Data protection and right to privacy legislation in Kenya

Andrew Matoke Mankone[1]

Abstract

The Parliament of Kenya enacted the Data Protection legislation which came into effect on November 25, 2019. The new law was passed giventhe provisionsof Article31 of the Constitution of Kenya, 2010 which guarantee the right to privacy as a fundamental right**.** Data Protection and citizens' right to privacy is now a topical concern as evident around the world in many jurisdictions.

The increasing globalization, cross-border transactions, internet penetration and the use of social media and digital platforms among citizens, governments and private institutions raises several data security and privacy concerns that breaches may amount to loss of reputation, identity, safety concerns, legal penalties or compensation for damages or loss of business. As a result, the enactment of Data Protection legislations plays a resounding role in providing the requisite legal framework to regulate the activities of market players, government and private entities, in collecting, storing, processing, accessing, transmitting, sharing and disposing of personal or corporate data among other subjects. This paper reviews the crucial provisions of Kenya's Data Protection law which covers regulated actions seeking compliance by data controllers and processors under the stewardship of the Office of the Data Protection Commissioner ('ODPC'). The paper will also provide a comparative analysis of the practice in other jurisdictions, case laws and court decisions, merits and demerits of data protection legislations and areas of possible data breach targets.

Keywords

Data Protection Legislation,Data Privacy, Data, Kenya

Introduction

A country's legal framework plays an inevitable role in stipulating acceptable conduct, behaviors, rules of procedure and sanctions applicable to its citizens and institutions in furtherance of the protection of individuals' natural rights from violation and preserving peace and unity. Historically, legal sanctions emanating from parliamentary legislative work are characteristically catalytic in fostering social stability and enhancing the realization of conducive conditions for conducting social, economic and political affairs.

The making of laws to govern and regulate the conduct and behavior of the people dates back to the formation of organized societies which consequently necessitated the formation of governments. John Locke, a renowned 17th century English thinker is known to have explained the origin of organized societies or states. People came together and formed the government, so that it could equalize and protect all members of society regardless of their physical and material strength. Thus, people ceded their power to do whatever they pleased and to protect themselves fromthe entity they had formed, that is, the government, henceforth mandated to act on behalf of the people. The People also formulated laws to further protect their rights and to ensure that no person was deprived of his or her rights arbitrarily. As society advanced, the government came to be divided into three arms: known today as the Legislature, the Executive and the Judiciary.

The Parliament of Kenya, is the legislative organ of the Republic of Kenya mandated under Chapter VIII of the Constitution of Kenya 2010 to legislate and deliberate on any matter affecting the people of Kenya including approving resolutions and making recommendations for action by other government organs and state officers. Under Article 94(4) of the CoK, 2010, the exercise of legislative powers by Parliament is envisaged to protect the Constitution of Kenya , 2010 and to promote the democratic governance of the Republic of Kenya.

In view of the above, one of the comprehensive legislative enactments by the Parliament of Kenya is the Data Protection Act, 2019. The law came into effect in November 25, 2019 and regulates data security and privacy in Kenya.

This paper examines Kenya's Data Protection Act, No. 24 of 2019 (the DPA) and other legislative frameworks providing for data security and privacy. The paper sets out a brief background, introduction, definition of data protection legislation and related concepts. Further to providing an analysis of the Data Protection Act of 2019, the paper will highlight the current environment within which the Act operates, and give recommendations on ways to improve and make the already-existing law more effective. This will be followed by a comparative analysis of the practice in other jurisdictions like the European Union (EU), United States (US) and Canada noting the practice and lessons, if any, that could be learnt from these jurisdictions. Finally, the paper will review fundamental court decisions and legal precedents relating to data security and privacy.

