KM6: Cybercrime

Introduction

1. The nature of cybercrime

2. The impact of cybercrime

3. Responses to cybercrime

4. The interplay between data protection and privacy

5. Conclusion

Module objectives

Crime always follows opportunity. The internet provides countless opportunities. Traditional crimes such as fraud, identity theft, or trade in illegal goods, are now conducted through the internet. Also, the increase in using personal information for online transactions has created the need to balance security and privacy, especially in law enforcement. This module will explore issues around cybercrime, its definition and its impact, legal and legislative responses by countries around the world, along with African examples. The module will also explore privacy and personal data protection through an overview of the interplay between data protection and security. The module will provide the participants with basic knowledge on how to address issues around cybercrime, privacy, and security.

By the end of this module, participants are expected to know how various countries approached the issues discussed in the text and proffer solutions. Some of the questions that would be addressed include:

- ☐ What is the nature of cybercrime?
- ☐ What activities may amount to cybercrime?
- ☐ How does crime impact Africa?
- ☐ Apart from the economic impact, what other areas in a acountry does cybercrime affect?
- ☐ What are the responses to cybercrime?
- ☐ What are the features of cybercrime legislation?
- ☐ What is the international community doing in response to cybercrime?
- ☐ What is privacy?
- ☐ What are the principles of data protection?
- ☐ How to balance the interest of data protection and security?

- ☐ What are the approaches to data protection?
- ☐ What are African countries doing to protect privacy?

1. The nature of cybercrime

It is difficult to provide a comprehensive definition of cybercrime. Some texts distinguish between cybercrime and computer crimes. This distinction is properly discussed in the ITU publication Understanding cybercrime: Phenomena, challenges and legal response. The United States National Institute on Standards and Technology (NSIT) defines cybercrime as criminal offences committed on the internet or aided by the use of computer technology. For our purpose, we can describe cybercrime as a crime, or an unlawful act committed using information and communication technologies (ICT). Such an act must be prohibited by law and punishment prescribed. Sometimes, the ICT is used as a tool while, in other cases, it is the target of an illegal activity.

The United Kingdom Crown Prosecution Service, in its definition of cybercrime, places cybercrimes into two categories. The first category is cyber-dependent crimes. Those are cybercrimes that can be committed only through the use of the ICT devices, where the devices are both the tool for committing the crime, and the target of the crime. For example, developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity. The second category is cyber-enabled crimes. These are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of the ICT, such as cyber-enabled fraud and data theft.

The uniqueness of cybercrime is that the internet enabled traditional crimes to evolve. Copying someone’s signature to withdraw funds from a bank account has been replaced with stealing credit card numbers with the use of online tools on a massive scale. Server hacking, malware infection, web defacement, and distributed denial of service (DDoS) attacks all fall into the category of new crimes that have emerged with the existence of the internet.

Cyberspace offers an abundance of tools to conduct or facilitate these crimes, new or old, such as botnets (which enable mass distribution of spam), malware infection, DDoS attacks, and many others. Any technological development offers criminals new opportunities to target a multitude of potential victims.

Emerging technologies are also changing society and, thus, the environment in which crimes occur. Developments in 3D printing have made it possible to produce fully operational printed guns, as well as bogus point-of-sale (POS) devices and ATM skimming devices to steal credit card details. Illegal markets in the so-called dark web

are flourishing. Some of them (Silk Road 1 and 2, Evolution, Agora, and Darkode) have already been successfully taken down. Digital currencies (also known as cryptocurrencies) like BitCoin, and related anonymising applications like Dark Wallet, which makes it almost impossible to track the flow of digital money, make it easier for illegal markets to evade law enforcement agencies.
(https://www.youtube.com/watch?v=2NKvkmGHevc)

African context
The African Union (AU) Assembly is considering negotiations for an e-commerce protocol in the AfCFTA. The onset of COVID-19 has added urgency for negotiations which will address operational aspects of e-commerce and utilisation of digital tools, including data protection, portability, security and privacy; cross-border data flows and data localisation provisions; coordinated cybercrime laws; and harmonisation of laws for the taxation of cross-border e-commerce.

