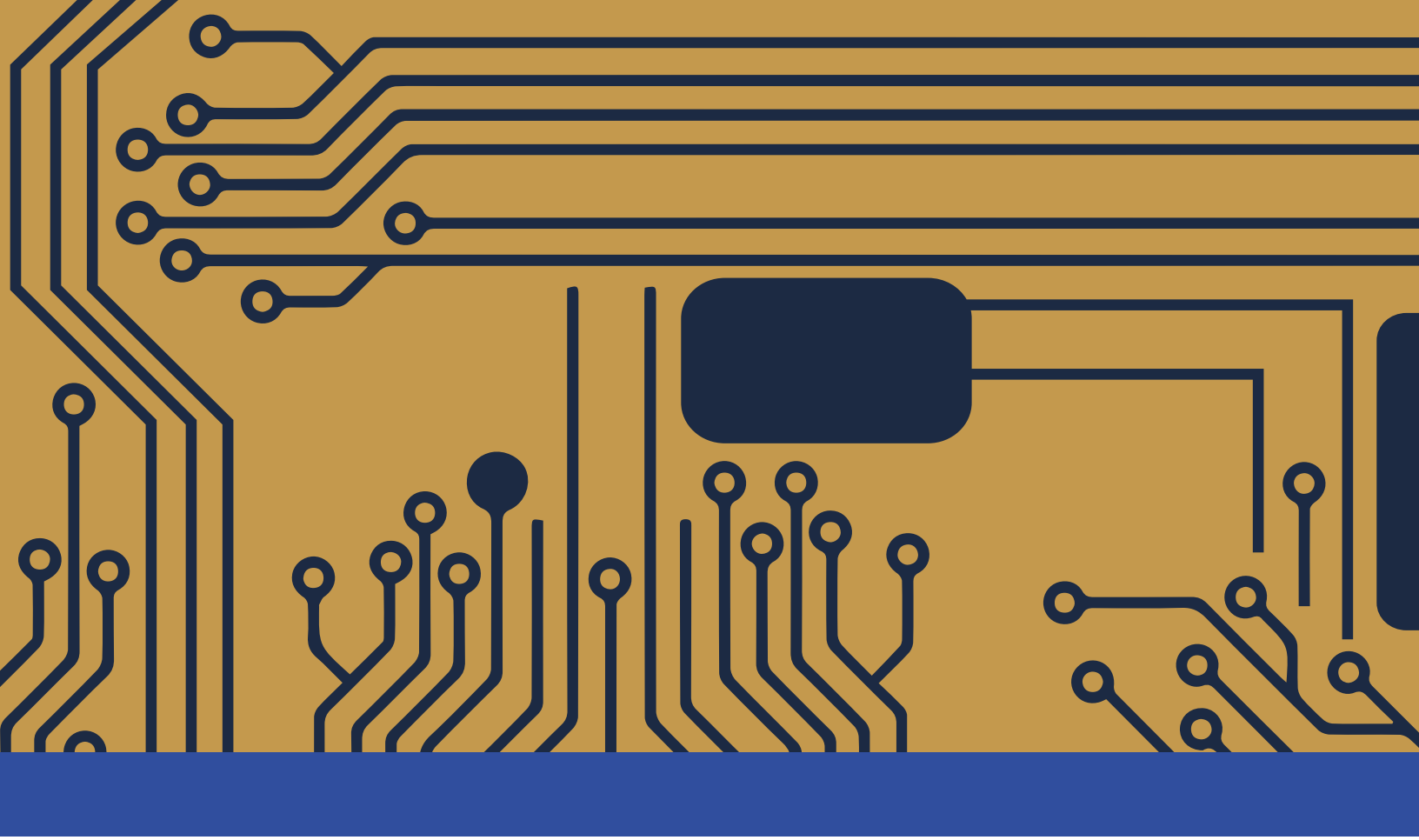

Understanding Cybersecurity and Data Protection in Mauritius, Kenya, and Zimbabwe

By Rachel Achieng' Odhiambo and Emmah Wakoli

Strathmore University
Centre for Intellectual Property and Information Technology Law

Executive summary

Legal policies and frameworks frequently lag behind technological advancements, resulting in unintended loopholes and gaps in legislation enacted to regulate data and emerging technologies. This is evident in cybersecurity and privacy, where technological advancements appear to be accelerating while legal policies and frameworks strive to catch up. In the long-term, this may result in gaps in legislation enacted to govern data and emerging technologies. This study examines the cybersecurity and data protection legislation in Mauritius, Kenya, and Zimbabwe in an effort to comprehend their perspectives on cybersecurity and cybercrime, as well as the reasons for their different approaches. It seeks to identify current issues at the intersection of cybersecurity and data protection in the countries of study, and to assess how they approach cybersecurity and data protection.