Objectives of the study

i. To review legislative frameworks providing for data security and the right to privacy in Kenya
ii. To examine Kenya's Data Protection Act No. 24 of 2019 (DPA)
iii. To conduct a comparative review of data protection and right to privacy practices in other jurisdictions

iv. To review fundamental court decisions and precedents providing for data security and the right to privacy

Statement of the Problem

The pace at which technological advancements are cascading into citizens' daily lives and requiring the acquisition of vast collections of data, storage, processing and sharing by state actors, and businesses is increasingly overwhelming. Governments maintain centralized databases containing millions of citizens' records and collect massive amounts of personal and corporate data sometimes allowing access byprivate players.On the other hand, globalization has opened new possibilities for cross-border transactions, internet penetration, the use of social media and digital platforms among citizens, governments and private entities posing severe data security and privacy concerns. It is argued that market players have the tendency to devise clever ways of avoiding compliance with data security and privacy laws thus precipitating data safety concerns, identity theft, litigations and loss of business(Accessnow, 2021). Possible breach targets involve personally identifiable information like financial, health, intellectual property and legal information concerning data subjects includingunsolicited marketing from private organizations, companies or individuals. Despite the vulnerability of data subjects, the right to privacy and data security provided for in the constitution and other sectorial legislations falls short of the requirements of the digital age thus necessitating the enactment of one progressive law consistent with the practice in other jurisdictions. This was crucial toempowering individuals with enforceable rights over their personal information and providing clear guidelines for data controllers and processors to handle personal data in conformity with legal requirements.

Data protection legislation definition

Data Protection Legislation refers to laws enacted by a House of Parliament to regulate the use of personal or customer information by individuals, organizations and government bodies in a country. The law regulates the activities of market players, locally, regionally and globally, involved with collecting, storing, processing, accessing, transmitting, sharing and disposing of data relating to different subjects. Such laws are anchored on the need to regulate the implementation of legally sanctioned administrative, technical and physical means for guarding against unauthorized, intentional, accidental disclosure, modification or destruction of personal or an entitys data subjecting them to data privacy breaches and insecurity. Protecting privacy is grounded on the notion of human dignity and autonomy on one hand and social order on the other.

Data protection spans three broad categoriesnamely; traditional data protection aspects (such as backup and restore copies), data security, and data privacyaimed at providingproper handling of sensitive data continual availability, and immutability and protecting subjects' rights and interests.

Data security and privacy frameworks in Kenya

Data security and the right to protection of privacy is principally regulated by the national government in Kenya through legislations enacted by parliament and policies and regulations developed by authorities established by the law.

Firstly, article 31 of the CoK (2010) provides for the right to privacy over information relating to family, private affairs and privacy of their communications. Further, article 35 provides for the right to access to information by every citizen including the right to correction or deletion of untrue or misleading information that may affect any person. Based on these fundamental constitutional provisions, the parliament of Kenya has enacted several legislations to provide for data security and protection of the right to privacy. The overarching legislation on data privacy in Kenya is the Data Protection Act, 2019 (DPA) which providesa comprehensive legislative framework on data security and the right to privacy in Kenya giving effect to Article 31 of the CoK (2010).

The Act is supplemented by the Data Protection (General) Regulations, 2021, the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations.

The Access to Information Act, 2016 provides for the right to seek access and obtain information by every Kenyan from public and private bodies acting in a public nature. The Kenya Information and Communications Act, 1998 regulates the information and communications technology industry and outlines the requirements and compliance standards licensed information and communication services as crucial data collectors and controllers must abide by. The law is enforced through the Kenya Information and Communications (Consumer Protection) Regulations of 2010 and the Kenya Information and Communications Act (Registration of SIM Cards) Regulations 2015. Processing of medical data is regulated under the Public Health Act 2012, the Health Act, 2017 and the HIV and AIDS Prevention and Control Act, 2006. Central Bank of Kenya Act and the Central Bank of Kenya's Prudential Guidelines provide for the confidentiality and data privacy provisions of personal information. While processing of financial data is regulated under the National Payment System Act, 2011 and the National Payment System Regulations, 2014. The Consumer Protection Act, 2012 also regulates the protection of consumers of all services cross-cutting all sectors in Kenya. It is worth noting that Kenya has also ratified the International Covenant on Civil and Political Rights (ICCPR) and is a member of the African Union despite having not signed the African Union Convention on Cyber Security and Personal Data Protection (‘Malabo Convention') to actualize the convention (PricewaterhouseCoopers Limited, 2022).

