DATA PROTECTION IN EAST AFRICA

By Victoria Nyawira Gitau and Louisa Ochilo

DATA PROTECTION

Data protection aims at greatly safeguarding the right to privacy and this is a matter that is of utmost importance in the current digital age. This is especially important as the global economy is a digital economy and hence it is heavily reliant on digitization in order to leverage its economic success. The right to privacy lies squarely at the centre of data protection and, therefore, a proper understanding and safeguarding of data protection in the digital age may be fulfilled only by properly understanding the right to privacy. Privacy is a term that has over the years taken on different meanings. Privacy in today's technological age is much different from the privacy envisioned by our forefathers, which undoubtedly affects the direction in which data protection is legislated and enforced nationally, regionally and internationally. This paper aims at providing a good comprehension, contrasts and comparisons of the enforcement of data protection in the East African Community (EAC) vis-à-vis in the European Union (EU) by analysing the community law in both areas. This paper will also make reference to some indicative practices in Kenya, the most progressive state in the EAC regarding all data protection matters.

Traditional concepts of privacy

In the 19th Century Samuel Warren and Louis Brandeis popularized the idea of privacy as the right to be let alone.[1] This meant that a person could carry out the state of his/her affairs without undue interference from the State and from other persons. However, this idea soon lost credibility as more and more circumstances arose where the State's interference was more than necessary. For instance, when paying taxes, persons were required to disclose information about their affairs when doing so. [2] This right soon evolved to perceive invasion as a violation of privacy. This now meant

[1]Warren S & Brandeis L, *'The right to privacy'*, 4 Harvard Law Review, 1890, 193.
[2] Muema Alan, '*The centralization of population registers in Kenya: A threat to the right to privacy in Kenya*' unpublished Dissertation, Strathmore University Law School, Nairobi, 14.

that while there were necessary intrusions, particular wrong doers' acts could be seen as an invasion of privacy. Nevertheless, this approach lacked a threshold to identify when the invasion amounted to injury. Later, the author June Inness posited that privacy is intimacy. ALL intimate information was private. However, some information such as your passport number was not regarded as intimate but was private information.[3] Later on, privacy was likened to secrecy: if one had nothing to hide then there was no need for privacy. However, this idea is problematic as it assumes only illegal activities are kept private.[4]

In the African context, things are slightly different. Privacy is often viewed as a private right and is closely associated with individuality and self-autonomy. In the African setting, life in itself is communal. In the African society, the general collective of the different and diverse African communities believe in the philosophy of *ubuntu* which loosely translates to 'I am because we are'. This means that an individual's life is related to the whole group. Social cohesion was both a priority and a good to be aspired to in the community and it was seen in the daily practices. Land was owned communally and each person had a role they played in tending to the communal land.[5] When a woman got married in the traditional African context she was married to an individual and married to the entire family and community as well. Any children coming from the union belonged not only to the family but also to the entire clan. As time passed, different factors such as colonisation, religion and capitalism changed this view into privacy as an individual right.

Privacy in the digital age

After colonisation, most constitutions had a legislative commitment made to safeguard the right to privacy. This, however, represented the views of their colonial masters rather than their own. Subsequently, at the time of independence, most conditions in Africa mirrored those of the states that colonised the Continent; in the 80's, the African charter on Human and People's Rights, which was under the then Organization of African Unity, did not have a privacy clause. This is because

[3] Inness J, *Privacy, intimacy and isolation*, Oxford University Press, Oxford, 1992, 56.
[4] Solove D, *'I've got nothing to hide' and other misunderstandings of privacy'* 44 San Diego Law Review, 2007, 745-772, 747
[5] Alex B. Makulilo '*A Person Is a Person through Other Persons"—A Critical Analysis of Privacy and Culture in Africa'* , Beijing law review ,2016,194

the African understanding of privacy was much different and was yet to evolve into the idea of privacy accepted today.

When the HIV/AIDS pandemic swept across the Continent, more and more people began to recognize the need for the right to privacy. The disclosure of one's HIV test results to third parties without such person's consent often led to stigmatization and discrimination. For example, if co-workers were notified of the medical status of one of the other employees, this usually led to someone losing his/her job especially if the person involved was positive. This is because of the stigma and misconceptions associated with HIV/AIDS in the past. In order to protect people, governments and law making bodies began to include clauses in their laws that made medical results private.

