**LAWS AND REGULATIONS**

***RWANDA:-***

***LAW-***

**CYBERCRIME LAW:**

* The law governing data protection in Rwanda is the Law n°058/2021 of 13/10/2021 relating to the protection of personal data and privacy (the “Data Protection Law”).
* The Law n° 24/2016 of 18/06/2016 governing Information and Communication Technologies in Rwanda (the “ICT Law”).
* The Law nº 60/2018 of 22/8/2018 on prevention and punishment of cyber-crimes (the “Cyber Crime Law”).

The Cyber Crime Law establishes spamming as a criminal offence (article 37). The Cyber Crime Law defines spamming as any intentional and without authorisation from a competent organ sending of unsolicited messages repeatedly or to a large number of persons by use of a computer or a computer system.

On 15th October 2021, a data protection law was officially gazetted in Rwanda, the Law on the Protection of Personal Data and Privacy (Data Privacy Law). This law establishes obligations for businesses to maintain records of users’ personal data, designate an individual data protection officer carrying out DPIAs, and set up breach notification.

The Data Privacy Law also outlines several data subject rights for organizations already in operation. However, there’s a transition period before enforcement; companies and individuals in Rwanda that personal process data of individuals living in the country have up to October 2023 to plan and comply. Rwanda’s Data Privacy Law is an important step that begins the foundational blocks for a more robust data privacy framework. Rwanda’s Data Privacy Law requires local and international organizations to process personal data securely. This is extremely important given that the country is experiencing a massive wave of progressive development that gives birth to modern services such as e-commerce and trade. Rwanda’s Data Privacy Law comes into enactment after a comprehensive consultation process. During the consultation process, multiple additions and revisions were received from private companies in Rwanda. The most feedback and corrections received were from the financial sector, which deals with Rwandese citizens' sensitive personal data.

According to Article 23 of the Constitution of Rwanda ('the Constitution'), the citizens of Rwanda are guaranteed the right to privacy as their fundamental right. It states as follows:

*'The private life, family, home or correspondence of a person shall not be subjected to arbitrary interference; his or her honour and good reputation shall be respected. A person’s home is inviolable. No search of or entry into a home may be carried out without the owner’s consent,* *except in the circumstances and accordance with procedures determined by law. Confidentiality of correspondence and communication shall not be subject to waiver except in the circumstances and accordance with procedures determined by law.'*

The statement mentioned above underpins the basis of the data protection law.

While the draft did take into account Rwanda’s culture, international best practices such as the GDPR were given significant consideration. In addition, the draft was heavily influenced by the African Union Convention on Cyber Security and Personal Data (Malabo Convention) that stresses the importance of respecting and protecting the rights of individuals both online and offline.

***Key Provisions:-***

*Application and Territorial Impact -*

As per Article 2, Rwanda’s Data Privacy Law applies to data controllers, processors, or third parties that are established or ordinarily residing in Rwanda (not just citizens) and processing personal data while in Rwanda. It also applies to those that are not established or resided in Rwanda but process personal data of data subjects located in Rwanda. This indicates that the application of the law isn’t just restricted to entities within the country but also to firms operating globally and dealing with Rwandan residents. A data controller can be a natural person, public or private corporate body, or legal entity that processes personal data and determines the means of their processing.

*Regulatory Body -*

To ensure smooth implementation, the National Cyber Security Authority (NCSA), the supervisory authority as per the law, will soon publish a compliance guide to help data processors and data controllers start the process. Here’s how they plan to implement the law:

**Create awareness:** NCSA and other stakeholders will conduct sessions to educate the general public and the specific concerned sectors on the requirements for compliance.

**Registration of data processors or data controllers:** Organizations that process personal data or intend to be data controllers or data processors are required to register with the NCSA. This would allow the regulatory body to identify companies that handle personal data and hold them responsible in case of a data breach or violation of the law.

*Data Protection Principles -*

The law requires data controllers and processors to ensure the fulfilment of the following data protection principles:

* Personal data to be processed lawfully, fairly, and transparently.
* Personal data to be collected only for explicit, specified, and legitimate purposes.
* Personal data to be kept accurate and up-to-date.
* Personal data to be retained no longer than is necessary for the purposes it is processed.
* Personal data to be processed in compliance with the rights of data subjects.