Source: The Futures Report: Making the AfCFTA Work for Women and Youth

While everything is getting ‘smart’ and connecting to the internet – from cars to light bulbs, from fridges to smart cities within the Internet of Things (IoT) – smart devices might be pretty dumb when it comes to security. Insecure devices allow criminals to perform various actions: from using them as part of botnets, requesting ransom if the device is important (a car, or a camera, for instance), to penetrating further through the network to which the device is connected.

Cybercriminals are also deploying artificial intelligence (AI), to bypass security measures (such as CAPTCHA), to improve the accuracy of phishing attacks, and to develop highly invasive malware. AI is a threat itself, because autonomous devices, which process a huge amount of data and decide on their own, might be more vulnerable to hacking, theft of personal data, interception, monitoring, and other crimes. Trend Micro Research, in collaboration with United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol’s European Cybercrime Centre (EC3) have provided a report on Malicious Uses and Abuses of Artificial Intelligence. The report presents the state of artificial intelligence and predicts the possible ways that criminals will exploit these technologies in the future.

2. The impact of cybercrime

One of the reasons that make it necessary to address cybercrime is the impact of the activities of cyber criminals. The changing environment discussed in the previous heading has sometimes created dire consequences for internet users. As economies continue to evolve with greater dependence on digital technologies, criminals have also seized this opportunity to cause harm on the economy. For example, the BBC reported that the attack on the Colombian Oil pipeline in the United States of America resulted in the payment of a ransom of US$5 million. The Cybercrime Magazine estimated that cybercrime will cost over US$10 trillion in loss annually by 2025. This estimate may not include unreported incidents.

For African countries there is a peculiar challenge regarding the impact of cybercrime. It appears that African countries may be more vulnerable to cyberattacks and cybercrimes. This is because there may be an increase in the use of digital technologies without the necessary remedial cybersecurity measures. Nir Kshetr, in his article Cybercrime and Cybersecurity in Africa, points to a trend, in which Africa presents the next soft target for cybercrimes. This is because most African countries are emerging markets and are soft targets for criminals. The Interpol Africa Cyberthreats Assessment Report 2021 quotes a research from a Kenyan IT cybersecurity company, Serianu, which highlighted that cybercrime reduced the gross domestic products (GDP) within Africa by over 10%, at a cost of about US$4.12 billion in 2021.

Apart from the economy, there are other areas where the impact of cybercrime may be severe. For example, the UK Department of Health report on the WannaCry cyberattacks showed that the attack caused 'the disruption in at least 34%' of the NHS trusts (organisational units) in England, which resulted in approximately 19,000 appointments that were cancelled. This caused patients in five areas to 'travel further' to access health care in emergency situations. Those were life threatening circumstances with the potential of causing mass casualties.

3. Responses to cybercrime

The emergence of cybercrime requires significant changes in national and international legislation, empowering law enforcement to deal with crimes involving technology. Perhaps the greatest challenge to cybercrime in terms of law making is the nature of law itself. As a general rule, laws can only be enforced within the country where they were originally made. This makes it difficult to enforce cybercrime laws in situations when the criminal is outside the impacted territory. However, criminal jurisdiction can be extraterritorial in nature when a nation asserts it, either generally or in specific cases under its domestic law. A supranational authority, such as the United Nations Security Council, can create an international court to deal with a specific case, such as war crimes in a certain country, or an international court created under a treaty to deal with a stated area of jurisdiction.

Resource
The United Nations Office on Drugs and Crime carried out a comprehensive study and provided a report in 2013. The report recognised that in developing an effective cybercrime legal framework, there are certain components that must be considered to make the framework efficient and effective. These include providing for institutional framework, building capacity for law enforcement, addressing issues of electronic or digital evidence, international cooperation, and preventive measures.
UNODC Comprehensive Study on Cybercrime

INTERPOL Cybercrime Strategy Guidebook
This step-by-step guide is the resource for INTERPOL member countries wishing to create or enhance their national Cybercrime Strategy. The Guidebook also helps countries gain insight into their current response to cybercrime and provides a means to design a more robust strategy and programme.

