How Africa can up its game

Yarik Turianskyi considers cybercrime and data privacy, and argues that Africa urgently needs to respond to these challenges

Africa is the fastest-growing continent when it comes to internet penetration. The percentage of people on the continent using the internet increased from a mere 2.1% in 2005 to 24.4% in 2018, according to the International Telecommunication Union (ITU), a specialised UN agency. Yet, while more African citizens are becoming connected, there are concerns about disregard for personal data by social media networks, the prominence of fake news and the growth of cybercrime.

African leaders are scheduled to meet at the upcoming AU Summit in February. While this year's theme is *Silencing the Guns: Creating Conducive Conditions for Africa's Development*, they should allocate enough time to discuss matters of cyber governance, data privacy and internet freedoms to adequately respond to these challenges.

The AU adopted the Convention on Cybersecurity and Personal Data Protection in 2014, but by January 2020 only 14 of the 55 AU member states had signed it and only seven had ratified it. This means that the convention is not yet in force, as it requires ratification by at least 15 member states. It also raises questions about the political will of AU members to adopt necessary legislation to protect their populations in the digital realm.

Legislation and regulation are crucial to enable the rights of citizens on the internet and protect them from cybercrime and the unauthorised use of personal data. A careful balancing act is required to ensure that there are appropriate regulations and systems in place to protect the data of citizens and allow government to deal with cybercrime without infringing on online freedoms or providing opportunities for security services to spy on their citizens. Although some AU states have passed cybersecurity and data-protection laws, these are often vaguely worded and used to stifle political dissent rather than to protect citizens.

The internet was supposed to bring about an era of openness, freedom and democracy. Unfortunately, like any technology, it can be used for positive as well as negative ends. Many African governments regularly shut down

social media sites and/or messaging apps, or even cut off access to the internet entirely during or after elections or in response to protests.

In 2018, there were 21 partial or total internet shutdowns — an increase from 13 in 2017 and four in 2016. Authoritarian governments, in Africa and globally, are increasingly using the internet as a propaganda outlet to monitor citizens and silence dissidents.

A multi-stakeholder approach that specifically includes technology firms alongside civil society, business and policymakers may be one of the important ways to move forward in addressing these challenges

What should the AU do?

Firstly, it clearly needs to put more effort into encouraging its member states to sign and ratify the above-mentioned convention. Secondly, it needs to ensure that all subsequently passed domestic legislation is drafted with respect of the rule of law and human rights. The second point, however, may be a stretch for the continental organisation acting alone.

This is where multi-stakeholder initiatives (MSIs) could come in. These initiatives bring together governments, civil society and businesses at both domestic and international levels to collectively improve governance. Two such initiatives are prominent in Africa: the African Peer Review Mechanism (APRM), with 38 members, and the Open Government Partnership (OGP), with 14.

Domestic laws are often insufficient as technology is borderless. Protecting personal data and fighting cybercrime requires international coordination. Policymakers need to work with technology experts to stay up to date with the latest developments, as well as to ensure that regulation does not stifle innovation. MSIs can be useful in both instances, promoting best practices and cooperation across borders.

They also represent a modern and progressive approach that recognises that governments do not have all the answers; and elevate the position of other key actors involved in these issues. Indeed, given the complexity of internet governance and the role of non-state actors, such as multinational technology firms, it is a worthy path to pursue.

One AU member, Mauritius, is already setting a good example of implementing a holistic cyber strategy. It was the first African state to become a party to the Budapest Convention on Cybercrime in 2014, the second non-European

state to ratify of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and it ratified the AU Convention on Cybersecurity and Personal Data Protection in 2018.

Subsequently, Mauritius adopted comprehensive data protection laws, a national cyber policy, data privacy regulators and established a central authority to champion these processes. The country ranked among the top three in Africa in the 2018 ITU Global Security Index, achieving first place in the technical, organisational and capacity-building pillars.

Although the AU should be commended for establishing a continental convention on data privacy and cybersecurity, it needs to do more to encourage member states to establish legislation at the domestic level to protect citizens while operating within the confines of the rule of law and respecting human rights.

It has previously cooperated with the Council of Europe and the Internet Society on cyber policies and should continue to do so in the future, while also bringing other actors on board.

Maintaining a balance between protecting citizens from cybercrime and maintaining their internet freedoms is indisputably difficult and further complicated by the fact that technology tends to be years ahead of policy.

A multi-stakeholder approach that specifically includes technology firms alongside civil society, business and policymakers may be one of the important ways to move forward in addressing these challenges. ■

Yarik Turianskyi is the Deputy Head of the African Governance and Diplomacy Programme at the South African Institute of International Affairs

This piece is based on his latest Policy Insights, "Africa and Europe: Cyber governance lessons".