Policy Insights
77
January 2020

Africa and Europe: Cyber Governance Lessons

YARIK TURIANSKYI

African perspectives
Global insights

SAIIA
SOUTH AFRICAN INSTITUTE
OF INTERNATIONAL AFFAIRS

Executive summary

This Policy Insights examines the lessons the AU can learn from the EU in the area of cyber governance. The AU has recently adopted one document in this respect, the 2014 Convention on Cyber Security and Personal Data Protection. This convention imposes obligations on signatories to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. However, five years since its adoption, only 14 of 55 AU member states have signed it and seven have ratified it. In order for the convention to come into force it must be signed and ratified by a minimum of 15 states. The AU therefore needs to work with its members to encourage them to ratify the convention and establish the cyber legislation necessary to protect their citizens, while operating within the confines of the rule of law and respecting human rights.

Introduction

Much of the contemporary discourse on the governance of the Internet focuses on legislating cyberspace. Almost 30 years have passed since the Internet became commonplace in society, yet there are now more arguments than ever on the need to legislate both it and related technologies. This paper uses case studies of the AU and the EU to analyse the way they have approached this task. While both have passed appropriate legislation, the EU has adopted a more nuanced approach, which the AU could learn from. This paper then looks at the AU Convention on Cyber Security and Personal Data Protection, the reasons for the lack of ratification, as well as other relevant processes relating to cybersecurity at the continental level. It ends with practical recommendations on how the AU could improve the status quo in cyber governance in Africa.

Background

The mass adoption of the Internet in the 1990s brought about an era of hope and optimism. Here was a platform that enabled instant communication and the sharing of and access to information. Early proponents claimed that access to the Internet would democratise societies in the long run. However, as *The Economist* points out: 'These days it is the Internet's defects, from monopoly power to corporate snooping and online radicalisation, that dominate the headlines.'[1] Indeed, disregard for personal data by social media networks, the prominence of fake news and deep fake content, as well as the growth of cybercrime have dampened the early enthusiasm for connected societies. There is also an increase in cyber fatigue, as Internet users are constantly bombarded with privacy and safety warnings.

[1] *The Economist*, 'Chips with everything', 14 September 2019.

Disregard for personal data by social media networks, the prominence of fake news and deep fake content, as well as the growth of cybercrime have dampened the early enthusiasm for connected societies

At the outset of the digital age in the 1990s, it was hoped that technology would inevitably bring about more openness, freedom and democracy. Unfortunately, since then authoritarian states have learnt how to manipulate technologies to silence dissidents and use the Internet as a propaganda outlet. These states furthermore cite security concerns, claiming protection of their citizens when they limit their rights to access social media platforms and messaging apps. The rise of fake news in a post-truth world[2] has indeed been exploited by certain politicians, who create their own narratives as part of information warfare against local and foreign dissenters and critics. Anyone who has an opposing point of view is typically labelled as a 'foreign agent'. This is often followed by attacks on the person's integrity and character on social media and may be coupled with physical harassment or intimidation in the real world.

However, now that humanity is no longer viewing technology through rose-tinted glasses, it may be more mature about the regulations required. The road ahead is not paved or even well lit. Legislation and regulation are necessary to both enable the rights of citizens on the Internet and protect them from cybercrime and the unauthorised use of personal data. Governments need to perform a balancing act in these matters to ensure that there are appropriate regulations in place that allow them to deal with cybercrime without infringing on online freedoms or providing opportunities for security services to spy on their citizens. Maintaining a balance between protecting citizens from cybercrime and maintaining their Internet freedoms is indisputably difficult and is further complicated by the fact that technology tends to be years ahead of policy. Therefore, 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.