Over the years, many countries managed to amend their existing legislation to extend the concepts of various traditional crimes to the digital world and to add new crimes. Others enacted entirely new laws dealing with cybercrime only. The United Nations Conference on Trade and Development (UNCTAD) provides a database of cybercrime legislation the world over. The database indicates that 80% of countries have cybercrime legislation, while 5% have draft legislations. In Africa (54 countries), 39 countries (72%) have cybercrime legislation, 2 (4%) have a draft legislation, 12 (22%) have no legislation, while 1 (2%) have no data available.

Cybercrime Legislation in Africa

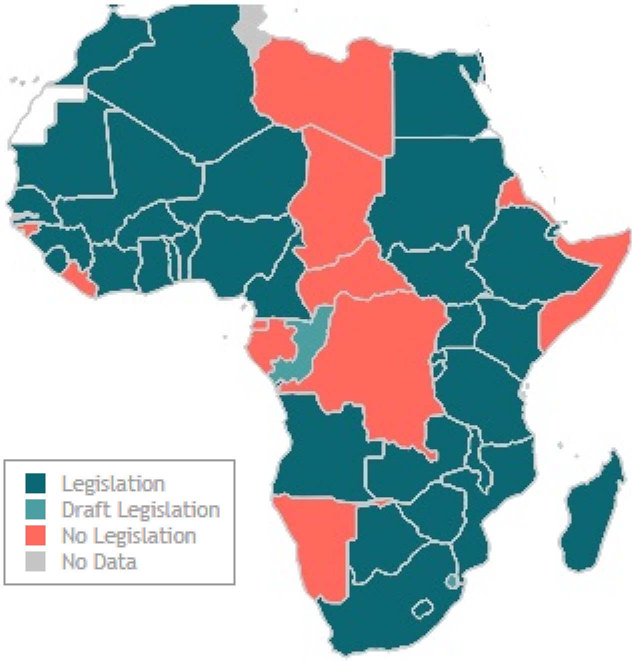

Figure 1 shows countries with cybercrime legislation in Africa.
Source: UNCTAD Database

Cybercrime legislation identifies acts that cause harm and prohibits them. This automatically creates acceptable standards of behaviour in the use of the ICT. Legislation addresses two distinct aspects – substantive aspect, which provides for criminal acts that are punishable and procedural aspect focusing on how to collect digital evidence and prosecute those identified for violating substantive law.

Under the substantive aspect of cybercrime legislations, the objective is to create or modify laws to prevent illegal activities using the internet. In some instances, existing laws may be adequate to deal with illegal activities online. However, in most cases, existing laws cannot address online harmful activities, so new ones need to be created to criminalise illicit activities. While there is no exhaustive list of cybercrimes the ITU provides some resources that can help countries develop appropriate legislation for cybercrime.

In Africa, Mauritius has developed the Mauritian Cybercrime Online Reporting System (MAUCORS). It is a national online system which allows the public to report cybercrimes occurring on social media securely. It will also provide advice to help in recognising and avoiding common types of cybercrime which takes place on social media websites.

The procedural aspect of cybercrime law addresses the gathering of evidence, identification of perpetrators, and prosecution, in order to secure conviction. However, this aspect is more complex since information on the internet crosses borders without showing travel documents. Thus, criminals can easily bypass national frameworks, tackling multiple victims in different countries, since the data needed for the investigation of crime can be stored at multiple providers across various jurisdictions. The need for transborder cooperation on the bilateral, regional, and multilateral levels to get timely access to this data, is critical.

African context

Combating Cybercrime in the Commonwealth

The Commonwealth Secretariat runs a project that builds capacity in cybercrime prevention and legal frameworks. The project started in September 2020 and will end in March 2023.

