JOURNAL OF AFRICAN POLITICS, 1 (2021): 66–88

KENYA'S DATA PROTECTION REGIME: CHALLENGES AND FUTURE PROSPECTS

Oscar M. Otele
Lecturer, Department of Political Science and Public Administration, University of Nairobi, Main Campus, Gandhi Wing – 4th Flr, Office No. 403 C, Nairobi, Kenya
Email: otele@uonbi.ac.ke

Abstract

In light of the emerging scholarly interest on data protection regimes in developing countries, this article addresses the following fundamental question. What are the challenges and future prospects for the data protection regime Kenya? The article utilizes Robert Cooter's Theory of market modernization of law, which postulates that several forces act as the impetus for the law reform, including the state, market (industry), and the public. The study findings indicate that the commitment to uphold the primacy of public security, absence of unified supervisory system, inadequate financial resources are some of the challenges of data protection regime in the country. Others include inability of data commissioner to control data processors and data controllers, and potential conflict between the data commissioner and the cabinet secretary. The prospect of the data protection law, the study concludes would depend on the following: ability of policy implementers and enforcers to pay more attention on protecting individuals' data privacy. There is also ample opportunity for policy implementers and enforcers to learn best practices from countries with data protection regimes.

Keywords

Data protection, Kenya, Law, Policy Implementer, Regime

1 Introduction

After close to a decade of debates, in November 2019 Kenya made into law the Data Protection Act (Act No. 24 of 2019) largely modeled along the lines of European Union General Data Protection Regulations (GDPR). The GDPR governs the use of personal data in the context of the activities of an establishment of a data controller or a data processor in the EU regardless of whether the processing taking place in EU or not. And much later President Uhuru Kenyatta appointed Ms. Immaculate Kassait as the first Data Protection Commissioner (henceforth Data Commissioner). Arguably, the enactment of the law and the appointment of the Data Commissioner represent a major triumph for the enthusiasts of the international expansion of data protection regime. Indeed the appointment placed Kenya on establishing "the institutional framework required for enforcement of data subjects rights provided for under the Data Protection Act and in effect guarantee the right to privacy as protected by Article 31 of the Constitution" (Laibuta, 2020a). However, these developments are likely to invite some challenges especially in the current context of Coronavirus (Covid-19), a global pandemic that has increased demand for use of information technology. Further, going by Kenya's poor implementation record of national laws, concern has raised as to whether the state would effectively protect citizen's privacy. In light of this concern, a fundamental question is: What are the challenges and prospects for the data protection regime in the country? Given that the implementation of the law is still in infancy, an additional concern is: What needs to be done to overcome the challenges?

Some of the existing studies on the subject focus on the impact of GDPR on global technology development (Laibuta, 2020b; Li, Yu & He, 2019), on cross-border issues concerning data protection law (Bu-Pasha, 2017); foundational understanding of the development of data protection regime (Greenleaf, 2012; 2017) and implications of cybersecurity law (Lee & Liu, 2016; Parasol, 2018). Much of the discussions in Africa center on directing standards and the spirit of subsequent data protection (Abdulrauf & Fombad, 2016; Breckenridge, 2019; Kivikuru, 2017;2019; Thiel, 2020). The "understanding of the concepts of [privacy] and personal data protection and institutional data governance" (Laibuta, 2020b) and the question about the challenges and prospects of Kenya's data protection regime remains largely unexplored.

This article was inspired by a study that sought to explore the impact and perceptions toward data protection and access to information related laws, proposals and policies.[1] Both secondary and primary data were collected. Secondary data was obtained from existing relevant academic literature with a view of understanding how access to information and privacy right is safeguarded in other jurisdictions. An analysis of the performance of data protection bodies in the EU and some parts of Asia was key in discerning the challenges and prospects for the Kenyan data protection regime. Primary data was collected at two levels. At level one, the study reviewed the legal framework governing information retrieval and security of personal data. At level two, the researcher collected data from key informants using a questionnaire generated by survey monkey via the *WhatsApp* platform. Further follow-up was made through phone calls and email communication for clarification about emerging issues in the context of Covid-19.

The article utilizes Robert Cooter's Theory of market modernization of law which postulates that several forces act as the impetus for the law reform, including the country, market (industry), and the people (Cooter, 1997). The development of law as influenced by various forces reveals different characteristics leading to different results. Consequently, the article examines challenges emanating from the following: Information and Communication Technology (ICT) strategies and the existing legal structure. Four concepts deserve clarity: personal data, data protection impact assessment, right to privacy and data compliance. Personal data refers to "information relating to an identified or identifiable natural person, that is, a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" (Republic of Kenya, 2019). Data protection impact assessment refers to "an assessment of the impact of the envisaged processing operations on the protection of personal data" (Republic of Kenya, 2019). Right to privacy refers to protection of "an individual's private life" from the undesirable investigation, data protection

[1] https://info.mzalendo.com/media_root/file_archive/DIGITAL_RIGHTS_IN_KENYA.pdf (Accessed 20 October 2021).

refers to the reasonable and appropriate use of a person's information, while data compliance refers to "protecting, respecting and promoting the individual right to privacy" (Laibuta, 2020c). The article is set out in the following manner. The first section provides descriptive information about the development of ICT strategies and their challenges for Kenya's data protection. This is followed by an examination of the strengths and weaknesses of the legal framework undergirding data protection in Kenya. The article then presents some of the challenges the data protection regime is likely to face. The concluding section provides prospects for a data protection regime in Kenya.

