ISSN No:-2456-2165

Data Protection from Policy to Practice

Dr. Fernando Wangila, Ph.D.,CDP

Abstract:- Currently, most services and operations are connected to the internet, and these raises concerns about the security of the client data. Each time the client requires a service, there is some information to be filled through the online platforms, and this can either be appropriately used or abused. Some countries have different data protection laws, while others lack them. For instance, according to the US, different data requires different protection guidelines. The guidelines determine the pieces of information that can be revealed to the general public and the one that can only be disclosed to a specific population for specific use. In the quest to meet these regulations, there is a need to come up with a legal code that elaborates on a comprehensive data protection policy. The current paper further conveys the importance of comprehensive codes in the issue of data protection in minimizing data theft and unauthorized access. Markedly, these rules and regulations are the basis of success in the Information Technology in the modern environment.

I. INTRODUCTION

The modern environment is defined by advanced computer technology. The overreliance on technology in different operations takes the criminals a notch higher as they use the internet to engage in different forms of cybercrimes. Unlike in the past, where crime was limited to the physical actions of the criminals, in the current situations, the crimes are limitless as the criminals can engage in them from the comfort of their homes. An example of high-tech cybercrime is the US government data theft from the highly secured pentagon by the Chinese Hackers (De Hert & Papakonstantinou, 2016). Such a situation leads to constant questions on the safety of ordinary individuals with regards to their online operations. Apart from data theft crime, cybercriminals may embark on the deviation of different sites to unauthorized pieces of information for malicious gains (Norris, 2018). Several inconveniences result from the unauthorized access and tampering with official data in different organizations and institutions. In some cases, the hackers go as far as deleting the pieces of information, and this affects their general operation. In the quest to protect these pieces of information, there is a need for robust cyber laws and efficient cyber forces to work and appropriately enforce these laws for compliance.

II. THE NEED FOR DATA PROTECTION POLICY

Globalization has improved the operation of different countries as they deal with both local and international clients. The trend is made possible through the advancement of the IT sector. Markedly, companies access different types of sensitive information (Norris, 2018). For instance, during some transactions, the clients require to make online payments, and this makes it mandatory for them to provide their financial and credit card details. These pieces of information are kept in the electronic platforms, and as such, they are handled by the respective employees. Given the sensitive nature of the information, it remains vulnerable in the hands of the workers that access it. Even though there have been privacy directives, they are directed towards personal Data. The element of personal data has not been succinctly defined to cater for all the needs of the clients whose data is at risk of being misused (De Hert & Papakonstantinou, 2016). Given the modern trends in the Information Technology (IT) sector, there are concerns about the element of data privacy.

Data protection bills are directed to the governments, data collection enterprises, and data controllers. These parties directly deal with different pieces of information, and as such, there is a need to offer guidelines to ensure that they protect all these pieces of information (Norris, 2018). Some of these parties have unlimited access to data, and hence they are capable of misusing it. Based on the data protection bills, these parties have the responsibility of securing sensitive information. In cases where the criminals get access and alter the information in question, penal sanctions are imposed on them (Dimitrova & Brkan, 2018). They are forced to cater to the damages caused by the individuals in question. Besides, information technology Acts are crucial in the constitution as they define the access that different individuals have with regards to the stored data.

The handling of data is divided into different stages, and this means that several individuals have access to it. It is crucial to enhance data protection in all stages of data collection, use, and disclosure. In cases where the privacy of individuals is compromised, then his/her data may fall into the wrong hands, and in the end, this result in cyber-crimes like cyberbullying (De Hert & Papakonstantinou, 2016). Markedly, this is a complex right that is related to one's fundamental rights like that of life.

III. KENYA DATA PROTECTION LAWS

In 2012, the Kenyan government, through the Commission for the Implementation of the Constitution (CIC), presented a revised version of the Data Protection Bill. Besides this bill, Kenya belongs to the East African Community, which required the members to come up with protection laws founded on international standards. Kenya adopted the 2010 constitution, which includes the element of privacy (Makulilo & Boshe, 2016). The draft Bill indicates that its requirements are in line with international standards.

The draft Bill categorizes information into sensitive and non-sensitive ones. For instance, in health facilities issues related to HIV testing and results, the medical practitioner has the responsibility of keeping the information confidential. Besides, the patient's consent has to be sought before carrying out the test. Failure to observe these requirements risks a fine of Ksh.100 000 or imprisonment for two years or both.

The Kenyan constitution incorporates the right to privacy. The legislation was inexistent until the introduction of the Data Protection Act in 2019. After the enactment, the Kenyans were assured of the enjoyment of the right in both online and offline basis (Makulilo & Boshe, 2016). Kenya has various statutes about data protection, but its implementation is not sufficient to meet the needs of the Kenyans.

Back in 2019, Kenya set the standard for the rest of the African continent with regards to the data protection laws. The president approved the data protection legislation that was in line with the European Union's General Data Protection Regulation. In this case, the legislation highlighted the processes to be followed during the handling, storage, and sharing of personal information. Given the high level of online innovation like the Kenyan Safaricom innovative online money transfer M-Pesa services, this regulation comes in handy in protecting the citizens using such services. The regulation is attached with harsh penalties for the defaulters as the guilty parties' risk paying a fine of $29,283 or two years in jail or both (Banisar, 2019). The move places Kenya among the other African countries that recognize the need for data protection laws and regulations. Some African countries like Burundi lack the protection regulations, and as a result, the citizens lack where to run to in case their rights are violated (Makulilo & Boshe, 2016). Markedly, the Kenyan progress on the data protection issue is impressive, and hence the welfare of the citizens is taken into consideration.