The aim of the project is to to influence the establishment of effective anti-cybercrime frameworks in the Commonwealth , i.e. laws, policies, institutions, and practices that can be harnessed to combat the growing scourge of cybercrime. The outcome would include:

- Increased awareness;
- Enhanced cybercrime-combating capacity; and
- Strengthened pan-Commonwealth anti-cybercrime cooperation frameworks.

The beneficiary countries of this phase are Botswana, Cameroon, Eswatini, the Gambia, and Ghana.

Details of this project can be found on the Cybil Portal.

Most bilateral agreements on criminal investigation are achieved through traditional Mutual Legal Assistance treaties (MLATs) – agreements between countries to gather and exchange information and address extradition issues (sometimes criticised for being slow and insufficient). Mutual legal assistance requires dual criminality – an act should be criminal in both jurisdictions when one country seeks legal assistance from another. Irrespective of the fact that most countries have national cybercrime laws, issues may arise where certain acts punishable in one country are not punishable in another. For example, Onel de Guzman from the Philippines, created the love bug computer worm in May 2000, which infected over 10 million widows personal computers worldwide, stealing passwords and sending them to all contacts on the computer's address book. At the time, the perpetrator could not be prosecuted because the Philippines did not have a cybercrime law, making his actions unpunishable. Incidents like this have led to various initiatives for the harmonisation of cybercrime laws globally.

Therefore, various regional blocks have developed legal frameworks for cybercrime to enable the investigation across their national borders. This has led to various initiatives to harmonise cybercrime laws across countries. Sometimes, more advanced countries provide assistance to less developed ones in creating cybercrime legal and regulatory framework.

.

The GLACY+ Project

GLACY+ is a Joint project of the European Union and the Council of Europe. GLACY+ is intended to extend the experience of the original GLACY project (2013 – 2016) and supports seventeen priority and hub countries in Africa, Asia-Pacific, and Latin America and the Caribbean region. The countries in Africa are Benin, Burkina Faso, Cape Verde, Ghana, Mauritius, Morocco, Nigeria, and Senegal. These countries may serve as hubs to share their experience in cybercrime issues within their respective regions.

Source: https://www.coe.int/en/web/cybercrime/glacyplus

Some of the International frameworks include the African Union Convention on Cybersecurity and Data Protection 2014, the Commonwealth Model Law on Computer and Computer Related Crime, the Commonwealth of Independent States Agreement (2016), the Shanghai Cooperation Organisation Agreement on Cooperation in the Field of Ensuring the international information security (2009), the EU Directive on Attacks Against Information Systems 2013, among others.

These instruments have, to a large degree, influenced each other, with a prominent role being played by the Council of Europe Convention on Cybercrime in setting international standards. The convention is the most comprehensive and widely accepted document in Europe and beyond, but still faces obstacles to becoming a globally accepted agreement. The goal of the CoE convention on cybercrime is to provide a platform for the harmonisation ol legal frameworks globally. However, there are various challenges facing this objective. Firstly, every country has territorial jurisdiction in criminal law and brings diverse perspectives based on legal traditions and culture. This leads to the second challenge, which is that transposing the substantive provisions of the convention to domestic law may not always work. This is because such transposition may contradict the domestic constitution. What may be considered a form of art in Australia could be child ponography in Mali. Any international legal framework for cybercrime must therefore seek to accommodate and reconcile these differences. While harmonisation does not mean creating identical laws, there must be a deliberate drive to recognise the differences in local laws of various countries. In Africa, these factors also affect the Malabo Convention.

Negotiating a new global or regional convention may take years, if not decades, so it is likely that for now, the CoE and Malabo Conventions will remain the most relevant international and regional agreements on cybercrime for African countries.

Other initiatives include those at UN level (such as the work by the International Telecommunication Union (ITU), the United Nations Commission on Crime Prevention and Criminal Justice (UNCCPCJ), and the United Nations Office on Drugs and Crime (UNODC)), as well as ongoing fora and processes for negotiating norms and other instruments. Other stakeholders, such as the private sector, also contribute towards tackling cybercrime in the form of information sharing, awareness-raising activities, and research appropriate to their unique roles as owners of gateways to internet infrastructure or services.