The structure of the Internet itself, which comes down to interconnected networks using standardised routing protocols and websites that may reside anywhere in the world, even on privately owned infrastructure, exacerbates the regulatory problems resulting in jurisdictional issues. The Internet is decentralised and so is its governance, yet the rate at which people are connecting is also increasing dramatically and cybercrime repression requires international coordination. Domestic laws are insufficient – technology is borderless. Furthermore, global solutions tend to be challenging to implement, given the

[2] In a post-truth world 'experts are dismissed, alternative facts are (sometimes flagrantly) offered, and public figures can offer opinions on pretty much anything'. See *The Guardian*, 'We're in a post-truth world with eroding trust and accountability: It can't end well', https://www.theguardian.com/commentisfree/2017/nov/17/were-in-a-post-truth-world-with-eroding-trust-and-accountability-it-cant-end-well, accessed 10 July 2018.

multitude of perspectives, ideologies and technical requirements. Significant differences remain between countries on how the Internet should be governed and it is unlikely that consensus will be reached any time soon. In addition, there are ideological divisions on the standardisation of data protection and Internet usage. The extreme sides of this debate propagate either no data privacy regulations whatsoever or extremely strict ones, which would make conducting business untenable. These divisions are similar to between those countries that make no effort to control or regulate Internet usage and those which strictly control it.

> The structure of the Internet itself, which comes down to interconnected networks using standardised routing protocols and websites that may reside anywhere in the world, even on privately owned infrastructure, exacerbates the regulatory problems resulting in jurisdictional issues

Debates on Internet governance start with its very definition, which is reflected in various perspectives, approaches and policy interests. Computer specialists focus on standards and applications, human rights activists are concerned with freedom of expression and privacy, while policymakers view it through the prism of cybersecurity.[3] Two camps can be identified: those advocating for multi-stakeholder governance of the Internet, on the one hand, and those in favour of state control, on the other.[4] Multi-stakeholder governance of the Internet is indeed an interesting idea. Currently, many global initiatives exist to address development challenges, entrench democratic practices and strengthen regulatory frameworks through multi-stakeholder partnerships between governments, civil society and the private sector.[5] This is seen as a modern and progressive approach that recognises that governments do not have all the answers and elevates 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 approach to pursue. However, not everyone agrees with it. Some governments see social control as a goal and are therefore open to establishing surveillance techniques at the state level. Debates about 'big data',[6] including governments and companies collecting information on citizens'

[3] Kurbalija J, *An Introduction to Internet Governance* (6th ed), https://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf, accessed 23 October 2019.

[4] New America, 'Internet Governance and Today's Context', https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/internet-governance-and-todays-context/, accessed 24 October 2019.

[5] Gruzd S *et al.*, 'Multi-Stakeholder Initiatives: Lessons Learned'. SAIIA Research Paper, April 2018, https://saiia.org.za/wp-content/uploads/2018/08/2018-MSIs-Lessons-Learned-Summary.pdf, accessed 24 October 2019.

[6] There are many definitions of 'big data'. For the purposes of this paper, it makes sense to define it as large datasets made available through modern technologies and consumer devices, including among other things smartphones and social media posts, sensors such as traffic signals and utility meters, point-of-sale terminals, consumer wearables such as fit meters, electronic health records. Adapted from University of Wisconsin, 'What is big data?', https://datasciencedegree.wisconsin.edu/data-science/what-is-big-data/, accessed 24 October 2019.

and consumers' online payments, social media posts, health records and credit history, are relatively recent. However, Zbigniew Brzezinski, an American diplomat and academic, saw this potential dark side of technology in terms of privacy and surveillance as far back as 1971:[7]

> [T]he capacity to assert social and political control over the individual will vastly increase. It will soon be possible to assert almost continuous surveillance over every citizen and to maintain up-to-date, complete files, containing even most personal information about the health or personal behaviour of the citizen in addition to more customary data. These files will be subject to instantaneous retrieval by the authorities.

Brzezinski's words become increasingly concerning when read in the context of the latest technological advances, such as artificial intelligence, machine learning and behaviour analytics. Together these would allow unprecedented levels of surveillance by governments which are not concerned with the privacy of their citizens.