2 Development of ICT strategies and the challenges for Kenya's data protection

Kenya's data protection regime is rooted in the gradual evolution of the ICT industries unequivocally bolstered by a cluster of national development strategies. These strategies drive national economic growth and have a significant effect on the security of common citizens' fundamental rights. This section examines the influence of Kenya's ICT development system on data protection. It contends that the emergence of an ICT development system in response to the "ever-evolving and innovative technology space" (Laibuta, 2020b) is likely to constrain the implementation of a data right.

2.1 ICT development strategies

In the early 2000s, the new leadership in Kenya embraced ICT in the economic blueprint when it explicitly recognized the economic values and benefits of ICT services in bolstering efficiency and empowerment of the populace. Consequently, the government laid out the following strategies: "I) Set up an Inter-Ministerial Committee to join forces with the [National Economic and Social Council] NESC to integrate ICT into government operations to improve proficiency and performance; II) Contribute sufficient ICT education and training…by reforming the education programs to consolidate IT studies to create suitable skill prerequisites; III) Actualize carefully-structured taxation

policies on both computer software and hardware to make them economical to small and medium enterprises, and citizens with low income; IV) Re-evaluate the legal structure to extricate obstacles that have debilitated adoption and utilization of e-commerce; V) Augment a blueprint for e-government by end of June 2004" (Republic of Kenya, 2003). Consequently, in 2004 the government developed a plan which prioritized the enactment of ICT policy and *E-Government Strategy*, expansion of the information infrastructure, development of information websites for ministries and educate all civil servants on IT literacy and computer-related studies in the short term. In the medium term, the government prioritized digitization and incorporation of government data and records, completion of network infrastructure development, implementation of web-based and database management systems to coordinate data sharing within government (Republic of Kenya, 2004). These strategies were comprehensively detailed in the *ICT Policy* of March 2006 which acknowledged the importance of accessing information and safeguarding ICTs (Ministry of Information, Communications and Technology, 2006).

The launch of *Kenya Vision 2030* in June 2008 further provided a policy environment for the development of ICT strategies. The vision considers ICT as a key foundation and enabler for all the other sectors (Republic of Kenya, 2008). Although the long-term vision draws a nexus between technological development and democracy, it lends itself more to technology while ignoring the utility of ICT in service sectors such as health, agriculture, transport, education, and business (Kivikuru, 2017), where a majority of citizens are found. Under the Medium Term Plan (2008–2013) of Kenya's grand strategy, the Ministry of ICT laid the foundation for enhancing digital money transfer. A sizeable proportion of the arranged national ICT infrastructure saw enhanced widespread of ICT services, seeing Kenya connected to the international broadband highway (Ministry of Information, Communications and Technology, 2013). As a result, many towns got connected to national core network infrastructure while at the same the government established a data centre to ensure that its own documents and citizens' applications were secured. Data transmission capacity to government offices expanded by 25 percent of the internet speed leading some ministries to develop the internet-based enterprise to foster better services. The government developed the Konza Techno City focusing on among others "Business Process Outsourcing (BPO),

Internet Enabled Services (ITES), software development, data centers, disaster recovery centers and call centers" (Ministry of Information, Communications and Technology, 2013). Other strategies entailed the launch of digital villages, digitization of government records and offering internet and network access to government, social instititions, film production, and creation of an open data portal. All these strategies saw Kenya rank positively in 2012 the global lobal data outlook initiative (Ministry of Information, Communications and Technology, 2013).

Later in 2013, the Ministry of ICT reviewed the *National ICT Policy* prioritizing internet access, and in the same year, the Ministry launched a strategic plan (2013-2017) hailed as strongly technology-oriented. The Ministry emphasized coordination and cooperation in ICT processes between the national government and county governments. Subsequently, President Kenyatta launched *The Kenya National ICT Masterplan (2014-2018)* anchored on three foundations, namely: human capacity in ICT; the consolidated ICT infrastructure; the consolidated information infrastructure (Ministry of Information, Communications and Technology, 2014a). In terms of ICT's human capacity, the expected results were the presence of a high-quality labor force for business, and also an "ICT literate population capable of exploiting ICT products and services for improved quality of life" (Ministry of Information, Communications and Technology, 2014a). Although the citizens are included, the shortcoming of the Masterplan is that the strategies to attain the goals are considerably more detailed in terms of the workforce qualification than ICT literacy for the public. The Masterplan re-introduced the idea of *e-government,* seeing it as the driver of Kenya's economy. Building on this Masterplan, the Ministry further launched *National Cybersecurity Strategy* anchored on four points:

> I) [e]nhance the nation's cybersecurity posture in a manner that promotes the country's growth, security, and wealth; II) [b]uild national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs; III) [f]oster an integrated system and communication among relevant stakeholders to facilitate

> a well-connected workplace focused on achieving the strategy's goals and objectives; IV) [p]rovide governance by laying out the national cybersecurity guiding principles and consolidating cybersecurity initiatives at the national level (Ministry of Information, Communications and Technology, 2014b).

Still, in 2014, the government announced plans to develop the National Digital Registry System (NDRS) for "panoptic biometric registration" (Breckenridge, 2019), but failed due to competing interests between banks, donors, telecom firms, politicians, and bureaucrats. Later in 2017, the government launched the *Big Four Agenda* focusing on revamping the manufacturing sector, attaining universal health coverage, advancing food security, and provision of affordable and decent housing for all Kenyans by 2022. Just like Vision 2030, the ICT was singled out as the enabler for the achievement of the Big Four. In 2018, the government further launched the *National Broadband Strategy* anchored on the execution of key flagship projects such as last-mile connectivity by extending broadband to the ward levels, design and manufacture of broadband devices in Kenya; establish a cyber-security operation center, and international collaboration on cybersecurity. Perhaps the most elaborate advancement in ICT industry came with the enactment of *Communications and Technology (ICT) Policy* in November 2019 focusing on ICT mobility, faster electronic of money, improvement in ICT skills and innovation, public service delivery, and security of ICT (Ministry of Information, Communication and Technology, 2019. *National ICT* Policy, pp. 12-25).

2.2 Influences of ICT policies on data privacy

The elucidated ICT policies are likely to impact the implementation of a data protection regime in the following three ways. First, the "ever-evolving and innovative technology space" (Laibuta, 2020b) derived from the application of these policies is likely to increase the risk to protection of individual privacy. Some scholars aver that the development in ICT tends to offer government and some private security companies surveillance powers over common people (Crawford & Schultz, 2014; Ohm 2010). Kenyan security agencies are now increasingly applying latest advancement in technology to perform their tasks. Under the evolving Covid-19 situation, technology companies assisted

public security agencies to design surveillance systems that capture "big data and cutting-edge voice". Technological advancement presents challenges to citizens' data privacy and even greater challenges to law enforcement in implementing better policies on data protection. Second, these policies are myopic in many facets of data protection. Even though the strategies consolidate on information security, these requirements are by and large brief and vague which is contradictory to the comprehensive necessities on technological developments. For example, the *National ICT Policy* seeks to "develop information security standards for the ICT sector which are to be adopted and applied by all government agencies and recommended as best practices to private sector business" (Ministry of Information, Communication and Technology, *National ICT Policy*, 2019, p.36). It is not clear what these standards are and what the best practices entail.

Third, the application of ICT to advance Kenya's ambitious economic growth set in *Vision 2030*, and as defined within a relatively short time defined by medium-term development plans tend to upset the balance of power between economic growth and the desire for data protection. The economic growth strategies layout specific dates for the conclusion and offers comprehensive objectives. Indeed, the short time for conclusion would imminently results to uncoordinated realization of appropriate strategies which may exert considerable pressure on law enforcers who may lack adequate time to respond to the reality of the law and the desired economic growth. Such uncoordinated implementation is likely to realize economic growth at the expense of network security and data protection.

3 The legal framework on data privacy

In Kenya, the law on data protection is spread within the rules on retrieval of information, sanctity of government records, data protection and information security. This section elaborates on the application of the provision of the Constitution of Kenya, 2010; Access to Information Act No. 31 of 2016; the Computer Misuse and Cybercrimes Act 2018; the Statute Law (Miscellaneous Amendments) Act No. 18 of 2018 and the Data Protection Act No. 24 of 2019.

3.1 The Constitution of Kenya, 2010

This is the supreme law regulating the conduct between the governor and governed in Kenya (Republic of Kenya, 2010, p.14). The document lays the foundation for the integrity and security of the basic rights and freedoms as stipulated in the Bill of Rights, touted as one of the most progressive and liberal regimes of human rights in the region. These rights must be honored, observed, and protected by every entity and agency within the government as well as its citizens. Article 10 of the Constitution of Kenya (CoK) further provides national values and principles of governance such as "rule of law, democracy, citizen inclusion, morality, openness, and accountability" key in the fulfillment of these rights.

