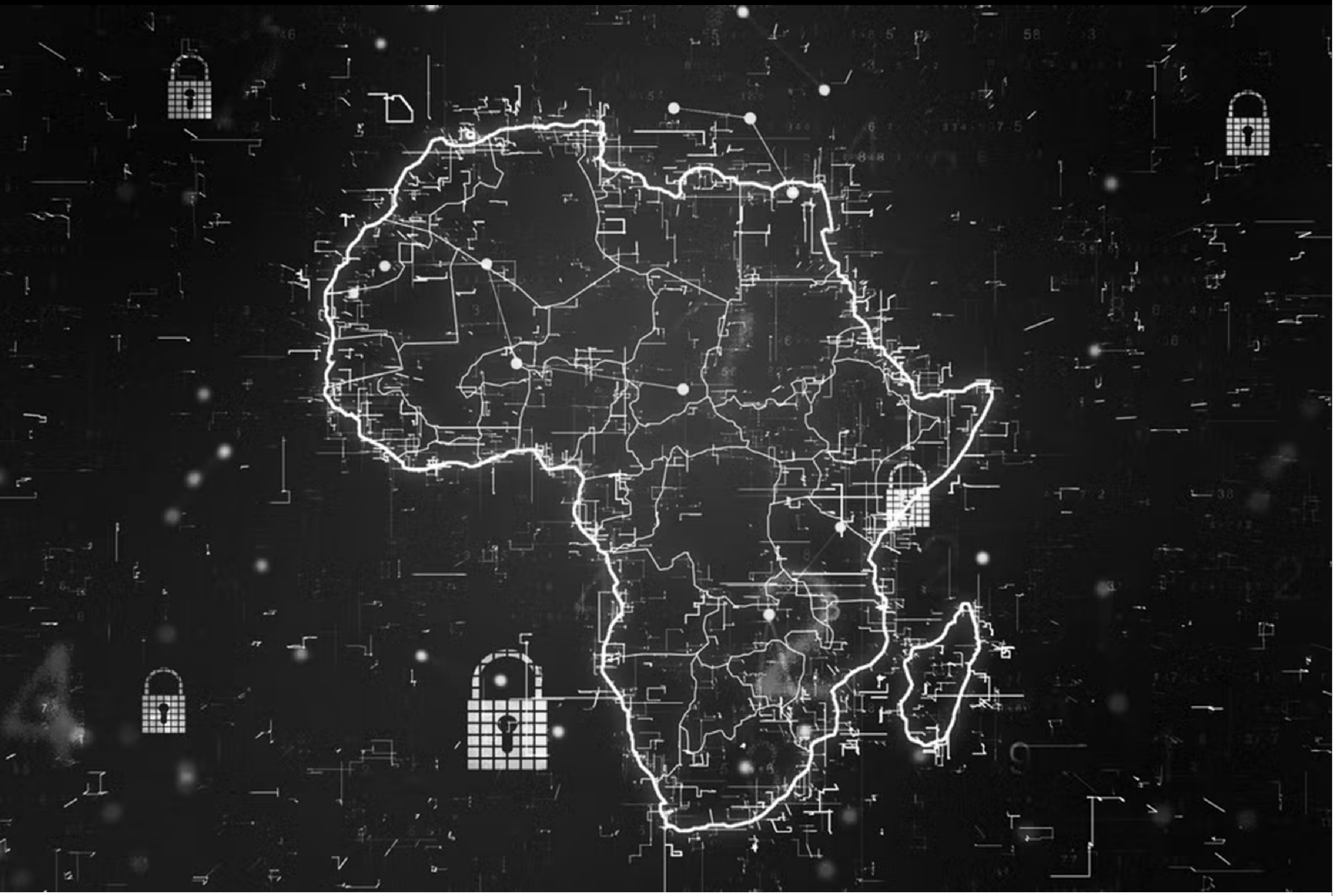
WERKSMANS
ATTORNEYS



DATA PRIVACY | REGULATORY

Cybercrime across borders: Navigating Africa's fragmented legislative landscape – Part 1