This study examines the cybersecurity and data protection legislation in Mauritius, Kenya, and Zimbabwe in an effort to comprehend their perspectives on cybersecurity and cybercrime, as well as the reasons for their different approaches.

Introduction

The evolving digital landscape poses a challenge for national, regional, and global policymakers, especially when technological advancements are progressing faster than legislation that govern these technological advancements. When it comes to information, 'privacy' refers to "making ostensibly private information about an individual unavailable to parties who should not have that information"[1]; this forms the basis of data protection. Security, meanwhile, refers to the methods, tools, and personnel an organization employs to protect its digital assets, and it aims to prevent unauthorized users, also known as threat actors, from disrupting, stealing, or exploiting these assets, devices, and services.[2] Cybersecurity is diverse in nature and is derived from doctrines concerning fair information practices, negligence, contract law, business practices, and consumer protection.[3] It may broadly be defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."[4]

Cybersecurity and data protection are intertwined; privacy cannot exist without security, and security draws attention to privacy, especially when data processing principles are applied. In addition to this, both

[1] *'At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues' at NAP.Edu* <https://www.nap.edu/read/18749/chapter/7> 2014.
[2] Brooks, D. J. (2009). What is security: Definition through knowledge categorization. *Security Journal*, 1–15. https://doi.org/doi: 10.1057/sj.2008.18
[3] *'At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues' at NAP.Edu* <https://www.nap.edu/read/18749/chapter/7> 2014.
[4] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

data protection and cybersecurity frameworks have ethical and legal ramifications across the private and public sector on all levels of society. In recent years, the criminal law response, that is the application of criminal law measures to cybersecurity governance, has concerned stakeholders in the digital and data spheres, as cybersecurity governance encompasses both legal, technical, and organizational measures that go far beyond criminal law.[5] Although the establishment of criminal law measures is believed to be an essential component of cybersecurity governance, the mere existence of such measures may not have the desired effect on the regulation of cybersecurity in Africa's information society.[6] In actuality, the development of additional essential components of cybersecurity governance, such as technical and organizational measures, is required, and data protection is beneficial in this regard. It is clear that understanding the two concepts independently and determining their relationship is crucial for determining their efficacy in application in each region of study.

The African Union Convention on Cybersecurity and Personal Data Protection, also referred to as the Malabo Convention, envisions Africa as a single entity for data and privacy protection and calls for a strong, unified legal system that protects all individuals against data processors and controllers. It addresses cyber security, data privacy, and electronic commerce (or "e-transactions"). By specifying the roles and responsibilities of state parties as liable entities, the unified legal framework seeks to increase the accountability of data controllers by mandating the establishment of a National Data Protection Authority (DPA), which would have an administrative role and be responsible for ensuring the processing of personal data is properly regulated. The ratification, or non-ratification, of the Malabo Convention by the three countries and a similar or different approach to that of the Malabo Convention will be beneficial to understanding cybersecurity and data protection. Additionally, an investigation of the cybersecurity and data protection frameworks in these three countries will illuminate legislative gaps governing data protection and security.

"14 of 55 African countries have signed the Malabo Convention."

14 of 55 African countries have signed the Malabo Convention. These countries include: Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome and Principe,

[5]Orji, U. J. (2021). Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa. In International Law of Criminal Justice 3(1), 60–98. Korean Institute of Criminology. https://doi.org/10.36889/IJCJ.2021.002

[6]Orji, U. J. (2021). Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa. In International Law of Criminal Justice 3(1), 60–98. Korean Institute of Criminology. https://doi.org/10.36889/IJCJ.2021.002

Togo, Tunisia, and Zambia. 13 countries: Angola, Cape Verde, Congo, Ghana, Guinea, Mauritius, Mozambique, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia, have ratified it.[7] In addition to ratifying the Malabo Convention, 9 of the 14 countries have established separate national legal frameworks for cybersecurity and data protection. These include: Angola, Ghana, Guinea, Mauritius, Niger, Rwanda, Senegal, Togo, and Zambia. The other 4 countries namely Cape Verde, Congo, Mozambique, and Namibia have developed and/or enacted either a cybersecurity framework or a data protection framework, but not both. At present (as of August 2022), 61% of African countries have developed data protection frameworks,[8] and 79% have developed cybersecurity frameworks.[9]

This study evaluates the strategies deployed by Kenya, Mauritius, and Zimbabwe in governing cybersecurity. It assesses the legal frameworks deployed in each country for this task and their efficacy. It also looks at the enforcement and regulatory structures in place for cybersecurity. Finally, using findings from the analysis of the cybersecurity laws and regulatory structures of the countries of study, we detail policy recommendations for cybersecurity governance.