Kenya’s data protection act No. 24 of 2019 (DPA)

The Parliament of Kenya enacted a comprehensive Data Protection law 2019 giving effect to article 31 of the Constitution of Kenya (2010) protectingthe right to privacy as a fundamental right.The Act amended several existing sectoral laws to include provisions on data protection. Where sectoral laws have not been amended to continue to apply to the extent they do not conflict with the Constitution or the Data Protection Act.

The Act covers recorded data whether in automated or non-automated means. The object and purpose of the Act is to regulate the processing of personal data and privacy while ensuring any data processing adheres to subjects’ rights under the established law. The new law is also lauded for establishing legal and institutional mechanism, the office of the Data Protection Commissioner (ODPC) to protect personal data and providing lawful remedies where breaches occur.

The new law also establishes principles of data protection and processing. Firstly, the law prohibits data controllers and data processors from any action unless they are registered with the Data Commissioner. Further, personal data ought to be processed adhering to the subjects' right to privacy, lawfully, fairly and in a transparent manner. The Act requires Data Controllers and Processors to process data lawfully, minimize collection of data, restrict further processing of subject data and requires data controllers and processors to ensure data quality and establish and maintain security safeguards to protect personal data (Deloitte, 2021).

Further, personal data ought to be collected for explicit, specified and legitimate purposes and ought not to be subjected to further processing. Personal data collected should be adequate, relevant, limited to what is necessary, collected only where a valid explanation, accurate and, where necessary, kept up to date, kept in a form which identifies the data subjects for no longer than is necessary and not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The law prescribes legal bases for the lawful processing of personal data including where consent is given, a contract with the data subject, legal obligations, interests of the data subject, public interest and legitimate interests of the data controllers. Where a processing operation is likely to result in a high risk to the rights and freedoms of a data subject, a data controller or data processor is under the law required to carry out a data protection impact assessment prior to the processing. Under the Act, a data subject has a right to be informed of the use to which their data is to be put, to access their data in the custody of a data controller or data processor, objecting to the processing of all or part of their personal data, correction of false or misleading data and deleting of false or misleading data about them. Where there is a real risk of harm to the data subject in case of a breach involving their personal data, there is an obligation to notify the Commissioner within 72 hours; and the data subject within a reasonable time.

The law covers data controllers and processors either established or resident in Kenya and process personal data while in Kenya or not established or ordinarily resident in Kenya, despite processing personal data of data subjects located in Kenya. Thus, it applies to data controllers or processors either established in Kenya or outside Kenya and offering goods or services to data subjects in Kenya or engaged in monitoring behavior of data subjects in Kenya. The law caters for increased territorialcoverage in that it does not matter if the data controller or data processor is established or residing within the country to be enforceable which is one of the similarities with the EU's GDPR.

Other fundamental legal aspects covered include permitted grounds for processing sensitive personal data, conditions for transfer out of Kenya, general exemptions including processing of personal data by an individual for personal or household activity, national security or public interest or disclosure required under any written law or by an order of the court. It further entrenches the following essential elements; penalties for non-compliance, explicit and retractable consent from data subjects, subjects breach notification, privacy by design, data inventory andmandatory data protection officers (Deloitte, 2021).

Despite having been lauded as a progressive law entrenching key provisions essential to the realization of the implementation of the new Act. Emerging evidence points to the fact that the full potential of

the Act of the right to privacy and general data protection, there remains room for improvements in terms is yet to be realized two years into its implementation. Further, the Act does not guarantee the independence of the Office of the Data Protection Commissioner (ODPC) as required to work in consultation and submit reports to the Cabinet Secretary for Information, Communication and Technology (ICT) (Accessnow, 2021).