Resource

The UNODC Cybercrime repository offers resources that provide a guide for drafting cybercrime legislations. It covers issues that must be considered in substantive law, procedural law, and international cooperation, among others.

UNODC Cybercrime Repository

Areas of cooperation are not restricted to legal and institutional frameworks only. The African Joint Operations against Cybercrime (AFJOC) is a project to drive intelligence-led, coordinated actions against cybercrime and their perpetrators in African member countries by creating a harmonised regional coordination framework that will produce joint action plans and conduct law enforcement activities. By doing this, the idea is to address the vulnerabilities of weak networks and security under a context of growing underground market and high levels of social engineering/financially motivated threats against vulnerable people.

Another issue worth mentioning when discussing cybercrime is the concept of cybersecurity. While cybercrime deals with crime using ICT, cybersecurity focuses on measures which individuals, organisations, and countries can take to protect themselves from cybercriminals and incidents. The ITU defines cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. Knowledge Module 1a discusses steps countries should take to develop cybersecurity strategies.

4. The interplay between data protection and privacy

According to the International Network of Privacy Law professionals, the history of data protection and privacy can be traced back to 1890 when two United States lawyers, Samuel D. Warren and Louis Brandeis, wrote the article 'The Right to Privacy'. The article argued that people should have the 'right to be left alone', using the phrase as a definition of privacy. The first legal document to provide for this right is the Universal Declaration of Human Rights of 1948, which adopted as its 12th right, the 'Right to Privacy'. Since then, many countries have included this right as a fundamental right of their citizens. For example, the South African Constitution contains the right to privacy in Article 14, Moroccan Constitution under Article 24, and the Ghanaian Constitution under Article 18.

Privacy is a right that is guaranteed by law and it is a fundamental right accrued to individuals because they are human beings. Data protection, on the other hand, is defined by the Oxford Dictionary as a set of legal controls that keep information stored on computers private, and that limit who can read it or use it. In case of data protection, as it relates to privacy, the focus is on personal information. So data protection and privacy are both created by legal regimes. Globally, 128 out of 194 countries had put in place legislation to secure the protection of data and privacy according to the United Nations Conference on Trade and Development (UNCTAD). In Africa, only 29 out of 54 countries have an established legal regime for data protection. Some have started developing the laws.

The interpretation of privacy has diverse views. These views include the rights such as to be free from observation; to be left alone; to keep one's thoughts, beliefs, identity, and behaviour secret; and to choose and control when, what, why, where, how, and to whom information about oneself is revealed and to what extent the information is revealed. This right is directly connected to the right of freedom of expression and association. There is a need for anonymity, if an individual's rights are to be protected.

Many users choose to access the internet anonymously, for a variety of reasons. One tool which helps users remain anonymous is the Tor concept, an open software developed to protect personal privacy and freedom by anonymising and preventing traffic analysis and surveillance. Similar to various encryption tools, Tor provides security and may even save the lives of activists and journalists working in politically unstable parts of the world.

However, the freedom from identification has created an environment for criminals to operate anonymously. It has also emboldened certain individuals to communicate cruel, discriminatory, racist, hateful, and/or other forms of harmful speech to others, which they would not otherwise have done if their identities were known. This creates a challenge for security agencies and law enforcement.

In recent years, the Snowden revelations that disclosed the use of surveillance programs by the United States National Security Agency (NSA), subsequent revelations of surveillance carried out in various other countries, and a rise in cybercrime and terrorism, have placed human rights in the context of security into sharper focus.

From a human rights standpoint, the right to privacy and other human rights should be protected. Encryption tools – including pervasive encryption – are essential to protect privacy. From a security standpoint, however, governments have reiterated the need to access encrypted data with the aim of preventing crime and ensuring public safety. This has put increasing pressure on internet and tech companies to allow governments access to data.