Global agreements on Internet freedoms and the protection of personal data are highly unlikely, given the vast ideological differences that exist

Global agreements on Internet freedoms and the protection of personal data are highly unlikely, given the vast ideological differences that exist. The idea of 'cyber sovereignty', that is, that states should be able to manage and contain their own Internet without external interference, which is propagated by countries like China, is illustrative in this context. This can mean partially cutting citizens off from global Internet services, service engines and websites. There are concerns that China's Belt and Road Initiative, a global development strategy, and specifically one of its subcomponents – the Digital Silk Road – will encourage recipient countries to adopt a similar model.[8] It is also worth mentioning the difference in existing data laws worldwide. Some countries insist that all or some specific data collected from its citizens must be stored and processed on servers located within its borders or in countries with equal and/or better data privacy regulations. In Russia this includes personal data, in Nigeria and Sweden government data, and in Australia and the US health records.[9] Others have not passed such legislation.

[7] Brzezinski Z, 'Moving into a technetronic society,' in *Information Technology in a Democracy*, Harvard University Press. Cambridge, Mass., 1971, pp. 161–7.

[8] *Nikkei Asian Review*, 'Beijing exports "China-style" internet across Belt and Road', 21 October 2019, https://asia.nikkei.com/Spotlight/Belt-and-Road/Beijing-exports-China-style-internet-across-Belt-and-Road, accessed 24 October 2019.

[9] Chander A & PL Uyen, 'Data nationalism', *Emory Law Journal*, 64, 3, 2015, http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html#section-c94d487f630c275b466ee7e3d3dc7114, accessed 24 October 2019.

Regional approaches may thus represent the best solution at this point in time. The EU, with its 28 member countries (the UK was still a member at the time of writing), offers an early example of what is possible. The broad commitment of members to the same political and economic values and principles allows the EU to establish uniform policies and regulations within its single market. Because of this, the EU is already seen as a 'norm entrepreneur' in cyberspace,[10] following the implementation of its General Data Protection Regulation (GDPR) in 2018, which was one of the first attempts to establish uniform rules, albeit across member states of a single political and economic community. A 'norm entrepreneur' is defined as 'a normative or value-driven leader or institution that encourages its constituency to uphold a range of norms for the improvement of the livelihood of the people who are subject to that constituency's jurisdiction or authority'.[11] Notably, there were already other initiatives prior to the GDPR, including the 1995 EU Data Protection Directive[12] (which the GDPR replaced) and the 2016 European Union Directive on Network and Information Security,[13] which aimed at improving cybersecurity.

The EU has since continued its efforts to create norms and rules through the introduction of the Cybersecurity Act, which will create a permanent and well-funded cybersecurity agency for the EU. This will be achieved by reinforcing the role and mandate of the current European Network and Information Security Agency (ENISA), which was originally established in 2004 with non-permanent agency status and limited funds. The Act furthermore establishes an EU framework for cybersecurity certification to boost the cybersecurity of online services as well as consumer devices.[14]

What are the lessons the AU can learn from the EU in the area of cyber governance? The AU was launched in 2002, with an institutional setup that closely resembled its European counterpart – a feature that was picked up by many observers at the time. Indeed, even at the July 2001 Organisation of African Unity (OAU) Summit in Lusaka, Zambia, which focused on the transition to the AU, 'several references were made to the African Union being loosely based on the European Union model.'[15] Similarities in the institutional model notwithstanding, the two bodies also differ greatly in their influence over member states, operational procedures and resources. The issue of a common market is also a key differentiator, with the EU being truly borderless, allowing for free movement of people and a single currency. While the AU has some way to go, the African Continental Free Trade Area (AfCFTA), which entered into its operational phase in 2019, is similarly paving

[10] Doninioni S, 'The (geo)political meaning of Europe's Cybersecurity Act', Istituto per gli Studi di Politica Internazionale (ISPI), https://www.ispionline.it/it/pubblicazione/geopolitical-meaning-europes-cybersecurity-act-22870.