Article 31 of the Constitution provides that "every person has the right to privacy, which includes the rights not to have (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed". Relatedly, Article 35 provides that: "(1) Every citizen has the right of access to- (a) information held by the State; and (b) information held by another person and required for the exercise or protection of any right or fundamental freedom". Therefore, the right to privacy and access to information are interrelated and the data protection regime is anchored on these constitutional foundations.

Whereas Article 31 ensures a common right to protection, while also guarding against particular encroachments of privacy, counting the pointless disclosure of data relating to family or private issues, Article 35 lays the foundation of the right to information because it articulates the rights of an individual concerning information access or deluding data relating to the influenced individual. It also stipulates the responsibility of the State relating to the publication of information that relates to the State. It follows that citizens' freedom of information access can only be limited on condition that the State produces evidence showing that the needed information falls within the ambit of limitations enshrined under Article 24 of the Constitution. The constitutional limitations could be viewed as parameters for any attempt at violating the privacy rights and access to information, and must be operationalized to such extent that is acceptable in a democratic society. In

this circumstance, it implies that in the event of a denial for a claim to privacy and access to information is not "acceptable and demonstrably justifiable", such a denial is assumed to violate the constitutional rights to privacy and access to information. For access to information, disclosure of such information may be useful in combating corruption and checking on the abuse of power in Kenyan governance. Also, respecting demands to access to information is a critical component in strengthening and elevating the democratic values of openness and accountability. Article 35 on Access to Information is therefore crucial in ensuring that publicly held information is in real-time access to the public for updates on government policy issues that have an immediate effect on the protection of their basic rights.

Further, although the Constitution provides that citizens have acesss to any information within the perview of the State, the broad definition of State that includes two levels of government and their accompanying institutions places heavy responsibility on the State than private bodies. Further, the constitutional interpretation of person includes "companies, associations, or other body of persons whether incorporated or unincorporated" (Republic of Kenya, 2010, Article 260). It is not clear whether the said person also includes private citizens like bloggers who may have the information.

3.2 Access to Information Act No. 31 of 2016

The Act was enacted pursuant to Article 35 of Constitution of Kenya 2010 and establishes the Commission on Administrative Justice (CAJ) as the oversight body. Among others, the Act seeks to:

> grant effect to the right to information access by citizens as directed under Article 35 of the Constitution; provide a system for public and private entities to uncover information that they possess and report information on request per the Constitution standards; give a system to encourage information held by private bodies in compliance with any right secured by the Constitution and by other law; advance schedule and precise data revelation by public and private bodies on constitutional standards relating to responsibility, straightforwardness, and public cooperation and access data; provide

> for the assurance of people who disclose data of public interest in great confidence, and provide a system to encourage public awareness on the right to access information under [the] Act (Republic of Kenya, 2016, Section 3).

According to the Act, a person shall be provided with the required information if justified reasons are provided (Republic of Kenya, 2016 Section 5) . Under Section 14 of the Act, requested information is thought to be denied when an applicant fails to receive a response from the information access officer regarding the information within the stipulated time. What is more, the Act allows an individual to apply for the review decision from the CAJ in the event the request is denied (Republic of Kenya, 2016, Part IV). Moreover, the Act shields for the security of the information and provides an offense for any individual to disclose absolved information in repudiation of the Act, that may lead to the imprisonment for three years, detainment or a fine not surpassing one million or both as provided in Section 28.

In realizing the above objects, the Act specifies the citizen's right to information in the State's domain or private entities by classification of information as per Article 35 of the Constitution. Section 6 (1) of the Act further clarifies the following limitations for the right of access to information.

> [threat to] the national security of Kenya; hinder[ance] to the legal procedure; [interfering with] the security, wellbeing or life of any individual; ...intrusion of the protection of a person, other than applicant or the individual on whose sake an application has, with legitimate specialist, been made; considerably preference the commercial interface, counting mental property rights, of that substance or third party from whom data was gotten; cause significant hurt to the capacity of the Government to oversee the economy of Kenya; essentially weaken an open or private entity's capacity to allow satisfactory and reasonable thought to a matter regarding which no judgement has been passed and which is open to interpretation; harm an open entity's position in any real or mulled over legitimate procedures; or encroach proficient privacy as indicated in law or by the rules of a constituted association of a profession (Republic of Kenya, 2016, Section 6).

This implies that there are circumstances where the request to access certain information could be maliciously rejected under the disguise of falling under the limitations. Following this, it could be argued that whereas it is fair to expect the Act to provide certain limitations of access to information from the public domain, the misuse of limitations by the State is unconstitutional.

The fact that an Act had to be put in place naturally means that the Constitution could not be comprehensive in its provision. Section 17 of the Act widens the scope of the information to include the management of records which include "documents or other sources of information compiled, recorded or stored in written form or any other manner and includes electronic records". Finally, Part IV, Section 25 provides for how regulations may be established to refine the realization of the Act. The Executive is yet to operationalize these regulations.