The interplay between encryption, privacy, and tackling cybercrime – and how to balance all of those issues – were highly debated when, in August 2021, Apple announced new measures for scanning iCloud Photos (i.e. user photos) for child sexual abuse material (CSAM). The measures were put on hold, due to at least two issues: the first being that Apple's ability to scan iCloud Photos was a privacy breach in itself; the second being that Apple could be strong-armed by governments to use the tool for their own undemocratic purposes. In light of those concerns, stakeholders are still debating what the way forward is.

In an information or data driven economy, the value of personal data cannot be overemphasised. Data is used to develop business models, provide an efficient platform for marketing of goods and services, understand the preferences of consumers, and develop products and services. However, because data, like technology, is neutral, it can also be used for harmful purposes. There have been high profile cases of data breaches from Facebook, eBay, Equifax, and Uber. Hundreds of millions of individuals' personal information (social security numbers, addresses, credit scores, etc.) were compromised. In order to address the issue of privacy and security, balancing the fundamental rights of citizens against the threat of cybercrimes, various countries have developed laws and regulations to create rights of citizens over their personal data and regulate the access and use of such data, especially by law enforcement.

Perhaps the most popular of these laws is the European Union General Data Protection Regulation (GDPR). The law creates rules for organisations and companies on how to use personal data in an integrity friendly manner. The law sets out principles for the processing of personal data, such as processing in a lawful, fair and transparent manner, limitation of purpose, data and storage, provides for the data subject's rights, and ensures privacy by design. The GDPR, in recognition of the lack of boundaries on the internet, makes the jurisdiction of the law to cover organisations established in the European Union and organisations located outside the European Union that offer goods or services to EU residents or monitor their behaviour. This widens the scope of the law.

Another interesting area worth mentioning is the EU Data Protection Law Enforcement Directive. Generally, the practice in most data protection legal regimes, was to exclude law enforcement activities, especially criminal investigations and issues that affect national security, from the application of the law. However, most countries have recognised that even when citizens are under investigation, they are still entitled to certain rights including how their data is processed. Based on this, countries are beginning to create special rules for law enforcement to maintain a level of privacy rights for citizens, even when they are under criminal investigation.

Best Practices
The Privacy and Data Protection Principles of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 2013 provides a template for the principles of Data Protection which has been adopted by data protection laws in various jurisdictions. The principles are:

Collection Limitation Principle: The collection of personal data should be limited based on the law and, where appropriate, the consent of the data subject.

Data Quality Principle: Personal data should be accurate and relevant to the purpose for which it is intended to be used.

Purpose Specification Principle: The purpose for collection should be specific and should only be used for that purpose.

Use Limitation Principle: Personal data, when collected for a purpose, should only be used for that purpose except with the consent of the data subject, or by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data.

Individual Participation Principle: The data subject has rights which may include to the right to obtain them from a data controller, or confirm if the data controller has data relating to him; to have communicated to him the data relating to him within a reasonable time and at a reasonable charge, if any, in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request for information on his data is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle
A data controller should be accountable for complying with measures which give effect to the principles stated above.

The African Union Convention on Cybersecurity and Personal Data Protection, states that parties shall under Article 8.1 *commit to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, the protection of physical data,* *and punishing any violation of privacy without prejudice to the principle of free flow of personal data*. Article 11.1 of the convention requires State Parties to *establish an authority in charge of protecting personal data*.

The Information Regulator (South Africa) is established pursuant to the Protection of Personal Information Act, 2013 (POPIA Act). Members of the Information Regulator (South Africa) began a new term effective 1 December 2021 following an appointment by the President. The new members were appointed after the Regulator took over the functions in terms of the Promotion of Access to Information Act (PAIA) 2000, and the coming into effect of enforcement powers in terms of the Protection of Personal Information Act (POPIA) 2013.

The Data Protection Law establishes the *Agência de Proteção de Dados* (APD) as Angola's data protection authority. APD's Organic Statute was established by the Presidential Decree 214/2016.