*Lawful Grounds of Processing -*

Data controllers must have a lawful basis for the processing of personal data. Where consent is used as a lawful basis of data processing, it is valid only when it is based on the data subject’s free decision after being informed of the consequences of his or her consent. Grounds for data processing are as follows:

* Data subject’s consent.
* Performance of a contract.
* Compliance with a legal obligation.
* Data subject’s vital interests.
* Public interest.
* Performance of public duties of a public entity.
* Legitimate interests of the data controller.
* Research purposes upon authorization by relevant institution.

*Key Responsibilities of Data Controllers and Data Processors -*

Data controllers and processors have the following key responsibilities:

* Implement data security measures.
* Maintain a record of personal data processing operations.
* Carry out data protection impact assessments where the processing is likely to result in a high risk to data subjects.

*Data subjects’ rights -*

Rwanda’s Data Privacy Law provides control to data subjects over their personal data by providing them the following rights:

* Right to information.
* Right to access.
* Right to object.
* Right to personal data portability.
* Right to not be subject to automated decision-making.
* Right to restriction of processing.
* Right to erasure.
* Right to rectification.
* Right to designate an heir to personal data.
* Right to representation.

*Breach notification -*

Rwanda’s Data Privacy Law requires data controllers to notify personal data breaches to the regulatory authority within 48 hours after becoming aware of the breach. Data processors are also required to notify data controllers, where a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, data controllers must communicate the breach to the data subject after becoming aware of it.

*Cross Border Data Transfers -*

Personal data storage outside Rwanda is permitted only if the data controller or the data processor holds a valid registration certificate authorizing him or her to store personal data outside Rwanda. The supervisory authority issues such a certificate.

In addition, the law provides that cross-border data transfers are permitted under one of the following circumstances:

* Authorization from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data,
* Where the data subject has provided his/her consent,
* Where a transfer is necessary for the performance of a contract, public interests grounds, the exercise of a legal claim, protection of vital interests of the data subject or of another person, legitimate interests of the controller, or for the performance of international instruments ratified by Rwanda.

Failure to comply with the law may result in administrative fines on data controllers, data processors, and third parties.

*Security -*

The DC and DP are required to ensure security of the personal data in their possession by adopting appropriate, reasonable technical measures to prevent loss, damage or destruction of personal data which include the following (article 47):- identify foreseeable risks to personal data under that person’s possession or control, establish and maintain appropriate safeguards against those risks; regularly verify whether the personal data safeguards are effectively implemented; ensure that the personal data security safeguards are continually updated in response to new risks or any identified deficiencies.

The NCSA is entitled by the Data Protection Law to conduct inspection and assessment of these security measures.

The Data Protection Law also provides for safeguards that DC or DP processing sensitive personal data must adopt including storing sensitive personal data separately from other types of data or applying measures such as tokenisation, pseudonymisation or encryption (article 11).

**CYBERSECURITY:**

Rwanda had established the following key laws and regulations related to cybersecurity:

* **Law Nº 36/2018 of 13/08/2018:** This law deals with the prevention, investigation, and punishment of cybercrimes in Rwanda. It criminalizes various cyber activities, such as unauthorized access to computer systems, data interference, computer-related fraud, and distribution of malicious software.
* **National Cyber Security Policy and Strategy:** Rwanda has also developed a National Cyber Security Policy and Strategy, which outlines the country's approach to cybersecurity and sets the strategic direction for enhancing cybersecurity measures.
* **Rwanda Information Society Authority (RISA):** This is the body responsible for implementing and enforcing cybersecurity laws and regulations in Rwanda. RISA oversees the country's efforts to strengthen its cybersecurity infrastructure and responds to cyber incidents.
* **Personal Data Protection Law:** While not solely focused on cybersecurity, Rwanda also has a Personal Data Protection Law that safeguards the privacy and security of individuals' personal data, including data stored electronically.
* **E-Transactions and Cybersecurity Law:** This law is aimed at facilitating electronic transactions and providing a legal framework for ensuring cybersecurity in the digital environment.
* **Rwanda Cyber Security Incident Response Team (Rwanda CSIRT):** This is a specialized unit responsible for monitoring and responding to cybersecurity incidents in Rwanda. It plays a crucial role in mitigating cyber threats and ensuring the country's cyber resilience.