3.3 The Computer Misuse and Cybercrimes Act 2018

The Act was enacted to "provide for offenses relating to computer systems, to enable timely and effective detection, prohibition, prevention, responsive investigation and prohibition of computer and cybercrimes and to facilitate international co-operation in dealing with computer and cybercrime matters" (Republic of Kenya, 2018a). The law addresses violations such as cybercrime, backdoor, computer forgery and counterfeiting, fraud, false publication, child pornography, cybersquatting, phishing, identify theft, cyber terrorism among others.

Shortly after the President assented to the Act, the High Court issued a conservatory order setting aside the enforcement of 26 sections of the Act, following a suit filed by some civil society activists challenging "the law for violating constitutional provision on rights of opinion, expression, free media, and the security of person, right to privacy, right to property and the right to a fair hearing". The conservatory order was hailed as a win for digital rights enthusiasts in Kenya and also marked a key milestone in the litigation in respect to the protection of digital rights in the country.

After a protracted court battle, the High Court lifted the conservatory order, affirming the 26 sections as constitutional, even though there are still some weaknesses. One, instead of placing more emphasis on crimes found in

cyberspace and those crimes related to ICT systems, transactions, and communications, the Act goes above and beyond to deal with free speech. Two, there is no scientific formula for determining what is false or 'fake news'. For example, it will be difficult to determine the authenticity of what is 'fake news' as provided in Sections 22 and 23 of the Act which prohibits false publication, deceptive or fictional data, or information that is intended to cause others to act on them as authentic. Three, the concept of 'fake news' is vaguely defined opening the door for varied interpretation, and law enforcers can take advantage of this gap to arbitrarily interpret what entails 'fake news'. Further, the law enforcers may conceal government misconduct, constrain the expression of critical opinions, and limit the free speech of the political opposition, bloggers, human rights defenders, and journalists.

3.4 The Statute Law (Miscellaneous Amendments) Act No. 18 of 2018

Through this omnibus law, the government amended several stipulations of existing decrees, especially laws pertaining to registration of persons. The Act establishes the National Integrated Identity Management System (NIIMS) whose registration process assigns applicant *Huduma Namba* (service number). The eleven functions of the NIIMs are outlined in Section 9A as follows: One, "to create, manage, maintain and operate a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya", two, "to assign a unique national identification number to every person registered in the register", three, "to harmonize, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons", four, "to support the printing and distribution for collection of all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification cards issued under the Births and Death Registration Act, Basic Education Act, Registration of Persons Act, Refugees Act, Traffic Act and the Kenya Citizenship and Immigration Act and all other forms of government issued identification documentation as may be specified by gazette notice by the Cabinet Secretary", five, "to prescribe, in consultation with the various relevant issuing authorities, a format of identification document to capture the various forms of information contained in the

identification documents for purposes of issuance of a single document where applicable", six "to verify and authenticate information relating to the registration and identification of persons", seven "to collate information obtained under th[e] Act and reproduce it as may be required, from time to time", eight " to ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register", nine "to correct errors in registration details, if so required by a person or on its own initiative", ten "to ensure that the information is accurate, complete, up to date and not misleading" and eleven, "to perform such other duties which are necessary or expedient for the discharge of functions under th[e]Act" (Republic of Kenya, 2018b, The Statute Law (Miscellaneous Amendments))

In reaction to the enactment of the statute, a section of the public raised concern and filed a suit at the High Court, expressing strong reservations on the security of their data. The petitioners claimed that the Statute contravened the Constitution and could threaten the individuals' rights. At the time of writing this article, the High Court had declared *Huduma Namba* unconstitutional.

3.5 The Data Protection Act No. 24 of 2019

The Act was enacted pursuant to the constitutional requirement of Article 31(c) and (d). The Act establishes the Office of the Data Protection Commissioner responsible "for the monitoring of the processing of personal data and providing for the rights of data subjects and obligations of data controllers and processors". Under Section 8, the Data Commissioner among others shall:

> oversee the implementation of and be responsible for the enforcement of the Act; establish and maintain a register of data controllers and data processors; exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verifying whether the processing of data is done in accordance with the Act; promote self-regulation among data controllers and data processors; conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the

> provisions of the Act or any other relevant law; receive and investigate any complaint by any person on infringements of the rights under the Act; take such measures as may be necessary to bring the provisions of the Act to the knowledge of the general public; carry out inspections of public and private entities with a view to evaluating the processing of personal data; promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements; and undertaking research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any development on the privacy of individuals (Republic of Kenya, 2019, Section 8).

The above wide statutory powers would ensure data protection, and when adhered to would allay fears of data processing in managing the Covid-19.