[11] Murithi T, 'The African Union at ten: An appraisal', *African Affairs*, 111, 445, 2012, p. 663.

[12] European Commission, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data', https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

[13] European Commission, 'The Directive on Security of Network and Information Systems (NIS Directive)', https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[14] European Commission, 'Cybersecurity Act', 11 December 2018, https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

[15] Babarinde O, 'The EU as a Model for the African Union: The Limits of Imitation', Jean Monnet/Robert Schuman Paper Series, 7, 2, April 2007.

the way for 'a common market for goods, services and investment and allowing the free movement of persons'.[16] Although the AU's 55-state membership will make it difficult to achieve consensus, and its structures do not provide it with the same authority as its European counterpart, it can nonetheless play an important normative role in promoting digitalisation on the continent and establishing common rules in the cybersphere. Indeed, since its establishment the AU has attempted to play a continental role as a norm entrepreneur through, for example, the adoption of Agenda 2063 – a 50-year development plan for Africa.[17] Increased efforts to establish continent-wide legislation on cyber governance should be its next goal, given its importance in 'mitigating emerging cyber risks and managing the growing complexity of cyberspace.'[18]

The AU should thus consider adopting and learning from some of the best practices and norms already established by the EU in cyber governance. Africa is the fastest growing continent in terms of Internet penetration. The International Telecommunications Union (ITU), a specialised UN agency, estimates that in Africa 'the percentage of people using the Internet increased from 2.1% in 2005 to 24.4% in 2018'.[19] Yet, while Europe has the slowest growth rates, it also has the highest proportion of the population already using the Internet – 79.6%.[20] Although Africa is currently behind, it is quickly catching up and has the benefit of learning from European experience, while building on this to help establish a safe and secure cyberspace environment for its people.

> Africa is the fastest growing continent in terms of Internet penetration

Current AU legislation

The only document available at the AU level is the Convention on Cyber Security and Personal Data Protection, which was adopted in 2014 as part of Agenda 2063.[21] As of October 2019 – five years after its adoption – only 14 of the 55 AU member states had

[16] Parshotam A, 'Can the African Continental Free Trade Area Offer a New Beginning for Trade in Africa?', Occasional Paper no. 280. Johannesburg: SAIIA (South African Institute for International Affairs), 2018, https://saiia.org.za/research/can-the-african-continental-free-trade-area-offer-a-new-beginning-for-trade-in-africa/.

[17] Murithi T, 'Reflections on Agenda 2063 and the AU as a norm entrepreneur', in by Gruzd S & Y Turianskyi (eds), *African Accountability: What Works and What Doesn't*. Johannesburg: SAIIA, 2015.

[18] World Economic Forum, 'Why we need to improve global cyber governance', 2 May 2015, https://www.weforum.org/agenda/2015/05/why-we-need-to-improve-global-cyber-governance/.

[19] ITU, 'ITU releases 2018 global and regional ICT estimates', https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx.

[20] *Ibid*.

[21] Turianskyi Y, 'Balancing Cyber Security and Internet Freedom In Africa', Occasional Paper no. 275. Johannesburg: SAIIA (South African Institute for International Affairs), 2018, https://saiia.org.za/research/balancing-cyber-security-and-internet-freedom-in-africa/.

signed and a mere seven had ratified it.[22] This signifies that the necessary political will to implement the provisions listed in the convention is currently lacking. It furthermore means that the convention is not yet in force, as it requires ratification by at least 15 member states.