Furthermore, many African countries, Kenya included, are continually trying to upgrade their national identification systems to include the use of biometrics. There is a need to set up laws to protect data that will be contained in these databases. Nonetheless, many African countries have set up laws that are privacy unfriendly. For example, there are Internet censorship and surveillance laws in many countries like Ethiopia and Uganda. In addition, Tanzania's Prevention of Terrorism Regulations adopts certain measures to ensure national security that are largely inconsistent and disproportional to the right to privacy and its protection.[6] Some countries do not have any laws pertaining to data protection at all. In this legislative void, countries worldwide are violating their citizens' privacy through activities ranging from conducting extensive surveillance without a legal basis and actively censoring the Internet for the failure to protect the privacy of personal data and digital communications.[7]

Regional Data Protection Framework

African Union

The AU in 2014 adopted the African Union Convention on Cyber Security and Personal Data Protection also known as The Malabo Protocol. Prior to this, data protection had not been captured

[6] http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf accessed on 18 November 2020.
[7] http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf accessed on 17 November 2020.

in the legislations and guidelines of the African Union. This is a new document and it faces many challenges such as no confidence from countries that are party to the AU. Out of the six East African Countries (Kenya, Uganda, Tanzania, Rwanda, Burundi and South Sudan) [*PLEASE CONSIDER WHETHER TO MENTION THE STATES IN ALPHABETICAL ORDER]*, only Rwanda has ratified it in 2019[8].

The African Commission, which is the body of the AU tasked with Human Rights, wrote in 2019 a draft declaration titled 'Declaration of Principles on Freedom of Expression and Access to Information in Africa'. This is still a draft and is yet to be implemented.

Common Market for Eastern and Southern Africa (COMESA)

This is a free trade area that spans over 21 countries within Eastern and Southern Africa.[9] Privacy in this context relates to trade. Article 25(1) of the European Union's Directive on the Protection of the Individuals with regard to the Processing of Personal Data and the Free Movement of such data (Directive 95/46/EC) specified that EU member states must prohibit the transfer of personal data to non-member states that cannot guarantee an adequate level of data protection.[10] These kind of incentives trigger a response and lead to consumer protection laws within COMESA that protect the right to privacy in trading activities.

Southern African Development Communities (SADC)

Although this is a Southern African regional body, it has Tanzania, one of the East African countries, as a member. In 2013, the Southern African Development Community (SADC) published a Model Data Protection Act.[11] However, this is more of a guideline on how to enact privacy and data protection laws within member parties' jurisdictions.

[8] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf accessed on 17 November 2020.
[9] https://www.tralac.org/resources/by-region/comesa.html accessed on 19 November 2020.
[10] http://www.hrforumzim.org/wp-content/uploads/2014/06/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf accessed on 19 November 2020.
[11] https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2 accessed on 16 November 2020.

East African Community

The East African Community consists of the six different member states that make up East Africa. It has a draft document on EAC Legal Framework for Cyber Laws that was published in November 2008.[12]

Overview Regional Bodies framework on data protection

Regional organisations have made efforts towards ensuring the right to privacy through data protection; nevertheless, the overall legislative framework is not harmonised. It is however possible to find some common ground on the legislation.

For example, most countries require consent to the access of data as a necessary condition for data processing. On a legal basis, there are no references made to the idea of a legitimate interest as a condition for data processing. Additionally, most statutes have provided for the establishment of a data protection authority reporting to the telecommunications or ICT regulator.

Furthermore, there are similar features when data controllers are obliged to notify the regulator of any data processing activities and to seek from the regulator an authorisation to transfer personal data to third countries [13]

A Taxonomy of Privacy

Professor Solove in 'Taxonomy of Privacy' conceptualized the idea of privacy being a group of different elements that must be fulfilled in order to ensure that there is no violation. In the taxonomy of privacy, there are certain harms and problems that amount to infringement of the right to privacy. Therefore, in order for data protection laws to fully protect the right to privacy, all the taxonomy must be followed and all possible infringements must be covered.[14]

1. Information Collection- there are certain problems expected to arise when information is gathered from people. These are surveillance and interrogation.

[12] http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq accessed on 17 November 2020.
[13] https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2 accessed on 16 November 2020.
[14] Solove D., '*A taxonomy of privacy'*, 3 University of Pennsylvania Law Review 154, 2006, 477- 560, 502.

