SAIPAR | Government of Ireland International Development Programme

THE CYBER CRIMES AND THE CYBER SECURITY ACTS: THE GOOD AND THE BAD

NUMBER 1, MAY 2025

POLICY BRIEF

THE CYBER CRIMES AND THE CYBER SECURITY ACTS: THE GOOD AND THE BAD

BY O'BRIEN KAABA

"What happens when bad guys take advantage of the digital spaces to undermine the offline world?"[1]

INTROUDCTION

President Hakainde Hichilema assented to the Cyber Security Act No 3 of 2025 and the Cyber Crimes Act No 4 of 2025 on 8th April 2025. The two statutes, however, will only come into force upon the issuance of the Commencement Orders by the President and responsible minister, respectively. The two Acts are intended to repeal and replace the Cyber Security and Cyber Crimes Act No 2 of 2021, which has been strongly criticized for limiting human rights.

The two new laws represent government's growing interest to control or secure the cyber space. The exponential growth of computer technology and increased penetration of the internet have drastically transformed opportunities and spaces for human interaction as well as accessing services from government and other service providers. Many government services, commerce and routine communication now heavily depend on the virtual space created by computer technology and networks. This, however, comes with significant risks as criminals often take advantage of the cyber space to advance their own goals. As Mark Young warned:

> This access comes with significant risk. Criminals, terrorists, hostile nation-states, and foreign industrial competitors share this ubiquitous access to information. In the industrial age, we protected ourselves with high walls and long-range weapons; in the digital age, the availability and rapid development of cyber weapons requires layers of defenses and improved awareness of adversarial capabilities and intentions.[2]

The advancement of technology has also led to the blossoming of social media and allowed people to express themselves in ways conventional media outlets could not allow. As a result, the online platforms have become foras of communication, debate, dialogue and exchange of ideas in ways never imagined before. But even here, dangers lurk. Reputations can be unjustifiably damaged, threats and harassment flourish and various forms of harm instigated. As Nanjala Nyabola noted:

> However, it is not all rosy. Social media platforms can be toxic spaces that replicate offline harm. Violent acts are encouraged and distributed on these platforms, such as politicians threatening physical violence against their opponents.[3]

[1] *Nanjala Nyabola, Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya (Bloomsbury Publishing Plc, 2021) xxiii*
[2] *Mark D Young, "Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security," (2011) 6 Stanford Law and Policy Review 11- 40*
[3] *Nanjala Nyabola, Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya (Bloomsbury Publishing Plc, 2021) 6.*
See also International Commission of Jurists, Regulation of Communication Surveillance and Access to Internet in Selected African Countries (ICJ, 2021)

To mitigate harm and to ensure optimal enjoyment of human rights in the cyber space, it is inevitable that cyberspace, just like offline space, be regulated. Inevitably, some harmful conduct has to be criminalized and law enforcement agencies empowered with appropriate tools of investigation and surveillance proportionate to the anticipated harm. Article 25(1) of the African Union Convention on Cyber Security and Personal Data Protection 2014, for example, enjoins states parties to enact laws to criminalise harmful conduct in cyberspace in order to protect citizens:

> Each state party shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive, criminal offence acts which affect confidentiality, integrity, availability, and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders.

However, considering that the cyberspace is primarily a theater of human rights, any intervention by the state should not lead to scaling down on the human rights enjoyed by citizens. The regulation of cyber space, therefore, has to find the right balance between appropriate state intervention and safeguarding human rights. It is for this reason that article 25(3) of the African Union Convention on Cyber Security and Personal Data Protection 2014 requires of states that:

> In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each state party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

This policy brief highlights how the Cyber Security Act No 3 of 2025 and the Cyber Crimes Act No 4 of 2025 balance off the need to criminalise harmful conduct online and the need to equip law enforcement agencies with appropriate investigative skills and powers, on the one hand, and the need to safeguard the rights of individuals on the other hand. It does this by pointing out provisions that appear progressive and those that are of concern. The analysis is through the lens of international human rights law and comparative best practices.