> The Global Cybersecurity Index (GCI) is a reliable resource that measures the commitment of countries to cybersecurity on a global scale in order to increase awareness of the issue's significance and various dimensions.

Approach and Methodology

For this study, Mauritius, Kenya, and Zimbabwe were chosen based on rankings from the International Telecommunications Union's Global Cybersecurity Index 2021, in which Mauritius was ranked 17th globally, Kenya was ranked 51st, and Zimbabwe was ranked 98th. The Global Cybersecurity Index (GCI) is a reliable resource that measures the commitment of countries to cybersecurity on a global scale in order to increase awareness of the issue's significance and various dimensions.[10] Each country's level of development or engagement is evaluated based on five pillars that include legal measures, technical measures, organizational measures, capacity development, and cooperation, and then an overall score is determined.[11] The study compares the frameworks governing data protection and cybersecurity in the three countries to identify their

[7]African Union, African Union Convention on Cybersecurity and Personal Data Protection Status List as last updated on 25 March, 2022. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf
[8]United Nations Conference on Trade and Development (UNCTAD), Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[9]UNCTAD, Cybercrime Legislation Worldwide, https://unctad.org/page/cybercrime-legislation-worldwide
[10]International Telecommunications Union, Global Cybersecurity Inedx, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[11]International Telecommunications Union, Global Cybersecurity Inedx, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

similarities and differences with regard to the following issues:

- Understanding and definition of cybersecurity
- The relationship between cybersecurity and data protection as reflected in the applicable laws.
- Management and coordination of regulatory authorities for both cybersecurity and data protection.
- Ratification of the Malabo Convention

The following regulations were examined:

i. In Mauritius:
   Cybersecurity and Cybercrime Act 2021
   Data Protection Act 2017
ii. In Kenya:
   Computer Misuse and Cybercrimes Act 2018
   Data Protection Act 2019
iii. In Zimbabwe:
   The Cybersecurity and Data Protection Act 2021

Key findings

The key findings from the study are detailed below:

- Of the three cybersecurity frameworks, Mauritius Cybersecurity and Cybercrime Act 2021 is the only one that defines cybersecurity. The Act defines "cybersecurity" as a means of protecting information, equipment, device, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.[12] Both the Kenya Computer Misuse and Cybercrimes Act 2018 and the Zimbabwe Cybersecurity and Data Protection Act 2021 do not explicitly define cybersecurity. The legal frameworks lack the required depth and breadth in the definition of the term "cybersecurity" in order to comprehend the concept and accurately classify and categorize it.
- None of the three cybersecurity frameworks explicitly defines "cybercrime." The Mauritius Cybersecurity and Cybercrime Act 2021[13] and the Kenya Computer Misuse and Cybercrimes Act 2018[14] have a section on offences which would ideally be referred to as "cybercrimes." On the other hand, the Zimbabwe Cybersecurity and Data Protection Act 2021, which starts off as a data protection framework, and then goes on to read as a cybersecurity framework, does not have examples or forms of

> Of the three cybersecurity frameworks, Mauritius Cybersecurity and Cybercrime Act 2021 is the only one that defines cybersecurity.

[12]Section 2
[13]Part III
[14]Part III

cybercrime. Cybercrime is mentioned severally when highlighting the functions of the Cyber Security and Monitoring Centre,[15] but other than that, there is little to no mention of it. These frameworks lack a definition of "cybercrime" that would serve as a relevant point of reference when addressing the issue; examples of cybercrime alone are not sufficient.