***SOUTH AFRICA:-***

***The Timeline -***

The [Cybercrimes Act](https://cybercrimesact.co.za/) was first published as the Cybercrimes and Cybersecurity Bill on 28 August 2015, updated on 19 January 2017 and was introduced in Parliament on 22 February 2017. The Bill sat with Parliament for a while as there was a strong push by the old regime in government to enact the Bill in its then-current form. There were extensive comments on the Bill during the public participation period in 2017, and particularly on onerous aspects of the Bill. Those comments were considered and incorporated into the new Cybercrimes Bill that was published in October 2018. The Bill was revived by the National Council of Provinces (NCOP) who opened another period of public participation from various stakeholders since October 2019. Yet again, NCOP received extensive comments and proposed changes. In June 2020, NCOP adopted the Cybercrimes Bill with their proposed changes. The Bill was sent back to the National Assembly for concurrence in July 2020. The Bill was passed by both houses of Parliament in December 2020 and was sent to the President to assent.

On 26 May 2021, the President signed the Bill into law. The President of South Africa has proclaimed the [commencement date](https://www.michalsons.com/blog/alert-the-cybercrimes-act-has-finally-commenced/54124) of certain sections of the Cybercrimes Act to be 1 December 2021. The President may fix different dates for different provisions of the Act.

**CYBERCRIME LAW:**

The ECT act creates the following offences in Chapter XIII:

* The unauthorised access or interception of data is a crime. In our view hacking, cracking and packet sniffing would fall within this category.
* The unauthorised interference with data in a way that causes such data to be modified, destroyed or otherwise rendered ineffective is a crime.  The creation and spreading of viruses, Trojan horses and worms would fall within this category. However, it is important to realise that, in order to be guilty of an offence in terms of the ECT Act, you must have the intent to commit the crime.  So there is no need for anyone to worry (from a criminal perspective anyway) if a virus that you’ve received sends itself to your whole address book.  While you should have had the most recent pattern or update for your anti-virus software, you’re not a criminal because the virus was not intentionally spread.
* The unlawful use of devices that are designed to overcome security measures for the protection of data is now a crime and this would include the creation or use of software used for cracking.
* The intentional overloading of web servers with the intention of crashing them (denial of service attack) is a crime.  The Distributed Denial of Service (DDoS) attack that [has previously happened](https://en.wikipedia.org/wiki/July_2009_cyber_attacks) is a great example.
* The crimes of computer-related extortion, fraud and forgery are also recognised.  For example, if someone threatens to hack your website or system unless you pay them a lot of money, then this would amount to extortion. (section 87)
* Any person who attempts to commit any one of these crimes (or who aids or abets someone to commit these crimes) is also guilty of an offence.  (section 88).

***Investigation and Enforcement -***

At a time when questions are being asked as to the enforceability of many laws being passed by parliament, the question obviously arises as to whether these new cyber crimes will be enforceable?

Quite a radical approach adopted by the ECT Act is the provision which vests jurisdiction in the South African courts to try an offender if, amongst others, the offence:

* or any part thereof or any preparation in contemplation of such offence was committed in South Africa;
* was committed by a South African citizen, permanent resident or person who was carrying on business in South Africa.

These are extremely wide and the question, which begs to be asked, is how long the arm of the South African law can and will be when we are struggling to combat basic everyday crime within our own borders?

In the United States, Computer Hacking and Intellectual Property ([CHIP](https://www.usdoj.gov/criminal/cybercrime/chipfact.htm)) units have been created specifically for this purpose. One cannot help imagining a virtual equivalent of the police officers from the popular TV series CHIPs in the late 80’s.