Section 26 of the Act specifies the "rights of the data subject, including the right to protest to the processing of his or her data", while Section 30 (1) of "the Act provides that the data subject must approve the processing of his or her data". These sections in the Act embolden protection of data rights. Section 31 of the Act provides for data impact assessment. In the event the processing of data may infringe upon the basic rights of data subjects, the Act provides that an information controller or information processor must carry out a data security impact evaluation. Section 31(2) provides that the evaluation of the elements of a data security impact appraisal might incorporate:

> an efficient portrayal of the imagined processing operations and the reason of the handling, including, where appropriate, the authentic interest sought after by the information controller or information processor; an appraisal of the need and proportionality of the preparing operations in connection to the purposes; an appraisal of the dangers to the rights and freedom of information subject; and the measures conceived to address the dangers and the shields, security measures and instruments to guarantee the security of individual information and to illustrate compliance with the Act, taking into

consideration the rights, and genuine interest of information subjects and other people concerned.

Section 31(3) provides that "the data controller or data processor shall seek approval from the Data Commissioner before the processing if a data protection impact assessment conducted under the section indicates that the processing of the data would present a risky scenario to the rights and freedoms of the data subject". Section 41 of the Act provides for "data protection by design or by default". Section 41(1) provides that "every data controller or data processor should implement practical and institutional safeguards designed to establish the data protection principles effectively and to integrate precautions for that purpose into processing". Section 41(3) further states that an information controller or information processor ought to execute fitting specialized and organizational measures for guaranteeing that, by default, as it were individual information which is vital for each particular reason is prepared, taking into perspective the sum of individual information collected, the degree of its preparation, the period of its capacity, its availability and the cost of preparing information and the advances and instruments utilized. Section 41(4) sets out-degree that an information controller or information processor might consider, these incorporate- to recognize sensibly predictable inside and outside dangers to individual information beneath the person's ownership or control and to set up and keep up fitting shields against the recognized dangers; to guarantee pseudonymization and encryption of individual information; to provide for access to individual information in an opportune way within the occasion of a physical or specialized occurrence, and to confirm that the shields are successfully executed and to guarantee that the shields are ceaselessly upgraded in reaction to new risks or insufficiencies.

However, there are some weaknesses in the Act. The Office of the Data Commissioner is not a constitutional independent office and this may erode data protection. Section (5) (5) of the Act states that "the Data Commissioner shall in agreement with the Cabinet Secretary institute such directorates as may be necessary for the better execution of the function of the office". This implies that in the execution of the functions, the Commissioner would not be totally independent, thus the office holder will be subject to the influence of the higher authorities.

Section 24(1) of the Act provides that "a data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine". However, this provision is not stated in mandatory terms, implying that it is not an obligatory commitment for the concerned officer to employ a data protection officer. Article 37 of GDPR states that "The controller and the processor shall designate a data protection officer". Further, Section 24 provides that the data protection officer would be employed or nominated where:- "the processing is carried out by a public body or private body, except for courts acting in their judicial capacity; the core activities of the data controllers or data processors consist of processing operations which by nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or the core activities of the data processors consist of the processing of sensitive categories of personal data. This is likely to create a conflict between the data controller and data processor that will need to carry out a data protection impact assessment to evaluate whether they fall into one of the above categories before deciding whether or not to designate or appoint a data protection officer. While at the same time, it is a data protection officer who carries out the data protection impact assessment" (Laibuta, 2020b).

Whereas the Act provides no obligation to employ or nominate an information protection officer, Section 24(6) requires that "a data controller or data processor shall issue the contact details of the information protection officer on the website and report them to the Data Commissioner who shall warrant that the same information is available on the official channel". Practically, this may require more clarity because once the information controller or processor assigns or designates an information security officer, they have legally enforcible duty to issue their contact points of interest and illuminate the Information Commissioner.

4 Challenges of the current data protection regime

Evidence from comparative jurisdictions on the implementation of the data protection regime indicate that the process has not been a smooth ride. Whereas contexts are different given that "how public and private institutions around the world engage with privacy is by and large the same" (Laibuta,

2020b), it presents opportunities for drawing some lessons on the kind of challenges data protection regime is likely to face. Thus, the current data protection regime in Kenya must strive to overcome the following challenges: First, the potential threats to personal or individual's data privacy. Security concerns have tended to take precedence in legislations on cybersecurity, public security, and national security. Aiming to curb unlawful online activities, Kenya enacted the Computer Misuse and Cybercrimes Act in 2018, a legislation that tends to essentially weaken online secrecy and, so, presents a genuine risk to information protection. The Act gives power to security apparatus to collect data for identifying criminal suspects. The law puts together restrictive provisions on collection and usage of information and states that the collected information ought to be "in line with important State rules" and should go through "strict approval procedures". Whereas the inability to control public security agencies' collection of individual information is probably intentional, it renders the government with free hand to develop and utilize surveillance technologies, which have proved to be effective administrative instruments in criminal examinations. The investigatory powers given to the security entities coupled with restrictive law and the need for pertinent important lawful control tends to create conventional citizens subject to government manipulation.