17 September 2026 *10 min read*

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

The Compliance Imperative

By the time you reach the end of this sentence, a cyberattack will have been launched somewhere on the African continent. That is not an exaggeration, but rather what has become the new reality on the African continent. Across Africa, financial services are digitising at speed, through mobile banking, cross-border insurance platforms and digital payment ecosystems, creating an attack surface of remarkable breadth and complexity. The laws meant to combat cybercrime and protect the institutions and people who rely on those services, however, remain patchy at best.

Multinational organisations, and specifically financial services and insurance groups operating across Africa do not experience this fragmentation as an academic curiosity. This is a live compliance risk with material consequences. Some jurisdictions have enacted sophisticated, modern cybercrime frameworks with mandatory reporting obligations, dedicated regulators and meaningful penalties. While others have no dedicated cybercrime legislation at all. Interestingly, there are several countries where, enacted cybercrime laws are facing constitutional challenges, adding another layer of uncertainty to the pandemonium. The result? A single multi-jurisdictional entity may face criminal liability for failing to report an incident in one jurisdiction, even as the law of the neighbouring country where the same incident began does not define "cybercrime" at all.

In this two part series, we scrutinised this issue further on what some may describe as a legislative quandary amongst the African countries.

The International Treaty Architecture in Practice

Understanding how the international treaties fit together is crucial for compliance, helping one grasp the global and continental response to cybercrime.

- **The Budapest Convention: A Global Baseline**

Adopted in Budapest in 2001 and later enforced from 2004 onwards,[1] the Council of Europe's Convention on Cybercrime remains the most influential instrument. It has provided the template, or at least the guiding reference point, for domestic cybercrime legislation. Its influence in Africa is expanding: with countries such Senegal acceding to the convention in 2016, and with Rwanda acceding to the convention in 2024. The Convention's real strength lies in its detail on substantive offences, procedural powers, and international cooperation, areas where many African domestic frameworks remain underdeveloped. In essence, the convention has become a yardstick for legislatures across the world on how to draft legislation aimed at adequately addressing cybersecurity issues in their respective countries.

- **The Malabo Convention: A Continental Framework**

The African Union Convention on Cyber Security and Personal Data Protection, adopted in Malabo in 2014,[2] is unique globally: it brings cybersecurity, cybercrime, electronic transactions and personal data protection together in a single instrument. It came into effect on 8 June 2023, after Mauritania's ratification. Yet, as at early 2026, only 20 of the 55 AU member states have ratified it[3], a level of uptake that materially limits its practical harmonising effect.

- **The UN Convention Against Cybercrime: A New Global Layer**

The most important recent development is the United Nations Convention Against Cybercrime, adopted by the UN General Assembly on 24 December 2024 and opened for signature on 25 October 2025 in Hanoi, Vietnam.[4] It is the first comprehensive global treaty devoted exclusively to cybercrime. Its nine chapters cover prevention, criminalisation, procedural measures, international cooperation and capacity building. For African countries reluctant to join the Budapest Convention because it is seen as a "*European*" instrument, the UN Convention offers a multilateral alternative that may carry greater legitimacy. However, its success will depend on the pace of ratification and the quality of domestic implementing legislation.

The harder and more interesting question is whether the political will may one day translate into more sophisticated legislation focused on combating cybercrime across Africa, encouraging optimism for future developments.