- Zimbabwe and Mauritius have ratified the Malabo Convention, while Kenya has not, and only Zimbabwe has a data protection and cybersecurity framework that takes a similar approach to the Malabo Convention. Mauritius and Zimbabwe's ratification of the Malabo Convention signifies that they recognize the need to protect critical cyber infrastructure and personal data, as well as to promote the free flow of information, in order to create a credible digital space in Africa. Notably, while Zimbabwe has taken a similar approach to the Malabo Convention in regulating cybersecurity and data protection, Mauritius and Kenya have not. Zimbabwe's Cybersecurity and Data Protection Act of 2021 does not clearly differentiate cybersecurity from data protection, nor does it explain the relationship between the two.
- Of the three countries, only Mauritius provides for collaboration between the cybersecurity and data protection regulatory authorities. The Mauritius Cybersecurity and Cybercrime Act 2021 is the only one of the three cybersecurity frameworks investigated in the study that encourages regulatory authorities to collaborate for both cybersecurity and data protection. The Act stipulates that a Data Protection Office representative shall serve on the National Cybersecurity Committee.[16] Although the legal frameworks in Mauritius, Kenya, and Zimbabwe clearly define the roles and responsibilities of the respective regulatory authorities, they do not provide for collaboration between data protection and cybersecurity authorities. Given how cybersecurity and data protection are intertwined and contribute to the protection of the right to privacy, collaboration between the respective regulatory authorities is necessary.
- While both the Mauritius Cybercrime and Cybersecurity Act 2021 and the Kenya Computer Misuse and Cybercrimes Act 2018 establish a cybersecurity incident response team (CIRT), the Zimbabwe Cybersecurity and Data Protection Act 2021 does not. A cybersecurity incident response team (CIRT) operates in a dynamic, ever-changing environment in which it must

"The Mauritius Cybersecurity and Cybercrime Act 2021 is the only one of the three cybersecurity frameworks investigated in the study that encourages regulatory authorities to collaborate for both cybersecurity and data protection."

[15]Section 37 (2)
[16]Part II, the Cybersecurity and Cybercrime Act 2021; Section 3(2)(a).

successfully manage information and solve problems while adapting to difficult circumstances[17] within cyberspace and to ensure both cybersecurity and national security. A country with a CIRT is better equipped to mitigate cybersecurity risks and incidents, and the existence of the CIRT demonstrates that the country is willing to comprehend the cybersecurity risks it faces and act accordingly.

Analysis of the key findings

» Understanding and definition of cybersecurity and cybercrime

The general approach to cybersecurity in African countries is based on criminal law rather than a multifaceted approach that includes fair information practices, negligence, contract law, business practices, and consumer protection. A study of the three countries and their respective cybersecurity frameworks reveals one thing to be true: definitions of cybersecurity and cybercrime are required to provide context and a deeper understanding of the concepts. While most cybersecurity laws in Africa are titled "Cybercrimes Act" and "Computer Misuse Act", which may not necessarily be a bad thing as they are particular about and deal with cybercrimes and related offenses, this naming system simply implies that a criminal law approach has been taken when dealing with cybersecurity. The Computer Misuse and Cybercrime Act of 2003 was the first cybersecurity law in Mauritius, and true to its name, it focused primarily on the offenses rather than the concept. This is no longer the case, as the current legislation - the Cybersecurity and Cybercrime Act 2021 - is a good example of progressive legislation that attempts to demonstrate an understanding of the concepts by keeping pace with the evolving cybersecurity and cybercrime landscape. While there is no universally accepted definition of cybercrime, it is crucial that cybersecurity laws aim to define it in a way that includes the fact that it is committed using information and communication technology and either targets networks, systems, data, websites, and/or technology to facilitate a crime.

"The Computer Misuse and Cybercrime Act of 2003 was the first cybersecurity law in Mauritius, and true to its name, it focused primarily on the offenses rather than the concept."

» Management and coordination of regulatory authorities for both cybersecurity and data protection

Of the three countries of interest's cybersecurity and data protection frameworks, only Mauritius' Cybersecurity and Cybercrimes Act 2021 mentions collaboration between cybersecurity and data protection

[17]S.J. Zaccaro et al., "A Taxonomic Classification of Cyber Security Incident Response Performance" in Psychosocial Dynamics of Cybersecurity, Routledge, 2015.

regulations. Existence and establishment of functional cybersecurity and data protection regulatory authorities in most African countries is a milestone in the continent's cybersecurity and data protection spaces. It underscores the continent's efforts to promote the development of a secure information society and promote the right to privacy. This could be further cemented by providing collaboration and coordination channels between the two regulatory authorities. This may be due to the fact that most of these laws are just becoming operational and, as a result, are in the process of establishing their regulatory offices

One of the common functions of the cybersecurity regulatory authority, as provided in the cybersecurity laws, is to promote capacity building on the prevention, detection, and mitigation of cyber threats. On the other hand, one function of the data protection regulatory authority, across the different data protection frameworks, is to conduct research on developments in the data processing of personal data and ensure that there is no significant risk or adverse effect on the privacy of individuals as a result of any such developments. This is an area where both regulatory authorities could collaborate and offer both legal and technical expertise on ways to prevent, detect, and mitigate any cyber threats, risks, or adverse effects on individuals' privacy.