2. Information Processing- this is the manner in which collected data is handled. The possible arising problems are aggregation, identification, insecurity, secondary use and exclusion.
3. Information Dissemination encompasses the ways in which information is transferred, the possible problems include: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion.
4. Invasion encompasses the direct interferences with the individual and included the following problems intrusion, and decisional interference.[15]

This taxonomy may be used to develop legislation, to make policies and to take executive decisions and judgments that can be said to truly uphold, protect and promote this right.

The implementation of data protection in Kenya

Within the EAC, there is a general lack of urgency when it comes to legislating on the right to privacy in the digital age. The only country that has taken some meaningful steps is Kenya, aside from the law enacted by EAC, Kenya has introduced some provisions in the Constitution as well as in the Acts of Parliament. As posited by a Kenyan scholar:

'*The importance of the right to protection of personal data has been recognized in the international sphere, but the government of Kenya has been slow in ensuring the protection of personal data of all of its citizens. Currently, the* ***national laws of general applicability regulating the collection and use of personal data in Kenya are the Constitution of Kenya 2010, the Access to Information Act of 2016 and the Consumer Protection Act 46 of 2012, and most recently, the 2019 Data Protection Act.*** *These laws have proved to be inadequate for the protection of personal data of citizens which is collected and processed by the Government in the provision of services and the execution of its functions. This inadequacy is perhaps best illustrated by the breach of the right to protection of personal data that was collected in the 2017 national elections. As the Centre for Intellectual Property and ICT Law observed in their report, Investigating Privacy Implications of*

[15] Muema Alan, '*The centralization of population registers in Kenya: A threat to the right to privacy in Kenya'* unpublished Dissertation, Strathmore University Law School, Nairobi, 20.

Biometric Voter Registration in Kenya's 2017 Election Process, it is the absence of a robust framework to protect the biometric data in the voter register and the deficiencies in data protection law that inevitably led to violations of Kenyan citizens' privacy and the monetization of their data when it was allegedly sold to political candidates in the elections.'[16]

While the Data Protection Act has the essence of the GDPR (the EU General Data Protection Regulation) in stating the principles of data protection and the rights of data subjects against the actions of the processors and collectors, in section 25 and 26 respectively, as observed by Muema above, it falls short in having efficient mechanisms for their enforcement in spite of making an attempt to catch up with the international standards.

European Legislation on Data Protection

Effective from the 25th of May 2018, the European Union (EU) ratified the General Data Protection Regulation (GDPR), the leading legislation in the EU mandated with protecting the right to privacy in the digital age. The GDPR is an extensive regulation that forms part of the community law in the EU and therefore legally binds the state parties of the EU to comply with it. It is regarded as an authority in data protection as it has a wide substantive scope, hence meeting the unaddressed legal lacunae in the EU that were present before its inception. Prior to this, the 1995 Data Protection Directive was adopted and while it was a good stride for the community in the protection of the right, it was outdated as the technological advancements overtook its competence, bringing about the said unaddressed gaps. [17]

The substantive provisions of the GDPR

The general provisions

Some of the novelty of the GDPR emanates from the fact that it is cognizant of the tripartite relationship that can occur during data protection. In its definition of terms, it recognizes the existence of the data subject, the data collector (the main entity which collects the data for a

[16] Muema Alan, '*The centralization of population registers in Kenya: A threat to the right to privacy in Kenya'* unpublished Dissertation, Strathmore University Law School, Nairobi, 18.
[17] https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

purpose) and the data processor (the agent of the collector that processes and stores the data).[18] It binds the tripartite relationship by granting guiding principles that confine the process of data collection and processing.

The guiding principles of the GDPR are enumerated in Article 5 and elaborate the manner in which data collection should be done. The first principle is that personal data shall be processed in a manner that is lawful, fair and transparent to the data subject.[19]

The second principle is that there shall be a limitation to the data collection concerning the purpose. Therefore, the data shall be collected for specific, explicit and legitimate purpose(s) and shall not be processed further outside the scope of the purpose that was communicated to the data subject.[20] The principle of a purpose limitation protects the privacy of the data subjects as it aims to ensure that their personal data is not overly exploited.

The third guiding principle present in the GDPR is the data minimization principle. It states that the data collected should be adequate, relevant and limited to what is necessary in relation to the purpose for which the data is processed.[21] For instance, if the collector is targeting the biometric data of a specific group of data subjects, then he/she should limit him/herself to only collecting that data and should not extend the scope to collecting health data. This is a measure that attempts to reduce the risk of unduly limiting or breaching the right to privacy of the data subject.