> The only document available at the AU level is the Convention on Cyber Security and Personal Data Protection, which was adopted in 2014 as part of Agenda 2063. As of October 2019 – five years after its adoption – only 14 of the 55 AU member states had signed and a mere seven had ratified it

What are AU members required to do under the convention? The document imposes obligations on signatories to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime.[23] Therefore, instead of establishing a unified legal framework for all member states, it guides them towards establishing their own cybersecurity and data protection laws. Given the principle of sovereignty of member states and the fact that the AU is not a common market, the implementation of conventions and other agreements is different from the European experience. Articles 8[24] (on personal data protection) and 24[25] (on promoting cybersecurity and combating cybercrime) are illustrative of this point:

> **Article 8**: Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of personal data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.
>
> **Article 24**: Each State Party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognises the importance of Critical Information Infrastructure for the nation identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved.

[22] African Union, 'List of countries which have signed, ratified/acceded to the AU Convention on Cyber Security and Personal Data Protection', https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf. This list does not appear to be up to date, as Chad and Rwanda have recently also ratified the convention.

[23] Orji UJ, 'The African Union Convention on Cybersecurity: A regional response towards cyber stability?', in *Masaryk University Journal of Law and Technology*, 12, 2, pp. 92.

[24] African Union, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf, p. 13.

[25] *Ibid*., p. 24.

While some guidelines in respect of the above are provided, and the need for international cooperation is stressed, ultimately it is up to the member states to interpret the convention and implement their own laws at the national level. Although some AU states have passed cybersecurity and data protection laws, there are instances where such laws are vaguely worded and often used to stifle political dissent rather than to protect citizens.[26] Indeed, it is important for any domestic legislation to respect the rule of law and human rights. 'Over-criminalisation – in particular with regard to content and speech – should be avoided, and conditions and safeguards limiting law enforcement powers should be established.'[27] In fact, common law on freedom of speech and defamation should apply in most of these cases. It is also worth mentioning that since the convention is not ratified (or even signed by the majority of AU members), these laws do not fall under it.

How does this compare to the EU? Twenty-eight member states had a two-year grace period to transpose both the Directive on Cybersecurity and the GDPR into national legislation and had a margin of discretion in terms of national adaptations. A recent study on the implementation of the GDPR in ten countries found that 'most of the national adaptations are still incomplete and raise(d) concerns regarding their conformity with the GDPR'.[28] The key differentiator is that all EU states are working towards domesticating these rules two years after the GDPR was adopted, while the AU convention has not been ratified even though five years have passed.

Other AU initiatives and the international dimension

Although the convention remains the only formally adopted AU document on cyber governance, the continental body clearly recognises its importance, as evidenced by other recent efforts on this theme throughout 2018. In April, the AU Commission (AUC) joined forces with the Council of Europe to organise a workshop on cyber security and cybercrime policies.[29] Following on from this, the AUC also worked with the Internet Society[30] to jointly develop Privacy and Personal Data Protection Guidelines. In July, a workshop took place on the Cybersecurity Strategies, Cybersecurity Legislation and Computer Emergency Incident/Response Team (CERT/CIRT).[31] The AUC then organised the first African Forum on Cybercrime, which was held in Addis Ababa in October.

[26] Turianskyi Y, *op. cit.*, p. 5.

[27] Symantec, 'Cyber Crime and Cyber Security Trends in Africa', 2016, https://www.symantec.com/content/dam/symantec/docs/reports/cyber-security-trends-report-africa-interactive-en.pdf, accessed 1 November 2019.

[28] Tambou O (ed.), *National Adaptations of the GDPR*, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf.

[29] African Union. 'AU Commission and Council of Europe join forces on cybersecurity'. Press release, 12 April 2018, https://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity.

[30] The Internet Society was founded in 1992 to work on the Internet standards process. For more, see https://www.internetsociety.org/.

[31] African Academic Network on Internet Policy, 'Why it is important for African states to ratify the Malabo Convention', https://aanoip.org/why-it-is-important-for-african-states-to-ratify-the-malabo-convention/.