The practice in other jurisdictions

European Union (EU)

Kenya's Data Protection law is closely modelled afterthe European Union (EU) General Data Protection Regulations (GDPR) by mirroring provisions, requirements, and definitions same as the European counterpart. Theregulations have been in force since May 2018 and give control of personal data to consumers and seek tounify data protection regulations across Europe. The GDPR defines principles for the lawful handling and processing of personal information of individuals who are residents of the European Economic Area (EEA) regardless of their location. Handling personal information involves the organization, collection, storage, structuring, use, consultation, combination, communication, restriction, destruction, or erasure of personal data. The regulations are anchored on the principles of fairness, lawfulness, and transparency**,** data minimization**,** storage limitation**,** accuracy**,** confidentiality and integrity**,** accountability. Concerning territoriality coverage, the regulations are automatically enforceable in EU member states and the processing of any information of any individual located in the EU regardless of where the processing occurs.

Further, GDPR establishes the EU's Data Protection Authority for the enforcement of rules and holding organizations liable to fines in the event of a breach of the rules. While The GDPR is enforced by the Information Commissioners Office (ICO), each EU State is required to appoint a Supervisory Authority to monitor the application of the regulations.Finally, the regulations impose penalties for noncompliance, which can go up to twenty million Euro (EUR 20 000 000) or four percent (4%) of the total worldwide annual turnover of a company.

The United States

In contrast to its European counterparts, the United States does not have one comprehensive federal law regulating data security and privacy. Nevertheless, there have been numerous attempts earlier and currently, the new proposed federal privacy law, the American Data Privacy Protection Act (ADPPA) has made it further than any of its predecessors (Osano Staff, 2022).

The US practice governing enforcement of data security and privacy matters isanchored on federal statutes at the Federal level and specific states legislations at the state level. The federal statutes are primarily sector-specific and regulate the collection, storage and use of sensitive non-public personal information. Federal Trade Commission (FTC) under the Federal Trade Commission Act is vested with very broad authority including setting the tone on federal privacy and data security issues. Other implementing entities include the Office of the Comptroller of the Currency (OCC), the Department of Health and Human Services (DHH), the Federal Communications Commission(FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), just mentioning a few. Some Federal- level statutes include the Drivers Privacy Protection Act of 1994 regulating privacy and disclosure of personal information gathered by state Departments of Motor Vehicles, the Children

Online Privacy Protection Act, the Cable Communications Policy Act of 1984, The Video Privacy Protection Act and Fair Credit Reporting Act.

State-level statutes on the other hand regulate a wide range of data security and privacy rights of individual residents. They impose restrictions and obligations relating to the collection, use, disclosure, security, and storage of personal information, biometric data, medical or financial records insurance information, payment card information etcetera. Every state has in place data breach notification legislation relating to types of personal information protected. Businesses must comply with specific states' regulations even when they have no physical presence in a particular state. Examples of state-level statutes include the Califonia Privacy RightsAct, the CalifoniaPrivace Protection Agency (CPPA). U.S. state attorneys general oversee data privacy laws governing the collection, storage, safeguarding, disposal and use of personal data collected from their residents, especially regarding data breach notifications and the security of Social Security numbers.

The USA federal and State level approach to data security and privacy enhances territorial scope considering businesses established in other jurisdictions are subjected to both federal and state data protection laws for activities impacting US residents. Further, the processing of personal data is regulated based on the principles of transparency, lawful basis, purpose limitation, data minimization, proportionality and storage. States level statutes provide for subjects' rights to access data, the rectification of errors, deletion, objection to processing, data portability, withdrawal of consent, objection to marketing, protection against solely automated decision-making and the right to complain to relevant data protection authorities. Further, it is notable that the appointment of Data Protection Officers is not required under US laws, despite certain statutes requiringthe appointment or designation of individuals or individuals charged with compliance with the privacy and data security requirements under the statute.

Almost every Data protection and privacy law in the United States has a breach notification provision requiring private or governmental entities to notify individuals of security breaches involving personally identifiable data and setting out what constitutes a security breach, notice requirements and any exemptions.

Canada

Data protection and privacy legislations in Canada are enacted at federal, provincial and territoriy levels and complimented by Sector-specific data privacy legislations. It is a practice of multiple legislations that tend to overlap but enforcement is overseen by different regulators depending on their jurisdiction and mandates.