The fourth principle is that of accuracy, which guides that the data collected should be accurate and, where possible, it should be kept up to date. Where the data is inaccurate and the inaccuracy is material to the purpose for which it is being collected, it should be erased.[22] The fifth principle suggests that the data should not be stored for longer than is necessary for the objectives of processing the data.[23] As a general rule, it is the responsibility of the controller to comply with the principles of data protection.

[18] Article 4), the General Data Protection Regulation, 2018.
[19] Article 5(1) (a), the General Data Protection Regulation, 2018.
[20] Article 5(1) (b), the General Data Protection Regulation, 2018.
[21] Article 5(1) (c), the General Data Protection Regulation, 2018.
[22] Article 5(1) (d), the General Data Protection Regulation, 2018.
[23] Article 5(1) (e), the General Data Protection Regulation, 2018.

Over and above the general principles, Article 24 states that the data controller has the primary responsibility regarding implementing the appropriate technical and organisational measures to ensure that the data collection is done according to the principles of the GDPR.[24]

The enforcement mechanisms of the GDPR

Article 51 of the GDPR gives further details on the supervisory authorities which are mandated with the enforcement of the GDPR. It details that each member state is to appoint one or more independent public bodies with the mandate of monitoring the application of the GDPR on a state level. On the regional level, the communities are meant to coordinate and cooperate so as to ensure that they are all applying the GDPR uniformly across the board and shall come up with a consistency mechanism that guides their state-level enforcement.[25]

Furthermore, each member state is obliged to notify the Commission with the provision of its laws adopted pursuant to data protection by the date of the enforcement of the GDPR and any subsequent amendment affecting them. [26]

Each supervisory authority shall have investigative powers that empowers it to carry out the following:

(I) To order the controller and processor or their representatives to provide any information necessary for them to perform their tasks

(II) To carry out investigations in the form of data protection audits

(III) To carry out a review on certifications issued

(IV) To notify the controller or processor of an alleged infringement of the GDPR

(V) To obtain access to any premises of the controller and processor, including data processing equipment and means in accordance with union or member state procedural law

Furthermore, the supervisory authorities have several corrective powers:[27]

[24] Article 5(2), the General Data Protection Regulation, 2018.
[25] Article 63, the General Data Protection Regulation, 2018.
[26] Article 51, the General Data Protection Regulation, 2018.
[27] Article 58, the General Data Protection Regulation, 2018.

(I) to issue warnings to a controller or processor when their intended processing operations are likely to infringe provisions of the Regulation;

(II) to issue reprimands to a controller or a processor where processing operations have infringed provisions of the Regulation;

(III) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the Regulation;

(IV) to order the controller or processor to bring processing operations into compliance with the provisions of the Regulation, where appropriate, in a specified manner and within a specified period;

(V) to order the controller to communicate a personal data breach to the data subject;

(VI) to impose a temporary or definitive limitation including a ban on processing;

(VII) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 of the Regulation;

(VIII) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 of the Regulation, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(IX) to impose an administrative fine pursuant to Article 83 of the Regulation, in addition to, or instead of measures referred to in another paragraph, depending on the circumstances of each individual case; and

(X) to order the suspension of data flows to a recipient in a third country or to an international organization.

The supervisory authorities also have a few advisory powers that further empower them in their mandate.

GDPR Jurisprudence

Various commercial entities have been fined and held liable for breaches of the right to privacy through the violation of the GDPR. Some recent examples are as follows. First, in 2019, Google was charged with a €50 million fine which has been the heftiest fine this far. Google was fined by the supervisory body of the French National Commission on Informatics and Liberty for the illegal obtainment and processing of personal data, considering that the personal data was obtained without free, prior informed consent and was later used for targeted advertising. [28]

The Hamburg Commissioner for Data protection and Freedom of Information fined fast fashion retailer H&M for the violation of the GDPR. A technical error occurred which made available the information that the company had been harvesting, including sensitive personal data, from its employees and storing it without consent. This resulted in a €35.3 million fine for the breach. [29]

Similarly, Italian telecommunications operator TIM was fined €27.8 million for a long list of breaches which include targeting and contacting customers through targeted advertising, without informing them of the improper management of consent lists, excessive data retention, data breaches, violation of the principles of data processing and more.[30]

Evidently, the supervisory authorities in the EU are able to efficiently enforce the GDPR in practice by holding accountable any data processors and controllers who breach the principles of data collection.

[28] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
[29] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ accessed on 20 November 2020.
[30] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ accessed on 20 November 2020.