Southern Africa: Uneven Progress at the Continent's Economic Hub

- **South Africa: The Leading Framework**

South Africa's Cybercrimes Act[5] is the most comprehensive cybercrime framework in sub-Saharan Africa. Signed on 26 May 2021 and brought into operation in key respects on 1 December 2021,[6] it criminalises unlawful access to data and computer systems, the unlawful acquisition or use of passwords and access codes, and the dissemination of harmful data messages. It repealed and consolidated the earlier cyber-offence provisions in sections 85 to 88 of the Electronic Communications and Transactions Act.[7]

For companies, the Act's dual reporting architecture is the point that matters most. Section 54 requires electronic communications service providers and financial institutions to report cyber offences to the South African Police Service within 72 hours of becoming aware of them; non-compliance is a criminal offence carrying fines of up to R50,000.[8] That duty sits alongside, and does not replace, the separate mandatory data-breach notification regime under section 22 of the Protection of Personal Information Act[9]. One cyber incident can therefore trigger parallel reports to different authorities, under different statutes, with different timelines and thresholds. Compliance teams need to be alert to that reality.[10]

- **Namibia: A Legislative Gap**

Namibia may present the Southern African Development Community's most significant legislative gap. No dedicated cybercrime act is currently in force. The Electronic Transactions Act of 2019[11] deals with electronic commerce but does not create cybercrime-specific offences. Draft Cybercrime and Data Protection Bills were circulated as early as 2013 and remain unpromulgated. Before the Electronic Transactions Act, the principal instrument was the Computer Evidence Act of 1985[12], a statute drafted long before the internet had any meaningful commercial presence in the world. Namibia has ratified the Malabo Convention and began a Commonwealth-assisted process in 2020 to develop cybersecurity strategy components, but progress has been slow. The gap means that cybercrime prosecutions must rely on general criminal-law principles, far from a satisfactory position.

- **Botswana, Zimbabwe, Zambia and Eswatini**

By continental standards, Botswana moved early, enacting its Cybercrime and Computer Related Crimes Act in 2007[13]. In 2018 a further development was made in Botswana, with the country's legislature promulgating a new piece of legislation which repealed the 2007 enactment. Though plausible, the 2018 enactment does not adequately address concerns regarding cybersecurity at the level it should given the limited number of new provisions which were introduced in the amendment Act, the Act therefore takes a reactive stance rather than proactive posture when it comes to the subject of cybersecurity.

Zimbabwe's Cyber Security and Data Protection Act of 2021[14] is distinctive in bringing cybersecurity, cybercrime and data protection under one statute which is regulated by the Postal and Telecommunications Regulatory Authority. Civil society organisations, however, have strongly condemned provisions said to permit government interference with private communications without adequate judicial oversight.[15] The tension is familiar across the continent: cybercrime laws can be deployed, or be perceived as deployable, as instruments of surveillance and political control.

Zambia's Cyber Security and Cyber Crimes Act is currently before the High Court in a pending constitutional challenge. Akin to the situation in Zimbabwe, civil society organisations have raised a number of concerns on provisions, which apparently threaten the constitutional right to freedom of expression for Zambians.[16] Until the challenge is resolved, the Act remains in force, but legal uncertainty hangs over it, a difficult position for compliance teams seeking a clear regulatory baseline.

Eswatini enacted the Computer Crime and Cybercrime Act which came into effect on 4 March 2022. At a high level, the Act criminalises various cyber offences and makes provision for the establishment of a National Cybersecurity Incident Response Team and National Cybersecurity Advisory Council. Moreover, the Eswatini Government has also adopted a five year National Cybersecurity Strategy with the aim of protecting key national infrastructure and to mitigate any risks of cybercrime within the Eswatini cyberspace.[17] This Act coupled with the country's own Data Protection Act, displays Eswatini's strong commitment to addressing and combating cybersecurity, a country riddled by growing threats of cybercrimes as reported by Eswatini Communications Commission.[18]

- **Mozambique, Lesotho, Malawi and Mauritius**

Mozambique has no distinct national cybercrime framework and instead relies on partial measures. It has ratified the Malabo Convention but has not enacted dedicated implementing legislation. Lesotho presents a confirmed legislative gap: no cybercrime statute has been identified. While a Computer Crime and Cybersecurity Bill was tabled before the National Assembly in 2024, it has not yet been enacted into law amidst significant scrutiny and opposition from media and civil society.[19] In 2024, Malawi enacted cybercrimes legislation replacing the data-protection provisions of the country's Electronic Transactions and Cyber Security Act. Impressively, the Act is inspired by the GDPR introducing amongst others: data-subject rights, mandatory breach notification; this signals that Malawi is indeed headed towards the right direction in its commitment to improving the country's cybersecurity laws.