In South Africa, one of the proposed enforcement mechanisms is that of cyber inspectors who will, amongst other functions, be monitoring and reporting illegal activities. To date, no cyber inspectors have been appointed. The cyber inspectors have the powers (with a warrant) to inspect and search your premises, information systems or data and seize your records. But because there aren’t any cyber inspectors don’t expect one to arrive at reception armed with a badge and a warrant!

Another means by which the provisions will be enforced is by the reporting of such illegal activity by victims or witnesses. A number of factors threaten to frustrate the enforcement of the provisions by this means, namely:

* many victims of cyber crime do not want it to be publicly known that their systems have been breached and are therefore unwilling to report the crime.  Can you imagine the negative public perception issues which would arise if a bank or a medical aid admitted to its website or databases being hacked (and it is often parties such as banks and security agencies like the NIA or FBI that present themselves as desirable targets for hackers seeking a challenge);
* very often it is extremely difficult to track and identify the hacker and even if this is achieved, they may be in a foreign jurisdiction.  Thus it may not be practically feasible to bring such a person to book.

***The Penalties -***

Do the cyber crime provisions of the ECT Act have any teeth?  Will the cyber crimes act as a deterrent and force people to comply with the law?  Depending on the nature of the offence, the penalties for committing a cyber crime range from an unspecified fine to imprisonment for a period between one to five years.  In the United States the penalty, in terms of their legislation, is US$250,000 or 5 years imprisonment but in our view, we are unlikely to see sentences of this magnitude being imposed on cyber criminals. We are not aware of any fine or imprisonment in South Africa pursuant to these cyber crimes.

**CYBERSECURITY:**

***Cyber Security Regulatory Compliances in South Africa -***

The journey towards enacting cyber security compliance started long back. South Africa rightly envisaged the importance of the Internet and its pros and cons.  In 2012, the South African Cabinet adopted the National Cyber Security Policy Framework (NCPF) to draw a centralized approach to ensuring the country's cyber security.  The NCPF addresses disputes among:

* different agencies,
* legal frameworks,
* inadequate public awareness, and
* a lack of capacity, skills, and resources.

The NCPF sets out security guidelines in South Africa for the government to develop comprehensive cyber-security policies and strategies.

***POPI -***

In South Africa, data security comes under the Protection of Personal Information Act (POPIA).

On July 1, 2021, the material implementation of the most critical provisions of POPIA was enforced. This legislation promotes the protection of personal data processed by public and private bodies.

It outlines the:

* rights of data subjects,
* regulates the cross-border flow of personal data, and
* introduces mandatory data breach reporting and notification obligations.

It also has the power to levy penalties for breaking the law. The safeguarding condition in the POPIA act dictates that a person must guarantee the confidentiality of personal data. It requires this to prevent loss, damage, or unauthorized access or destruction of personal data.

POPIA puts South Africa up to the standards with international data protection laws. This is achieved by regulating the processing of personal data of individuals and entities. If there is reason to believe that personal data has been breached in relation to POPIA, the responsible party must notify the data controller.

In case of a data breach the business may also be subject to a:

* fine,
* administrative penalty, or  sanction,
* civil action, and a class-action lawsuit.

***NIGERIA:-***

***Categories of Cybercrime in Nigeria –***

* Cybercrimes against People
* Cybercrime against property
* Cybercrime against the Government

**CYBERCRIME LAW:**

[***Cybercrimes (Prohibition and Prevention) Act, 2015***](https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf) *–*

The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

***Cybercrimes highlighted under this ACT include -***

* Offences against critical national information infrastructure
* Hacking Computer Systems and Data Alteration
* Unauthorized Access of Protected Systems
* Illegal Registration of Cybercafé or Usage of Unregistered Cybercafé
* System Interference
* Interception of electronic messages, email, electronic money transfers
* Tampering with critical infrastructure
* Willful misdirection of electronic messages
* Unlawful interceptions
* Computer related forgery
* Computer related fraud
* Theft of Electronic Devices
* Unauthorised modification of computer systems, network data and system interference
* Publishing False Digital Signature and Certificates
* Cyber terrorism
* Exceptions to financial institutions posting and authorised options
* Fraudulent issuance of e­-instructions
* Tampering with Computer Source Documents
* Identity theft and impersonation
* Child pornography and related offences
* Cyberstalking
* Cybersquatting
* Racist and xenophobic offences
* Attempt, conspiracy, aiding and abetting
* Importation and fabrication of e-­tools
* Breach of Confidentiality and Privacy
* Manipulation of ATM/POS Terminals
* Phishing, spamming, spreading of computer virus
* Electronic cards related fraud
* Use of fraudulent device or attached e­-mails and websites