The Country has 28 federal, provincial, and territorial privacy statutes legislating the protection of residents' data in private, public and health sectors. The different statutes vart in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) was enacted in 2000 and amended by Canada's Data Privacy Act, 2015 which came into force only in November 2018 and regulates the collection, use and disclosure of employee personal information by federally regulated employers, personal information handled in the course of a commercial activity, federally

regulated business like banks, airlines and telecommunications and exempts provinces and territories with substantially similar legislation. PIPEDA upholds the principle of accountability, lawful purpose for data collection, subjects consent, limiting collection, use and disclosure, accuracy of data, security, openness, subjects' access and right to challenging compliance.

Canada's Privacy Act, RSC 1985, c P -21 is sector-specific law governing personal information processed by the federal government information. Specific provincial legislations also apply to personal and consumer information handled by public bodies and institutions within their jurisdiction.

Further, three provinces namely, Alberta, British Columbia and Quebec have data security and privacy legislation of general application to the private sector, which are substantially similar to PIPEDA and apply to the collection, use and disclosure of employee and non-employee information within their jurisdiction. Health data in other provinces are also protected by local legislation but once data crosses provincial or national borders PIPEDA applies. Collectively, PIPEDA, Alberta Personal Information Protection Act, 2003, British Colombia Personal Information Protection Act, 2003, and Quebec Act are referred to as Canada's principal legislation on data protection and privacy.PIPEDA lacks provision for its territorial reach. Further, the Federal Court of Canada has ruled that PIPEDA does apply to businesses found in other jurisdictions if there is a substantial connection between an organization's activities and Canada. This raises serious ramifications for any countries and international organizations targeting Canadian customers.PIPEDA and the Privacy Act are overseen by the Office of the Privacy Commissioner of Canada (OPC) while provinces and territories appoint regulators for overseeing compliance with privacy statutes within their jurisdiction.

African countries

In recent years, there has been increased interest in the regulation and governance of personal data throughout Africa following 2016 General Data Protection Regulation (GDPR) of the European Union (EU). Brian Daigle, 2021 –Numerous countries have sought to amend existing data protection policies or working to establish structures to enforce existing laws and regulations. As of August 2020, that number had quickly risen to 31 countries. Countries including Ghana, Kenya, Madagascar, Mauritius, Nigeria, Rwanda, South Africa, Togo, Uganda and Zimbabwe Egypt.

In Ghana, like the practice in Kenya, data protection is regulated under the Data Protection Act, 2012 (DPA) together with Article 18(2) of the 1992 Constitution, which provides citizens with a fundamental right to privacy. There has been resurging dialogue among African states on consolidating and harmonizing data protection and privacy laws and the need for standardized data protection laws across the continent informed by the emerging discussions on data sovereignty, economization and data localization. Other emerging considerations include the need for entrenching data protection certifications as an eligibility criterion for running a business in countries and other measures for expediting the swift handling of fast growing data breaches and cyber-crimes.

Court decisions and cases

The following court rulings and decisions lay fundamental principles and precedence on the place of individuals' rights to privacy and data protection under the rule of the law;

I. The High court case *Nubian Rights Forum & 2 others v Attorney General & 6 others;*

The petitioners challenged the Statute Law Miscellaneous (Amendment Act), 2018 that amended the Registration of Persons Act by introducing National Integrated Information Management System **(**NIIMS**),** intended to be a single repository of personal information of all Kenyans as well as foreigners resident in Kenya. The amendments raised concerns regarding constitutional right to privacy considering there were lacking proper mechanisms in place to safeguard personal information to be collected under the NIIMS system. The High Court ruling cited imminent threat to the right to privacy with respect to the collection of biometric data and GPS coordinates when protection measures in place were inadequate. Biometric data and GPS coordinates required as per the new law were regarded as personal, sensitive, and intrusive data that required protection, a strong security policy and detailed procedures on its protection and security in accordance with international standards. In a nutshell, the judgement acknowledged the importance of a data protection framework.