NOTABLE POSITIVES

(a) Criminalizing harmful conduct

The Cyber Crimes Act criminalises several aspects of harmful conduct in relation to cyber space.[4] These include prohibition of the following: unauthorized access to computer system; interference with computer system; unauthorized disclosure of data relating to critical infrastructure; illegal acquisition of data; introduction of malicious software into a computer system; illegal system interference; recording of private conversation without notifying the parties; computer misrepresentation and fraud; cyber extortion; identity theft; child pornography; child solicitation and grooming; online human trafficking; transmission of unsolicited deceptive electronic communication; harassment and humiliation; and cyber terrorism.

In terms of scope, the listed crimes appear generally consistent with crimes recommended for criminalization in international treaties (although, of course there are some crimes poorly crafted and in some cases the sentences look excessive). For example, the Council of Europe's Convention on Cybercrime (Budapest) 2001 lists the following as criminal offences in cyberspace: illegal access; illegal interception; data interference; system interference; misuse of devices; computer-related forgery and fraud; child pornography; and infringements of copyright.[5] Similarly, the African Union Convention on Cyber Security and Personal Data Protection 2014 outlaws many similar forms of misconduct in relation to cyberspace.[6]

An impression, should, therefore, not be created that, harmful conduct online, such as hate speech, is more tolerable than when it is offline. Indeed, may countries have responded strongly to such cybercrimes. In the case of R v Jordan Parlour [2024] EWHC 2323 (Ch), for example, the English courts convicted Jordan Parlour and sentenced him to 20 months imprisonment for his Facebook

[4] *See part II of the Cyber Crimes Act No 4 of 2025*
[5] *See Articles 2 to 12 Convention on Cybercrime (Budapest) 2001.*
[6] *See articles 29 to 31 African union Convention on Cyber Security and Personal Data Protection 2014.*

posts encouraging attacks on immigrants. One of his posts on Facebook, for example, read: “Every man and their dog should be smashing f*** out Britannia Hotel.” Similar examples of convictions for social media expression of hatred include the case of Austria / Higher Regional Court Vienna / 18 Bs 339/18m, where a woman posted on Facebook, calling refugees as "human garbage" and "deranged, criminal, escaped murderers"; in the case of Luxembourg / First Instance Court of Luxembourg City / no. 1005/2022 the defendant referred to refugees on Facebook as “like monkeys.”[7]

(b) Inadmissibility of Illegally obtained evidence

Section 62 of the Cyber Security Act limits the admissibility of evidence obtained as a result of an illegal interception of communication without leave of Court as follows:

“Despite any other law, evidence which is obtained by means of an interception effected in contravention of this Act, shall not be admissible in any criminal proceedings except with the leave of the court, and in granting or refusing such leave, the court shall have regard to the circumstances in which the evidence was obtained, the potential effect of its admission or exclusion on issues of national security and the unfairness to the accused person that may be occasioned by its admission or exclusion.”

This provision significantly modifies the law on the admissibility of illegally obtained evidence as a result of unlawful interception of communication. The Supreme Court in the cases of Liswaniso v The People (1976) ZR 272 and Liswaniso Sitali and Others v Mopani Copper Mines PLC (2004) ZR 176 set dangerous precedents admitting evidence obtained even in violation of constitutional norms and human rights. Section 62 of the Cyber Security Act now entails that these precedents cannot stand in relation to evidence obtained as a result of an illegal interception of communication.