*Administration and Enforcement Cyber Law in Nigeria -*

Under the 2015 Cybercrime Act, the National Security Adviser's office serves as the coordinating body for the security and enforcement authorities. The Attorney-General of the Federation reinforces and improves Nigeria's existing legal frameworks regarding cybercrime.

All law enforcement, security, and intelligence agencies develop the institutional capacity necessary for the effective implementation of the provisions of the 2015 Cybercrime Act, and in collaboration with the Office of the National Security Adviser, initiate, develop, or organize training programs for officers charged with cybercrime on a national or international level.

**CYBERSECURITY:**

* **National Cybersecurity Policy and Strategy:** Nigeria has developed a National Cybersecurity Policy and Strategy, which outlines the country's approach to cybersecurity and sets strategic objectives for enhancing cybersecurity measures.
* **Central Bank of Nigeria (CBN) Cybersecurity Framework:** The CBN has issued a comprehensive cybersecurity framework for financial institutions, aiming to enhance the security and resilience of the financial sector against cyber threats.
* **Nigeria Computer Emergency Response Team (ngCERT):** ngCERT is the national cybersecurity incident response team in Nigeria. It is responsible for coordinating responses to cybersecurity incidents and supporting organizations in mitigating cyber threats.

It's important to note that cybersecurity is a rapidly evolving field, and laws and regulations may change or be updated over time. Therefore, for the most current and accurate information on cybersecurity laws and regulations in Nigeria, it is recommended to consult official Nigerian government sources or legal experts specializing in cybersecurity in the country.

***KENYA:-***

**CYBERCRIME LAW:**

The enactment of Kenya’s first comprehensive cybercrime legislation, the Computer Misuse and Cybercrimes Act 2018 (‘Cybercrimes Act’), was a significant milestone in laying down legal regulations for cyber-activities. Two international treaty instruments – namely, the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection – were influential in drafting the Cybercrimes Act. Yet some of the provisions of the Cybercrimes Act that establish key definitions and criminal offences are inconsistent with these international treaty standards and in breach of Kenya’s Constitution. The DPA regulates the processing of personal data in Kenya and provides measures to protect the privacy of individuals. It establishes the Office of the Data Protection Commissioner responsible for overseeing data protection compliance and handling data protection-related matters.

This article argues that, if not reformed, these defective provisions run the risk of (i) interfering with digital rights and (ii) undermining the efficacy of Kenya’s cybercrime law. To systematically make the case for reform, this article comparatively reviews sections of the Cybercrimes Act by juxtaposing them with their equivalents in international treaties and selected national laws. The article proposes amendments to the Cybercrimes Act so as to result in a much more effective regime of cybercrime law in Kenya.

**CYBERSECURITY:**

* **Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC):** KE-CIRT/CC is Kenya's national cybersecurity incident response team. It is responsible for coordinating responses to cybersecurity incidents and providing guidance and support to organizations and individuals in dealing with cyber threats.
* **Kenya National KE-CIRT/CC Cybersecurity Strategy and Master Plan:** This strategy outlines Kenya's national approach to cybersecurity and sets strategic objectives for enhancing cybersecurity readiness and resilience.
* **National Payments System (NPS) Regulations:** The Central Bank of Kenya has issued regulations that include provisions related to cybersecurity and the protection of electronic payment systems.
* **Banking Act and Banking (Credit Reference Bureau) Regulations:** The banking regulations in Kenya also address cybersecurity concerns, especially regarding the protection of customer data and financial information.