One of the common functions of the cybersecurity regulatory authority, as provided in the cybersecurity laws, is to promote capacity building on the prevention, detection, and mitigation of cyber threats.

- **Establishment of Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs)**

While Mauritius and Kenya have established CIRTs and clearly set out the functions in the cybersecurity frameworks, Zimbabwe has not. Incident response is a crucial security function within organizations that aims to manage incidents in a timely and cost-efficient manner.[18] As such, a CIRT or CERT is responsible for documenting, analyzing, organizing, and responding to cyber security incidents and activities i.e. responding to cyber incidents effectively.[19] To achieve this, it is imperative that African countries develop plans and resources to implement cyber security mitigation and practices that can effectively respond to the ever-increasing number of information system attacks.[20] As such, this is a concept that Zimbabwe could learn from Mauritius and Kenya.

[18]Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams - Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

[19]Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. *IEEE Security & Privacy*. https://doi.org/978-1-4244-5494-5/10/

[20]Wara, Y. M., & Singh, D. (2015). A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN). *African Journal of Computing & ICT*, *8*(2), 1–8.

» **Ratification of the Malabo Convention**

While Kenya and Zimbabwe have not ratified the Malabo Convention, Mauritius has. The Convention's primary purpose is to address the need for harmonized legislations in the area of cybersecurity and personal data protection in the African Union Member States and to establish in each country a mechanism capable of combating cybercrime and privacy violations. It also calls for human and institutional capacity building on cybersecurity, cybercrime, personal data protection, as well as the formation of national and regional Computer Emergency Readiness Teams (CERTs). While most African countries have been slow to ratify the Convention, it would be an excellent opportunity to encourage cooperation with regional and international organizations working in the cybersecurity space to establish cooperation mechanisms to address the cyber security issue, combat various forms of cybercrime, and advance the development of the information security ecosystem in Africa. This can be accomplished by establishing national and regional definitions for cybersecurity and cybercrime, establishing CIRTs with comparable functions in each nation, and fostering an environment favorable to the advancement of cybersecurity engagement in terms of understanding and application. Since cybercrime is a global phenomenon, international cooperation is essential to combating it. Therefore, it would be critical for Zimbabwe to evaluate why it has chosen an approach similar to the Malabo Convention despite not having ratified it, and for Kenya to evaluate why it has not yet ratified it, as well as the implications, if any, for regional cooperation.

“The formulation of a concise, all-encompassing, and unifying definition of cybersecurity will allow for an enriched focus on the interdisciplinary nature of cybersecurity.”

Recommendations

The following recommendations are proposed for the improvement of cybersecurity legislation and the comprehension and application of cyber security:

1. **Clearly define cyber terms especially “cybersecurity” and “cybercrime”**

The formulation of a concise, all-encompassing, and unifying definition of cybersecurity will allow for an enriched focus on the interdisciplinary nature of cybersecurity. This will influence how relevant stakeholders such as academia, industry, government, and non-governmental organizations approach cybersecurity challenges and cybercrime in general.

The cybersecurity laws should clearly outline the following in order to better understand cybersecurity:

» Network security: which is the practice of protecting a computer network from intruders, including both targeted attackers and opportunistic malware.

- Application security: concerned with safeguarding software and devices from threats.
- Information security: safeguards the confidentiality and integrity of data during both storage and transmission.[21]
- Operational security: encompasses the processes and decisions for managing and securing data assets. This encompasses the permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared.

The inclusion and differentiation of the various areas of cybersecurity will not only inform an understanding of the concept but will also be relevant when grouping the various cybercrimes, not generally but specifically. This could eventually trickle down to better understanding, implementation, and management of cybersecurity.

Only Mauritius has provided clear definitions of cybersecurity and cybercrime in its definitions sections. Kenya and Zimbabwe could learn from this so that they can address cybercrime and cybersecurity with a clear understanding of the two concepts.