Particularly noteworthy here is the fact that most of these activities were conducted in tandem with other partners, which signifies willingness to share best practices and promote peer learning. Indeed, governments need to work with other stakeholders, such as technology experts, civil society and businesses, to create 'the rules, checks and balances to maintain justice, competitiveness, fairness, inclusive intellectual property, safety and reliability.'[32] This is also important in a context in which technology is advancing at much faster rates than governments are responding to it through legislation and regulation.

In this regard, the AU should also consider 'A Call for Agile Governance Principles', issued at the World Economic Forum Global Agenda Council on the Future of Software and Society in 2016. According to these principles, '[g]overnments will need a new framework for governance both in the ways evolving technologies and the personal and business opportunities they create affect policy decisions; as well as the means for efficiently executing government functions to the benefit of citizens'.[33] Therefore the document emphasises the importance of encouraging citizen engagement in decision-making processes, as well as ensuring clear roles and responsibilities for government, industry stakeholders and citizens. Of note is the fact that there is a recognition that legislation that governs 'employment, industry, and consumer protections' came into being before the introduction of modern technology. Incorporation of such principles in future AU legislation would enable it to have broader oversight. Instead of just focusing on technology itself, it would provide guidelines on how technology should affect modern societies. Technology companies should also be obligated to secure systems, develop skills and share insights to enable the combating of cybercrime.

It is also important to note that the AU is not the only game in town – there are also international conventions. One of the most prominent ones is the Budapest Convention on Cyber Crime. This could provide guidelines for domestic legislation that establishes an effective criminal justice system, while being cognisant of the rule of law and human rights. Mauritius was the first African state to become a party to this convention in 2014.[34] In total, seven AU member have signed and ratified it (Benin, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria and Senegal).[35] Although South Africa has signed it, it has never ratified it. The Budapest convention is an important document, as it is the first international effort to provide guidelines for countries to develop their national legislation on the one hand, and establish a framework for international cooperation on the other, which is crucial for cybercrime investigation and prosecution, given how often it transcends borders.[36] There is also cooperation between Europe and Africa to make this convention effective. The Council

[32] Schwab K, *The Fourth Industrial Revolution*, 2016, New York: Crown Business.

[33] World Economic Forum, 'A Call for Agile Governance Principles', 2016, http://www3.weforum.org/docs/IP/2016/ICT/Agile_Governance_Summary.pdf, accessed 25 October 2019.

[34] Symantec *op. cit.*

[35] Council of Europe 'Chart of signatures and ratifications of Treaty 185'. Status as of 01/11/2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XvRotrxq, accessed 1 November 2019.

[36] Microsoft, 'The Budapest Convention on Cybercrime: 15th Anniversary', 17 November 2016, https://www.microsoft.com/security/blog/2016/11/17/the-budapest-convention-on-cybercrime-15th-anniversary/, accessed 31 October 2019.

of Europe, often in conjunction with the EU, is supporting African states that have acceded to the convention through initiatives such as the training of criminal justice authorities.[37]

Best practice: Mauritius

Mauritius, singled out earlier, seems to be a good case study on the continent for responsible cyber policies and legislation. It was one of the first African countries to adopt comprehensive legislation on cybercrime as far back as 2003.[38] Since then it has developed a national cybersecurity strategy and has embarked on a five-year (2014–2019) process to implement it. It has also adopted a national cyber policy, intended to coordinate cybersecurity efforts, as well as a number of laws to protect personal data, including the Electronic Act (2000), the Computer Misuse and Cyber Crime Act (2003) and the Data Protection Act (2004). A focal point – the Ministry of Technology, Communication and Innovation – has been designated to drive cybersecurity policy. Importantly, the government also works with civil society to educate and raise public awareness on cyber risks.[39] These measures, including comprehensive data protection laws, a national cyber policy, data privacy regulators and the establishment of a focal point to champion these processes and work with the public, should be considered a best practice in terms of putting in place a holistic cyber strategy at the national level by other AU countries.