The Office of the Data Protection Commissioner (ODPC) Kenya was established in 2020 following the enactment of the Data Protection Act, 2019. The Act is expected to be supported by Data Protection (General) Regulations, 2021 that set out the procedures to enforce the rights of data subjects, while elaborating on the duties and obligations of Data Controllers and Data Processors. Data Protection (Compliance and Enforcement) Regulations, 2021, that outline the compliance and enforcement provisions for Data Commissioner, Data Controllers, and Data Processors and Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, define the procedure that will be adopted by the Office of the Data Protection Commissioner in registering Data Controllers and Data Processors.

Network of African Data Protection Authorities is an organisation of data protection regulators in Africa. It was established in Ouagadougou, Burkina Faso, in September 2016, at a side event to the African forum on personal data protection. It currently comprises several African privacy and data protection authorities from different geographical and linguistic areas, with the aim of setting up a platform for exchanges and co-operation between its members and making Africa's voice heard in its dealings with partners around the world. The members are: Angola, Benin, Burkina Faso, Chad, Cape Verde, Gabon, Ghana, Kenya, Mali, Mauritius, Morocco, Niger, Nigeria, Sao Tome & Principe, Senegal, South Africa, Tunisia, and Uganda. Please note that the International Standards Organisation (ISO) has a standard for data privacy. This is the ISO 27701 standard.

Finally, in recent times, an issue has emerged regarding the control and movement of data generally. This invariably affects personal data and privacy. The emergence of cloud computing has created a platform for ubiquitous storage of data. Thus data processing can take place virtually without recognition of geographical or national boundaries. The need for governments to keep pace with data collection, movement and control has led to policies that affect the flow of information on the internet.

Concepts like data sovereignty, data residency, and data localisation, attempt to regulate the physical location of data. Data sovereignty refers to the principle that data, irrespective of where they are stored, must comply with the laws of a particular sovereign country. Data residency simply refers to a situation where the law specifies the physical location of the data. Data localisation refers to a mandatory administrative or legal requirement that data must be stored or processed, exclusively or non-exclusively within a specified jurisdiction.

The argument in favour of data localisation is based on a few issues, namely, the interest of national security; protection of personal data and enforcement of data protection laws; securing faster and better access to data for law enforcement; advancing local economic competitiveness; increasing economic growth and boosting employment; and preventing foreign surveillance.

Internationally, various countries have created data localisation regimes. Russia has data localisation requirements for all personal data. Kazakhstan requires all data for servers on the country's specific (.kz) domain. Australia requires health records to be stored locally. Canada requires public service providers to follow data localisation requirements. China has data localisation requirements that affect all personal, business, and financial data. India's data localisation requirements apply to payment service providers and government procurement. The USA requires the data related to the country's citizens to be processed and/or retained in that country. The data covered by these laws can range from all personal data to only specific types of data such as health or financial information.

However, the Indian National Institute of Public Finance and Policy, argues that the assumption that data localisation will necessarily lead to better privacy protections is a fallacy. This is because the security of data is determined more by the technical measures, skills, cybersecurity protocols, put in place rather than its mere location. Overall, the degree of protection afforded to data will depend on the effectiveness of the applicable data protection regime and not the location of data.

5. Main takeaways

The use of the ICT has increased tremendously as it provides opportunities for businesses and countries to work efficiently and promote economic growth. However, since technology is neutral, it also provides opportunities for criminals to perpetrate their illegal activities. This menace, usually referred to as cybercrime, needs to be addressed through legal and institutional frameworks.

This module highlighted the definitions of cybercrime, related initiatives and concepts, and the challenges faced in curbing illegal activities online. The module discussed the economic impact of cybercrime, African and international approaches to addressing cybercrime issues, and resources available for countries that intend to develop legal frameworks for cybercrime. The text also mentioned various regional and international frameworks, as well as the challenges in implementing such frameworks.

The module also discussed privacy, data protection, and national security within the context of human rights. Issues such as basic contents of legal frameworks for data protection, guidance of drafting such frameworks and application of the basic principles of privacy based on fundamental human rights.

Issues identified in this module are to serve as guides for further action or activities on legal regimes to address cybercrime, privacy, and data protection.