Second, a unified supervisory system is yet to be created. At the moment, the oversight role rests squarely on respective government agencies. For instance, the Communication Commission of Kenya (CCK) is tasked with data protection in the communication industry. The absence of a unified oversight body greatly impacts the implementation of data protection law. A unified oversight institutional framework would create even playing regulatory field so as to reduce discrepancies in the implementation of legal requirements. Given that data protection is not acknowledged in the existing supervisory bodies as part of their primary duty, they forego certain important works in data protection. For instance, even though the CCK bears the absolute obligation for data protection in the communication industry, its primary role is "development of the information and communications sector, (including broadcasting, multimedia, telecommunications, postal services), and electronic commerce" (Republic of Kenya, 2015).

Third, like other data protection authorities elsewhere, the Office of the Data Commissioner is likely to be financially constrained (Laibuta, 2020a).

Given the funding challenges in other government agencies, the Office of the Data Commissioner would likely follow similar pattern. This financial impediment limits the data protection authority's capability to tap into the pool of talented personnel. That pool includes data analysts, system administrators, lawyers, forensic analysts, among others.

Fourth, it remains to be seen how the Data Commissioner would handle complaints arising from data protection breaches caused by data processors and data controllers. As reported in Europe, data protection bodies have been under immense pressure for relenting in penalizing for breaches occasioned by officers tasked with processing and controlling data. Fifth, it would be difficult to regulate unregistered international data controllers and data processors and regulate cross-border data transfers (Laibuta, 2020a). It remains to be seen how the Office of the Data Commissioner would handle companies like Twitter, Facebook, Instagram, and Google. As recently reported, the Irish data oversight agency has been under scrutiny for reluctance in taking punitive measures against Facebook for apparent violation of EU GDPR (Lomas, 2021).

Sixth, there is likely to be a conflict between the Data Commissioner and the Cabinet Secretary as far as the formulation of regulations under the Act is concerned. Section 71 of the Act commissions "the Cabinet Secretary to make regulations primarily for enforcing the Act". In this Section, the Data Commisioner is not given powers to come up with regulative procedures. Finally, Section 9 of the Act entrusts "the Commissioner to arbitrate on disputes arising from the Act". It is guaranteed that parties will agree with the ruling of the Commissioner. The Commissioner may be overwhelmed by appeals made to the High Court. Without enough finances to procure the services of a competent lawyer, operation at the Data Commissioner's office may reach an abrupt end.

5 Conclusion

The promulgation of the Data Protection Act in 2019 places Kenya in the leagues of other countries that commenced their regulations thirty years ago. This article has examined two main determinants of the implementation of the Act. The primary determinant is from the execution of ICT policy noting that

changes in industry tend to raise the threat to personal security and thus, force real impediments on the law on information security. The second determinant is the established legal framework. Lack of assurance and the commitment to maintaining the primacy of security are the main features of the current information security administration. These two features indicate that the existing legislative foundation isn't conducive to accomplishing important assurance of an individual's rights to protection.

The above-mentioned obstacles in the implementation of data protection is not an indicator of a gloomy future to the law. Creating an enabling environment is a justifiable expectation because the Kenyan legal system has been more moderate and consultatory since the enactment of the Constitution in 2010. Kenya has now a progressive Bill of Rights in the region. Compared to the period before 2010, parliament is freer and has been considered a vital defender for rights assurance. The legal and legitimate calling have been created quickly as evidenced by the rising number of jurists and legal counselors, and their expertise. Such advancements have expanded the scope of justice system empowering citizens to seek legal redress whenever their rights are encroached upon. All these developments are indicative of a fundamental need for a workable information assurance law within the close future. In the future, the prospect of the information security law would hinge on the following: First, implementers and authorities ought to focus more on securing data rights of persons. The success to the victory of an information security legislation is to realize an adjusted advancement in public security and technological improvement, and personal privacy. Since the State and the industry play a significant role, it is fundamental to improve security environment. Future law should make more adaptable components to supply space that permits administrative assurance to advance productively by institutionalizing innovative rules. Given the open mindfulness within the long run, Kenya ought to continuously embrace bottom-up standards, emanating from open interaction between citizens, other private parties, courts, enforcement agencies, and assemblies. Consequently the implementation of data protection law would be subjected to consultative process. Second, policy implementers and enforcers should borrow best practices from comparative jurisdictions. The entry point would be to embrace foundational principles that define conceptual map of data protection as basis of conversation between Kenya and other external actors. Third, from the best

practices Kenyan enforcement agencies could proceed to tailor what works out well in the local context. Parliament and county assemblies must be more willing to explore data protection rules. Fourth, for enforceability, a centralized agency should be established to oversight data protection. A key reform measure to enhance government oversight is to allow at least one national agency to have data protection as its main mandate. What is more, comprehensive regulatory procedures should be place to enforce statutory requirements.