Conclusion

The fact that the AU is recognising the importance of 'new governance' concepts, such as the protection of citizens from cybercrime and the protection of their personal data, is to be welcomed. Indeed, the organisation has previously acted as a norm entrepreneur, most recently through the adoption of Agenda 2063. The danger is that its initiatives in the realm of cyberspace will run into old AU institutional problems, including inefficient bureaucracy, lack of implementation, inadequate funding and an inability to find consensus among its 55 member states.[40] There is hope that the AU will become a more efficient organisation following the reform process spearheaded by Rwanda's President Paul Kagame. Its efforts to promote and embed cyber governance on the continent will be the litmus test for the changes currently under way. It is also important that the AU recognise the importance of a multi-stakeholder dimension for cyber initiatives and work with its European counterparts and cyber security experts. Going forward, it should make a concerted effort to involve African civil society organisations, which is an area it has struggled with in the past. Civil society can both act as a bridge between the AU and African citizens and ensure that

[37] Symantec *op. cit.*

[38] *Ibid.*

[39] *Ibid.*

[40] Turianskyi Y & S Gruzd, 'The Kagame Reforms of the AU: Will they Stick?', SAIIA Occasional Paper No 299, July 2019, https://saiia.org.za/research/the-kagame-reforms-of-the-au-will-they-stick/.

concerns about human rights are not glossed over. In conclusion, the AU is off to a good start and should continue its efforts in establishing continental policies and initiatives on cyber security and data privacy. However, it needs to do more to encourage member states to establish legislation at the domestic level, which protects citizens while operating within the confines of the rule of law and respecting human rights.

Recommendations

- The AU should put more effort into encouraging its member states to sign and ratify the Convention on Cyber Security and Personal Data Protection – seven ratifications in five years is an abysmal statistic, especially for legislation that is so relevant in modern digital societies. Specifically, the AU should engage individually with member states to find out why they have not signed and ratified this convention.
- A possible avenue to secure buy-in from states to sign and ratify the convention is the Pan-African Parliament which, although lacking legislative powers, may be an effective forum for discussion at a continental level. This may lead to MPs becoming champions of legislation at the national level. For instance, in the Parliament's 'Eleven by 2011' campaign, it secured enough ratifications to bring the African Charter on Democracy, Elections and Governance (2007) into force.
- The AU should also continue to work with other stakeholders, such as its European partners, civil society and technology experts, as it designs new policies. Sharing of existing knowledge and expert advice is crucial in an area where policymakers often lack the know-how.
- Governments should ensure that African citizens, represented by the continent's civil society organisations, are part of the process and that all legislation adopted at the domestic level includes provisions on the rule of law and human rights.
- Drawing on a lesson from the EU, the AU could consider creating a body similar to the European Network and Information Security Agency (ENISA) at the continental level.
- African states and the AU should consider applying the World Economic Forum's 'A Call for Agile Governance Principles' in future legislation on technology.

Author

Yarik Turianskyi

is the Deputy Programme Head for African Governance and Diplomacy at the South African Institute of International Affairs (SAIIA). His research interest is the intersection of governance and technology.

Acknowledgement

Corien Vermaak is thanked for her peer-review and inputs.

SAIIA gratefully acknowledges the support of the Swedish International Development Cooperation Agency (SIDA).

About SAIIA

SAIIA is an independent, non-government think tank whose key strategic objectives are to make effective input into public policy, and to encourage wider and more informed debate on international affairs, with particular emphasis on African issues and concerns.

SAIIA's policy insights are situation analysis papers intended for policymakers, whether in government or business. They are designed to bridge the space between policy briefings and occasional papers.

Cover image

ipopba

SOUTH AFRICAN INSTITUTE
OF INTERNATIONAL AFFAIRS

*African perspectives.
Global insights.*

Jan Smuts House, East Campus, University of the Witwatersrand
PO Box 31596, Braamfontein 2017, Johannesburg, South Africa
Tel +27 (0)11 339–2021 • Fax +27 (0)11 339–2154
www.saiia.org.za • info@saiia.org.za