Mauritius, by contrast, offers a regional model. Its Cybersecurity and Cybercrime Act of 2021,[20] enacted on 19 November 2021, replaced the earlier Computer Misuse and Cybercrime Act of 2003. It establishes a National Cybersecurity Committee and the Computer Emergency Response Team of Mauritius, and aligns with both the Budapest Convention and the Malabo Convention. Mauritius shows what a small island state can achieve when political will exists: a framework that meets international standards.

Conclusion

It is clear that there are disparities amongst the African countries discussed above in relation to the approach to cybersecurity. Certain countries can be seen to take proactive measures to address an issue which is becoming more prevalent as societies become more digitised and make use of emerging technologies. While in countries such as Malawi, the importance of cybersecurity is simply not prioritised. In the end, multi-jurisdictional entities are confronted with a compliance dilemma insofar as it concerns how to deal with cyberattacks in various jurisdictions in light of the fragmentation and lack of uniformity of cybercrime legislation across the African continent.

In part two, we delve into this issue further – where shockingly we find that cybercrime legislation in some African countries is potentially being used as a means for censorship rather than for its intended purpose – curbing cybercrime!

---

[1] Convention on Cybercrime, opened for signature 23 November 2001, Budapest; entered into force 1 July 2004. ETS No 185.

[2] African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014 in Malabo, Equatorial Guinea; entered into force 8 June 2023.

[3] See African Union Commission Status List of the OAU/AU Treaties, Conventions, Protocols and Charters (2025).

[4] United Nations Convention Against Cybercrime, adopted by UN General Assembly Resolution 79/243 on 24 December 2024; opened for signature 25 October 2025 in Hanoi, Vietnam.

[5] Cybercrimes Act 19 of 2020.

[6] The key operative sections of the Cybercrimes Act commenced on 1 December 2021 following Presidential signature on 26 May 2021.

[7] Sections 85–88 of the Electronic Communications and Transactions Act 25 of 2002 (ECTA), repealed by the Cybercrimes Act.

[8] Section 54 of the Cybercrimes Act 19 of 2020.

[9] Section 22 of the Protection of Personal Information Act 4 of 2013.

[10] Burns Y and Burger-Smidt A Protection of Personal Information: Law and Practice 2nd ed (2023) LexisNexis ch 1.

[11] Electronic Transactions Act 4 of 2019 (Namibia). A draft Cybercrime Bill and Data Protection Bill were circulated in 2013 but remain unpromulgated.

[12] Computer Evidence Act 32 of 1985 (Namibia).

[13] Cybercrime and Computer Related Crimes Act (Botswana), enacted 2007.

[14] Cyber Security and Data Protection Act (Zimbabwe), 2021.

[15] See, eg, Zimbabwe Human Rights NGO Forum "Analysis of the Cyber Security and Data Protection Act" (2021) noting provisions enabling state interception of private communications without adequate judicial oversight.

[16] Cyber Security and Cyber Crimes Act (Zambia). At the time of writing, the constitutional challenge remains pending before the High Court of Zambia.

[17] Cybersecurity law & regulation in eSwatini (2026) by Anurag Verma.

[18] Eswatini Faces Rising Cybercrime Threats: ESCCOM Warns of Facata Scams and Online Fraud by Eswatini Observer (2025).

[19] Repressive cybercrime law poses grave threat to Lesotho's fragile democracy by Daily Maverick (2024).

[20] Cybersecurity and Cybercrime Act 2021 (Mauritius), enacted 19 November 2021, superseding the Computer Misuse and Cybercrime Act 2003.

Ahmore Burger-Smidt

Head of Regulatory

View Profile