References

Abdulrauf, L.A & Fombad, C.M. (2016). The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?, *Journal of Media Law*, 8 (1): 67-97.

Breckenridge, K. (2019). The failure of the 'single source of truth about Kenyans': The NDRS, collateral mysteries and the Safaricom monopoly. *African Studies* 78 (1): 91-111.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection." *Information & Communications Technology Law* 26, no. 3 (2017): 213-228.

Cooter, R. (1997). Market modernization of law: Economic development through decentralized Law. In J.S. Bhandari & A.O. Sykes (Eds.), *Economic dimensions in international law: Comparative and empirical Perspectives (pp.275-314),* Cambridge University Press, Cambridge.

Crawford, K & Schultz, J (2014). Big data and due process: Toward a framework to redress predictive privacy harms *Boston College Law Review* 93: 99–110.

Graham G. (2012). China's internet data privacy regulations 2012: 80% of a great leap forward? *Privacy Laws & Business International Report* 1: 1–5.

Greenleaf, G. (2017). *Graham Greenleaf, Asian Data Privacy Laws: Trade and Human RightsPerspectives*, Oxford University Press, Oxford.

Jyh-An, L & Liu, C. (2016). Real-name registration rules and the fading digital anonymity in China *Washington International Law Journal* 1: 1–34.

Kivikuru, U. (2017). Ideals, buzzwords and true trying: ICT and communication policies in Kenya. *Journal of African Media Studies* 9 (2): 307-321.

Kivikuru, U. (2019) From community to assemblage? ICT provides a site for inclusion and exclusion in the global south, *The Journal of International Communication*, 25:1, 49-68.

Li, H., Yu, L & He, W. (2019). The impact of GDPR on global technology development, *Journal of Global Information Technology Management*, 22: 1-6.

Lomas, N. (2021), Ireland's draft GDPR decision against Facebook branded a joke https://techcrunch.com/2021/10/13/irelands- draft-gdpr-decision-against-facebook-branded-a-joke/ (accessed 24 October 2021).

Parasol, M. (2018). The Impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and smart city dreams. *Computer Law & Security Review*, 34(1):67-98.

Ministry of Information, Communications and Technology (2006). *National Information and Communications Technology (ICT) Policy (2006)*, http://www.ist-africa.org/home/files/ Kenya ICT Policy 2006.pdf (Accessed18 March2020).

Ministry of Information, Communications and Technology (2013). *Ministerial Strategic Plan (2013–17)*, www.ict.go.ke/wp-content/uploads/2016/04/ MinistryStrategic.pdf (Accessed 18 March 2020).

Ministry of Information, Communications and Technology (2014a). *The Kenya National ICT Masterplan (2014-2018).*

Ministry of Information, Communications and Technology (2014b). *Ministry of Information, Communication and Technology, 2014. Cybersecurity Strategy.*

Laibuta, M. (2020a). "What awaits the data protection commissioner", https://www.laibuta.com/data-protection/what-awaits-the-data-protection commissioner/(Accessed 21 October 2020).

Laibuta, M. (2020b). Two years on: The impact the GDPR has had on privacy and data protection in Kenya" https://www.laibuta.com/data-protection/two-years-on-the-impact-the-gdpr-has-had-on-privacy-and-data-protection-in-kenya/ (accessed on 19 October 2020).

Laibuta, M. (2020c) "The Business Case for Data Protection", https://www.laibuta.com/data-protection/the-business-case-for-data-protection/(Accessed on 19 October 2020).

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review 1703, 1703–1706.

Republic of Kenya (2003). Economic *recovery strategy for wealth and employment creation, 2003-2007,* Ministry of Planning and National Development.

Republic of Kenya (2004). *E-Government Strategy: The Strategic Framework, Administrative Structure, Training Requirements and Standardization Framework*, Cabinet Office: Office of the President.

Republic of Kenya (2008). *Kenya Vision 2030*, A Vision for a competitive and prosperous Kenya http://thereddesk.org/sites/default/files/vision_2030_brochure_july_2007.pdf. (Accessed 19 March 2020).

Republic of Kenya (2010). *Constitution of Kenya, 2010*, Nairobi: Government Printer.

Republic of Kenya (2015). *Kenya Information and Communication Act*, Nairobi: Government Printer.

Republic of Kenya (2016), *Access to Information Act*.Nairobi: Government Printer.

Republic of Kenya (2018a), *The Computer Misuse and Cybercrimes Act*. Nairobi. Government Printer.

Republic of Kenya (2018b), *The Statute Law (Miscellaneous Amendments))*. Nairobi. Government Printer.

Republic of Kenya (2019). Data Protection Act. Nairobi. Government Printer.

Thiel, A. (2020). Biometric identification technologies and the Ghanaian 'data revolution'." *The Journal of Modern African Studies* 58 (1): 115-136.