AREA OF MAJOR CONCERN: MASS SURVEILLANCE

While the Cyber Security Act, appears to put in place measures to prevent illegal interception of communication (sections 22, 29 and 30), it seems at the same time, allows mass surveillance. This is the elephant in the room. Section 39 of the Cyber Security Act requires an electronic communication service provider to use an electronic communication system that is capable of being intercepted; install hardware and software capable of being intercepted; provide services that are capable of real time and fulltime monitoring and interception of communication; provide all call-related information in real time or as soon as possible; provide interface from which intercepted communication should be channeled to the Central Monitoring and Coordination Centre; transmit intercepted communication to the Centre; and provide access to all intercepted subjects to operating temporarily or permanently within the service provider’s communication system.[8]

The Act further stipulates that despite any other written law, an electronic communication service provider shall provide service which has capability of being intercepted and that the service provider shall store call-related information or internet connection records in accordance with the Act.[9]

These provisions clearly establish a system that allows for the collection and surveillance of electronic data, records and communications that may lead to violations of the right to privacy and freedom of expression. Although surveillance is a necessary too for maintaining national security and fighting crime, it must be done in a manner that balances the human rights of individuals. To avoid encroaching on human rights, surveillance must be particularized and specifically targeted. It should not be generalized. The state should in fact be promoting privacy enhancing technology and not demand from service providers to install surveillance enhancing gadgets. The African Commission on Human and Peoples’ Rights, in a 2023 Resolution, summarized the state obligation in this regard as the duty to:

> Promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards.[10]

[7] *For a detailed discussion of these cases, see Chaloka Beyani, “R v Jordan Parlour[2024] EWHC 2323: Punishing Inciting Racial Hatred Through Social Media” (2024) Saipar Case Review, 1-6*
[8] *Section 39(1) Cyber Security Act No 3 of 2025*
[9] *Ibid, section 40(1)*
[10] *Para iv Resolution on the Deployment of Mass and Unlawful Targeted Communication Surveillance and Its Impact on Human Rights in Africa – ACHPR/Res. 573 (LXXVII) 2023*

The South African Constitutional Court in Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others CCT 279/19, declared as unconstitutional, provisions allowing for bulk or mass surveillance akin to those in the Cyber Security Act, for potentially violating freedom of speech and privacy. The court noted that the law had "no legal limits placed on how data obtained through bulk surveillance is captured, copied, stored, analysed, or distributed; this unregulated, untargeted surveillance of all information is an extreme violation of the right to privacy."

The Court further noted the significance of freedom of speech and privacy and how surveillance may impact them:

> By nature, human beings are wont – in their private communications – to share their innermost hearts' desires or personal confidences, to speak or write when under different circumstances they would never dare do so, to bare themselves on what they truly think or believe. And they do all this in the belief that the only hearers of what they are saying or the only readers of what they have written are those they are communicating with. It is that belief that gives them a sense of comfort a sense of comfort either to communicate at all; to share confidences of a certain nature or to communicate in a particular manner. Imagine how an individual in that situation would feel if she or he were to know that throughout those intimate communications someone was listening in or reading them.

The Courts in Kenya took a similar approach in the cases Okoiti v Communications Authority of Kenya [2017] eKLR and Kenya Human Rights Commission v Communications Authority of Kenya Petition No 86 of 2017 by declaring as unconstitutional, the decision to install gadgets that would potentially allow for mass interception of communication for violating the right to privacy.

CONCLUSION AND RECOMMENDATIONS

Cyberspace plays a dominant role in human interactions and provision of services. It is also a major forum for the exercise of human rights, especially freedom of speech and the right to privacy. While there might be genuine need for the regulation of cyberspace by the government, any intervention must strike the right balance in that it must not undermine the enjoyment of human rights. It seems, in terms of the scope of conduct criminalized, the newly enacted laws generally mirror conduct which is recommended for criminalization in relevant treaties. However, this does not necessarily entail that the crimes have been appropriately crafted. In some cases, the sentences appear excessive.

The major concern, however, is the potential for mass surveillance. The law is not particularlised to specific forms of harm when it comes to surveillance. It lacks effective control, accountability and oversight mechanisms that would ensure it is not abused. The provisions on surveillance are at variance with human rights standards as they are a gross danger to privacy and freedom of expression. The government must consider amending the two laws to refine the definition of crimes, rethink the sentences and make them proportional to the likely harm, and overhaul the framework for surveillance in order to align it with international human rights standards.

For further information contact:
Tel: +260 761327702
Email: marja.hinfelaar@saipar.org
Address: SAIPAR, 32a District Road, Lusaka