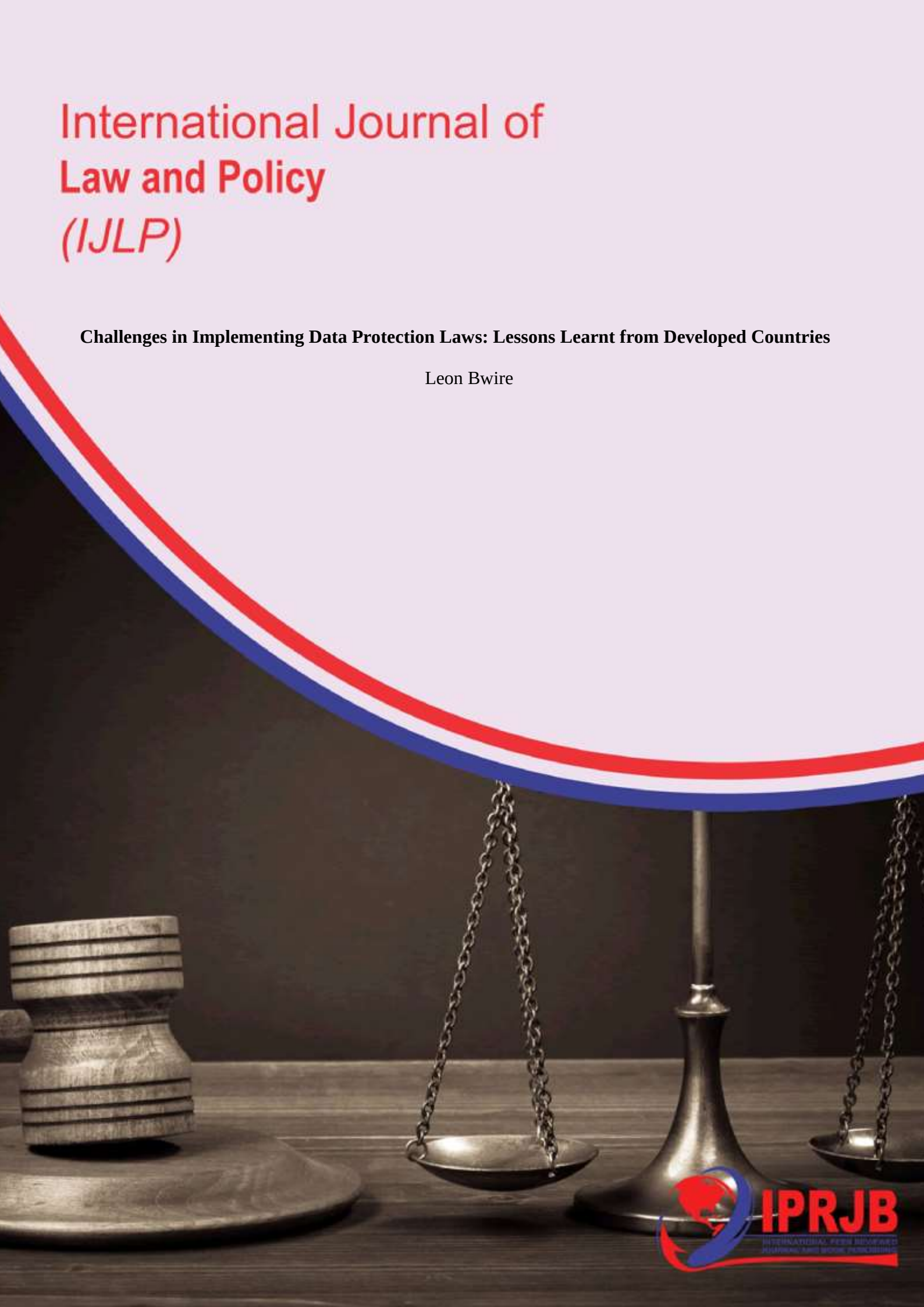
International Journal of
Law and Policy
(IJLP)

Challenges in Implementing Data Protection Laws: Lessons Learnt from Developed Countries

Leon Bwire



International Journal of Law and Policy
ISSN 2520-4637 (online)
Vol.8, Issue 1, No.3. pp 28 - 39, 2023

www.iprjb.org

Challenges in Implementing Data Protection Laws: Lessons Learnt from Developed Countries

Leon Bwire

Article History

Received 25th February 2023
Received in Revised Form 17th March 2023
Accepted 29th March 2023

Abstract

Purpose: The purpose of the study is to examine the challenges experienced in implementing data protection laws.

Methodology: This study adopted a desktop methodology. This study used secondary data from which include review of existing literature from already published studies and reports that was easily accessed through online journals and libraries.

Findings: The study concludes that monitoring and inspections by the regulatory authority regulatory bodies is not properly done because the regulatory authorities lack the resources to monitor and inspect.

Unique Contribution to Theory, Practice and Policy: The study was anchored on Adaptive Structuration Theory and Absorptive Capacity Theory. The study recommended that personal information processing management framework is required to aid the critical industries in understanding how personal information can be processed in line with the requirements of the Act. The study recommended that a wider variety of enforcement strategies should be used apart from the persuasion and warning letters issued to who do not comply.

Keywords: *Data Protection, Laws, Challenges, Implementation*

INTRODUCTION

All nations, including developing nations, embrace the art of technical growth (Jones, 2017). Nowadays, the world is like a village where individuals use the internet to communicate knowledge simultaneously across the globe. Developing nations use new technology without fully comprehending their effects or the legal frameworks that govern them. While technology progress is rapid, legal progress is still notably slow. Because of this, underdeveloped nations might not be able to successfully combat crimes perpetrated online or in the workplace. For instance, spammers could distribute spam online without knowing anything about users in impoverished nations. Although these nations may have data protection laws, these rules may not apply to offenses like spamming because they are generic in nature. According to Eboibi (2021), several nations employ existing laws with broad applicability to combat crimes like spam. Regrettably, these laws fall short of their goals.