Kenya protection law borrows various elements from GDPR. For instance, like GDPR, the Kenyan protection law offers guidelines on the collection, sharing, and storage of consumer information. The law applies to both the technology and the hospitality industries. Currently, there is the misuse of consumer data by different corporations as they seek to establish the creditworthiness of the Kenyans (Banisar, 2019). The Kenyan restrictions protect the citizens from engaging in their exploitative practices in connection to these pieces of information.

Additionally, the Kenya Data Protection Act highlights similar principles as those of GDPR. For instance, the data processors and controllers are required to respect the citizens' right to privacy. Besides, the purpose for which they use or collect information is limited. In this case, the purpose should be legitimate, specified, and explicit. Also, the principle of data minimization applies in Kenya. Here, the data collected should be relevant, limited, and adequate. Moreover, there is a scrutiny of the different types of data to ensure the safety of the Kenyans. In this case, the element of consent during transfers is mandatory. Thus, there are no transfers beyond Kenya without the authorized safeguards (Banisar, 2019). These are the underlying principles behind the Kenya Data protection act, and they are in line with the EU GDPR requirements.

IV. U.S.A DATA PROTECTION LAWS, POLICIES AND THEIR APPLICATION

The U.S.A has established complex laws about data protection policies. Here, data is divided into different categories based on its sensitivity and utility. Different guidelines are set for each of these categories. Since the 20th century, different acts have been passed regarding privacy in the US. For instance, in 1974, a privacy act with regards to collection, application, and disclosure of different types of information was passed. In this case, the consent of the owner of the information in question was to be sought before applying the information in any circumstance (De Hert & Papakonstantinou, 2016). Additionally, in 1986, the US government passed the Electronic Communications Privacy Act. In this case, any unlawful access, application, and disclosure of information in the electronics were prohibited, and in case it occurred, it was punishable by law. The law catered for all types of electronic communications and intelligence (Dimitrova & Brkan, 2018). It advocated for fair and authorized use of these pieces of information.

Moreover, the minors were not left aside as the government introduced the Children's Online Privacy Protection Act. No doubt, children are vulnerable, and information about them can be used for selfish gains. Given this, the government came up with regulations to protect them in the online environment. Here, the web owners were to collect information in good faith and not for malicious purposes. The act required that the consent of the parents would be sought during the collection, use, and disclosure of the minors' information (De Hert & Papakonstantinou, 2016). Equally, different procedures were laid aside to guide the web owners on the application and disclosure of the information collected from the minors.

The protection law incorporated the welfare of the consumers. The Consumer Internet Privacy Act was passed in 1986 (De Hert & Papakonstantinou, 2016). Considering the increase in online services, the service providers require the consumers to subscribe to their sites, and in the process,

they offer their private information. Given their vulnerable state, the service providers may take advantage of the information and use it for their malicious gains. Thus, the act requires that any use or disclosure of the consumer information should be after the written consent of the subscriber (Dimitrova & Brkan, 2018). The Federal Trade Commission takes part in the enforcement of this requirement as it engages in the investigation of different types of computer services to establish that the providers do not engage in illegal actions, as stated by this particular act.

Logically, the creation of data protection laws, policies, and bills alone are not enough to curb the constant trends of data insecurity. The government should take it as its core responsibility to protect the vulnerable parties from the damages caused by the unauthorized access of sensitive information. Strict and harsh penalties should be directed to the defaulters of these requirements (De Hert & Papakonstantinou, 2016). Besides, the cybercriminals should not be left with the opportunity to compare both the benefits and losses that result from the misuse of different pieces of information. The costs and penalties should outweigh their expected malicious gains from the respective cybercrimes. In the end, both the users and data collectors will be assured of their safety (Dimitrova & Brkan, 2018). Markedly, the application and enforcement of these laws matter in the enhancement of security of the vulnerable individuals.

V. CONCLUSION

Data protection and privacy is a significant concern in the current environment, and it is crucial to handle it. Comprehensive laws relating to the issue of data security are among the significant measures to curb the whole situation. The USA divides the types of data based on their sensitivity and their utility. The division of the requirements enhances the coverage of different types of situations. Additionally, different groups of individuals are covered through the categorization of the data. The different bills and acts cover the needs of adults, children, consumers, and electronic communication. Generalization of these elements leads to generalization in their enforcement, and as a result, the cybercrimes continuously increase with the advancement of technology. Besides, the establishment of the guidelines is not enough to deal with these crimes. Therefore, there is a need to create comprehensive elements of the protection laws alongside comprehensive enforcement agencies to ensure that the guidelines are followed to the letter. Ultimately, the needs of the consumers and other online users will be appropriately met concerning the data protection policies. In a nutshell, the enactment of the laws and bills is the basis of the welfare of the E-commerce sector and other online platforms, which results in the solidity and thriving of the information technology sector.

REFERENCES

[1]. Banisar, D. (2019). National Comprehensive Data Protection/Privacy Laws and Bills 2019. *Privacy Laws and Bills*.
[2]. De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, 32(2), 179-194.
[3]. Dimitrova, A., & Brkan, M. (2018). Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair. JCMS: *Journal of Common Market Studies*, 56(4), 751-767.
[4]. Makulilo, A. B., & Boshe, P. (2016). Data Protection in Kenya. In *African Data Privacy Laws* (pp. 317-335). Springer, Cham.
[5]. Norris, H. (2018). Data Protection Policy. *Policy*.