Seven Years in the Making: The Kenya Data Protection Act, 2019

On November 8, 2019, the Kenyan president, Uhuru Kenyatta, signed into law the Data Protection Bill, 2019, seven years after the publication of the first draft bill in 2012. This brief presents a review of Kenya's journey and efforts to develop a data protection law. It also provides an overview of the implication of the new law to the protection of privacy and improved data governance in the East African country.

Brief History

Efforts to have in place a privacy and data protection framework in Kenya commenced with the introduction of the right to privacy under Article 31 of the Constitution of Kenya, 2010. The provision guarantees the right to privacy of every person, including their communications, property, homes and family life .

In 2012, the first Data Protection Bill was published, only to lapse due to inaction. The bill was republished in 2013 but it was also not progressed.[1] The inaction by Parliament on the Bill continued until May 2018, when the Senate published a fresh private member's bill, the Data Protection Bill, 2018.[2] During the same month, the Ministry of Information, Communications and Technology constituted a taskforce to develop a Data Protection Policy[3] and a Data Protection Bill[4] (different from the private member's bill) and these were opened to the public for comments.

The two bills had shortcomings and there was confusion especially in the mode of their separate development. However, they were welcomed by stakeholders as a positive step towards better understanding of, and realisation of the right to privacy in Kenya, especially coming at a time when there were widespread concerns around privacy in the country. Such concerns included the fragmented oversight over privacy and data protection; the increased mass data collection programmes by the government; enhanced state surveillance capacity of the government; rampant privacy breaches by business entities; limited dispute resolution mechanisms and absence of remedies in case of breach of privacy.[5]

Stakeholders were subsequently provided opportunities to provide input into the development of the two Bills, which, after several consultations with the Senate, were consolidated into the Data Protection Bill, 2019.[6] On November 8, 2019, the Bill was signed into law by the President.[7]

Implications of the Data Protection Act, 2019

One of the key concerns prior to the enactment of the law was the weak regulatory frameworks for the enforcement of privacy rights in the country. The new law addresses this issue as it provides a comprehensive framework to regulate the processing of personal data and the protection of the privacy of individuals in Kenya. It also consolidates the law on privacy in the country, and more importantly, articulates several principles of personal data protection under section 25, as the minimum standard which all data controllers or processors are required to abide by. These principles include lawfulness, transparency, fairness, legitimate purpose, data minimisation, accuracy, transparency, anonymisation, confidentiality and consent.

Further, the Act provides for autonomy of the data subject over their data. Hence, it defines what constitutes consent, and makes the requirement of consent mandatory. This potentially addresses situations where personal data is collected arbitrarily and without the explicit consent of users. The law also prohibits the use of personal data for commercial purposes without the consent of the data subject. It also places the burden of proof for establishing a data subject's consent on the data controller or processor, while allowing the subject to withdraw consent at any time. Data controllers and processors will therefore have to modify their agreements, contracts and practices to ensure that they seek prior informed consent, and obtain it explicitly.

1 *Data Protection Bill 2013, http://icta.go.ke/data-protection-bill-2012/*
2 *Senate Data Protection Bill, 2018, http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf*
3 *Draft Data Protection Policy, http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf*
4 *Draft Data Protection Bill, 2018, http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf*
5 *CIPESA, State of Internet Freedom in Africa 2018, https://cipesa.org/?wpfb_dl=278*
6 *Data Protection Bill, 2019, http://www.parliament.go.ke/sites/default/files/2019-07/The%20Data%20Protection%20Bill%2C%202019.pdf*
7 *Uhuru signs Data Protection Bill into law, https://www.businessdailyafrica.com/releases/Uhuru-signs-Data-Protection-Bill-into-law/1941082-5341658-njto1jz/index.html*

The other important development is that this law, in its Second Schedule, amends other legislation that have an impact on privacy and requires that the principles under the new Act are observed in the management of personal data. The affected laws that it amends include the Births and Deaths Act, Capital Markets Act, Independent Electoral and Boundaries Commission Act, Kenya National Examinations Council Act, Employment Act, 2007, Kenya Citizenship and Immigration Act, 2011, Basic Education Act, 2013, Universities Act, 2012, Central Depositories Act, 2000, Anti-Money Laundering and Proceeds of Crime Act, Kenya Information and Communications Act, and the Insolvency Act, 2015.

This requirement to observe the principles under the Act is, among others, addressed to the various data collection programmes by government. It will therefore require that the relevant institutions responsible for the handling of the registration of individuals at birth and death, issuance of national identity cards and passports, Huduma Namba registration, registration of students at all levels, and the registration of telecommunication services consumers, review their current policies, practices and procedures to ensure compliance with the principles set forth in the Act.

The lack of an oversight body and the fragmented oversight over privacy in the country meant that every institution collecting personal data "owned" and used such data as they wished. The law addresses this challenge by establishing an independent office of the Data Protection Commissioner. Its key functions include having an oversight over the implementation of the Act; registration of data controllers and processors; promotion of self-regulation; conduct of assessments of public and private bodies; receipt and investigation of complaints; civic awareness; inspection of public entities, among others.

In the conduct of its functions, the office of the Data Protection Commissioner shall have power to conduct investigations; facilitate dispute resolution; issue summons to witnesses; impose administrative fines; and, provide assistance to the public. The Data Commissioner is also empowered to carry out periodic audits of data controllers or processors.

Prior to the enactment of the law, many aggrieved persons lacked adequate dispute resolution mechanisms and remedies in case of breaches. Under this law, the Data Protection Commissioner is empowered to receive and investigate complaints and issue enforcement notices. The requirement for mandatory disclosure of data breaches is a big plus too. Under the Act, penalties for non-compliance are up to five million Kenya shillings (USD 49,085) or 1% of the annual turnover of a company. Aggrieved persons can also proceed to seek compensation from the data controller or processor for damages, which include for both financial and non-financial losses. However, it provides an exemption to data controllers or processors from complying with its provisions where it is necessary for national security or public interest, or where disclosure is required under the law or by a court order. Hence, victims of data breaches in instances termed "national security" or "public interest" may have no remedy.

Implementation

Whereas the Act spells out several important and positive features, its implementation remains key. Passing of the Act's regulations and establishment of the Office of the Data Protection Commissioner are a priority for action to ensure swift implementation of the law. Further, all data controllers and processors will need to take critical action-oriented steps to ensure compliance with the Act. This will include mapping data they hold, enhancing the security of the data, and reviewing their policies, procedures and processes of handling personal data; and, as relevant, designating Data Protection Officers. This could also create an opportunity for innovation and employment opportunities.

Notably, capacity building of data controllers and processors is critical to ensure that the principles set out in the Act are widely understood and adhered to. Greater awareness of the public of their privacy rights will also be crucial. Civil society, and the communications regulator, can play a key role in this.

Conclusion

While there may be concerns about the law, its passing creates an opportunity for all stakeholders to assess and recognise the value of assuring the privacy of the data that they hold; and ensure transparency and accountability for the storage, processing and use of personal data. As such, the new law can go a long way in addressing the live issues in protecting the privacy of data in Kenya.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda
Tel: +256 414 289 502,+256 772 406 241
www.cipesa.org