> In instances where cybersecurity strategies are already in place, ensure improved coordination and, consequently, stronger implementation.

2. Encourage collaboration between the cybersecurity and data protection regulatory authorities

The data protection regulatory authority can achieve compliance with a number of administrative and technical data protection controls with the assistance of cybersecurity practices. The two regulatory authorities can collaborate to develop a model for classifying data based on its impact on security, including confidentiality, integrity, availability, and privacy. In addition, these regulatory authorities can collaborate on data mapping exercises, which can help the data protection regulatory authority demonstrate compliance with regulations and provide the cybersecurity regulatory authority with a fuller picture of the data it must protect. Finally, the two authorities can agree on operational data controls, such as encryption, backups, retention, and destruction procedures, that address their respective concerns while clearly distinguishing their roles and responsibilities to avoid an overlap. In instances where cybersecurity strategies are already in place, ensure improved coordination and, consequently, stronger implementation. This collaboration would also be ideal for strengthening partnerships between domestic stakeholders in the cyber and digital rights space in order to promote the sharing of

[21] Collard, G., Ducroquet, S., Disson, E., & Talens, G. (2017). A definition of Information Security Classification in cybersecurity context. *11th International Conference on Research Challenges in Information Science (RCIS)*, 77-82, doi: 10.1109/RCIS.2017.7956520.

intelligence on potential threats and collaboration in the search for long-term solutions. Only Mauritius includes this provision in its cybersecurity frameworks; Kenya and Zimbabwe could learn from this.

3. Establishment of CIRTs

It is of the utmost importance for state and non-state actors engaged in developing cyber capacity in Africa to construct and understand the cyber policy, technical readiness, and capacity of African governments and one such way is through establishing CIRTs. Only 19 of the 131 CIRTs found around the world are in Africa, with 2 of those being in Kenya and Mauritius. This suggests that the cybersecurity measures in the area are still in their infancy as it pertains to technical measures.

4. Ratification of the Malabo Convention

The Malabo Convention is not yet legally binding because the requisite number of Member States have not yet ratified it. Of the countries analyzed in this study, Zimbabwe and Mauritius have ratified whereas Kenya has not. The Convention aims to provide protections for cyber infrastructure, protection of personal information, cyber security, and the foundations necessary to enable an information economy on the African continent. Even though it was ratified in 2014, only 8 countries have ratified it so far. This goes to show that there exists a disconnect between those working in and developing cybersecurity tools and policymakers in cybersecurity and data protection, who may not understand the necessity of providing both protections. Eventually, it is hoped that all African nations will ratify the Malabo Convention to ensure that data protection and cybersecurity are properly regulated. Regional treaties should encourage and strengthen the transnational cooperation of national DPAs so as to enhance the enforcement of regional and national data protection laws. This could even extend to the CIRTs, allowing collaboration on data protection and cybersecurity not only in certain parts of Africa, but throughout the entire region. Ratification of the Malabo Convention will also enhance regional cooperation among African states so that they can negotiate multilateral cybersecurity standards with a unified front.

> “..... it is imperative that cybersecurity and data protection regulatory authorities collaborate to mitigate risks in advance.”

Conclusion

Due to the exponential growth of data breaches resulting from cyberattacks and internal threats,[22] as well as the enactment of legislation to combat cybercrime, it is imperative that cybersecurity and data

[22]Daniel, J. (2022, January 26). *African data breaches: A look at the evolving threat landscape*. CIO; www.cio.com. https://www.cio.com/article/201509/top-african-data-breaches-the-threat-landscape-changes.html

protection regulatory authorities collaborate to mitigate risks in advance. Current market regulations implemented in African countries, as well as new and existing cybersecurity laws, require assessment, reporting, and compliance in near real time. Collaboration could be one way to meet the demand for ensuring the right to privacy in light of recently enacted data protection laws that have significantly altered data protection requirements.

Understanding cybersecurity as a means to focus on the specific technical implementations required to protect systems and networks, as opposed to criminalizing it, will alter the approach to drafting and implementing legislation. This could also facilitate collaboration between cybersecurity and data protection regulatory authorities and assist them in achieving their shared objective of protecting the right to privacy. Both data protection and cybersecurity are concerned with safeguarding sensitive data from various digital threats and risks, making them inseparable. There is room for the African continent as a whole to adopt a regional strategy that encourages peer learning and knowledge sharing.

This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.