II. In the case involving *Volker and Markus ScheckeGbR (C-92/09) and HartmutEifert (C-93/09) v State of Hesse*

The proceedings were brought by agricultural operators against the Land of Hesse following the publication on the website of the German Federal Office for Agriculture and Food of the operators' personal data after benefiting from funds from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). The agricultural operators contested such publication, claiming, it was not justified by an overriding public interest. Further, the operators argued that the European Union rules which imposed on the Bundesanstalt the obligation to publish such data amounted to an unjustified interference with the fundamental right to the protection of personal data.

The Administrative Court upheld that the publication on the website of data naming the operators as beneficiaries and indicating the precise amounts they received amounted to interference with theirfundamental rights, respect for their private life and the protection of their personal data because of the fact that such data become available to third parties.

Conclusion

There is increasing awareness ofthe need for data protection and privacy regulation frameworks around the world including mechanisms for strengthening the implementation of such laws.Most advanced economies like the USA and Canada have in place comprehensive data protection and right to privacy laws enforced at different levels of governance such as federal and decentralized structures and sector-specific laws and regulators appointed to enforce and oversight legislation within their jurisdictions. The enactment and enforcement of multiple legislations at different levels of governance provide a water-tight approach to protecting and strengthening the implementation and oversight of data security and individuals' privacy.

In Kenya, data protection and the right to privacy is comprehensively legislated by national legislations enacted by the parliament of Kenyaand enforceable throughout the republic by National Authorities. Considering the place of devolved governance as relates to data security and protection, as needful as it may appear, giving some roles to county governments in developing and enforcing data protection laws within their jurisdictions like other jurisdictions may trigger constitutional validity of the distribution of functions between the national and county governments. While the Fourth

Schedule of the CoK (2010) provides for the distribution of functions between the national and county governments, it does not come out clearly on who is vested with data security and privacy regulation despite providing expressly on consumer protection as a preserve of the national government and mandating parliament to legislate on any matter affecting Kenyans and the law being enforceable nationally.

Whereas Kenya's data protection and privacy law bears resemblance with the practice in other jurisdictionslike European, the United States and African Countries, the key areas of convergence include the recognition and giving of data subjects' rights, regulating controllers and processors, providing territorial coverage of the law, lawful handling and processing of subjects data, the appointment of authoritiesfor enforcingthe law, legal bases for lawful processing subjects data, exemptions to the law and fines and penalties.

Kenya's data privacy law prides itself on its extra-territorial coverage in that it not only regulates the activities of data controllers and processors established in Kenya but also those outside Kenya andengages in processing data relating to Kenyan subjects. This is a crucial feature considering the interconnectedness of the global economy.

Finally, the reforms under the Data Protection Act introduce new requirements for compliance in terms of organizational accountability and enforcement of data security and the right to privacy. This will affect ways in which new technologies will be designed and managed by organizations to address the privacy threshold set by the law.

Despite having been lauded as a progressive law entrenching key provisions essential to the realization of the right to privacy and general data protection, there remains room for improvements in terms of the implementation of the Act. Further, the Act ought to guarantee the independence of the Office of the Data Protection Commissioner (ODPC) as required to work in consultation and submit reports to the Cabinet Secretary for Information, Communication and Technology (ICT) .

REFERENCES

Access Now (Website):Access Now. (n.d).Home. https://www.accessnow.org/

Gitau. V,Ochilo Louisa (2018).Data Protection in East Africa.

The Constitution of Kenya (2010)

The Data Protection (General) Regulations, 2021

The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021

The Data Protection (Civil Registration) Regulations, 2020 (DPA Regulations

The General Data Protection Regulation (GDPR) (European Union)

Nubian Rights Forum & 2 others v Attorney General & 6 others

Volker and Markus ScheckeGbR (C-92/09) and HartmutEifert (C-93/09) v State of Hesse

Endnotes

[1]Andrew Matoke Mankone is the Chief Librarian at the Parliament of Kenya. He can be reached by email: andrewmankone@gmail.com