Due to the accessibility of enormous volumes of consumer data, also known as big data (Martin & Murphy, 2017), businesses are now using marketing analytics and psychological targeting (Matz et al., 2020) to target their marketing efforts at particular customer segments. A customer's consent is required in order to send marketing messages via email or SMS (Hartemo, 2016). Companies gather and analyze client personal data to obtain a competitive edge, mostly to tailor or align products with the wants of particular customers. Additionally, some businesses' primary objective is the creation and sale of data, so the study and use of data enhances business intelligence and boosts productivity. This suggests that consumer data is a valuable resource for gaining a competitive edge. There are currently markets for personal information that are seen as a tradeable commodity (Spiekermann et al., 2015).

Important contact information, such cell phones, landlines, and e-mail addresses, can be found in collected personal data. Companies can utilize this data to get in touch with current and potential customers to sell them products and services. Customers consider this to be unsolicited commercial communication and a violation of their privacy (Krafft, 2017). Cybercrime such as fraud, database hacking to steal customer information from businesses, unsolicited emails, and eventually customer privacy invasion can be caused by the perceived worth of customer information (Martin & Murphy, 2017). It is essential that nations enact regulations to safeguard against the misuse of personal information obtained during routine business transactions in an effort to reduce worries about security, privacy, and fraud.

In comparison to any U.S.-based initiatives, the European Union (EU) Data Protection Directive (revised in 2015) represents a significantly more comprehensive set of consumer information privacy regulations (Yeh, 2018). The EU Directive requires a single set of data protection laws, making businesses answerable to a single regulatory body for privacy-related actions. Also, consumers in the EU have the right to ask for the removal of web links that no longer accurately reveal their personal information under the terms of a "right to be forgotten." The EU-U.S. Privacy Shield was developed as follows after some discussion about how the EU directive will impact consumers and businesses: With the new agreement, American businesses will have greater obligations to protect the personal data of Europeans, and the U.S. Department of Commerce and Federal Trade Commission (FTC) will have greater oversight and enforcement authority, including through closer coordination with European Data Protection Authorities (European Commission 2016). Numerous requests to be forgotten, one manifestation of the EU Directive, have not yet materialized to harm American businesses, despite the fact that U.S. companies expressed great concern about the burdensome European

regulations on them directly and indirectly by potentially inciting consumer unrest (Manjoo 2015). As a result, the de facto strategy endorsed by both U.S. authorities and businesses continues to be the default mechanism for supporting industry self-regulation in the context of customer information privacy issues.

European customers are more concerned about their privacy, and as a result of EU lawmakers' subsequent regulation to address these issues, much of the formal knowledge regarding consumer privacy has a distinctly Western flavor (Hartzog, 2020). Privacy concerns in eastern, more collectivist cultural societies like India and China represent a significant gap in the literature. In general, there is a significant gap in our knowledge of privacy issues and strategies at the organizational and consumer levels in BRIC nations as well as in still-developing markets. Further research is required in the area of examining differences in privacy beliefs and desires across national and cultural boundaries.

Public and private authorities both have different data protection policies. For instance, only specific categories of data gathered, held, analyzed, and disseminated by private companies are subject to regulation in the United States. These categories include financial, health, educational, and child-related data (Maras and Wandt, 2019). Also, depending on the type of data, regulations vary in some nations (e.g., email content is afforded greater protection than the email address of sender or recipient). Different data protection rules apply to different types of data, including sensitive data, sectoral data, online data, offline data, and data subjects (e.g., adults and children). The Federal Law on Protection of Personal Data Held by Private Parties of 2010 and the General Law for the Protection of Personal Data in Possession of Obligated Persons of 2017 govern the public and private sectors, respectively, of Mexico (Schwartz, 2017) Also, there are legal restrictions in Mexico that govern the handling of private data after cloud services have ended as well as the access of law enforcement to material that has been held there.

The Singaporean government is powerless to significantly regulate the internet (Neo, 2020). Instead, the government restricts internet access while also profiting from the information age. This clearly demonstrates how poor nations aspire to take use of emerging technologies without establishing sound regulatory frameworks for data protection. This exemplifies how several countries' internet regulations have contradictory legal provisions. Censorship is a crucial component of internet governance (Froomkin, 2020). The legal frameworks of governments have been contested in court.

The European Court of Justice (ECJ) and the Advocate General (AG) have consistently limited the scope of data protection law to evaluating the legality of the input stage of personal data processing in their standing jurisprudence (Wachter, 2019). Data subjects have some control over how their personal data is acquired and processed, but very little control over how it is evaluated. This includes the ability to correct and erase inputs and object to undesirable processing. The ECJ makes it plain that, rather than data protection law, the data subject must pursue redress through sectoral regulations that apply to particular circumstances if they seek to contest their evaluation (Phillips, 2018). The security provided to data subjects against inferences will become even less effective as a result of the impending conflict in Europe.

Data collection and processing companies must always behave in the best interests of the data subjects and refrain from doing anything that would be harmful to them, according to a fiduciary obligation requirement (Balkin, 2020). Such legislation, which is now being

discussed in India and the United States, would prevent providers from selling or sharing customers' data with parties who do not prioritize the needs of their customers or using data in ways that benefit them over their customers. This strategy would reduce information asymmetry in many industries where suppliers have a considerably greater understanding of how customers' data may be utilized than their clients. The fiduciary duty model also acknowledges that those who are less fortunate shouldn't have to forfeit their data protection rights in order to use digital services (Dobkin, 2018). Alternatively, requiring companies to operate in the best interests of their clients can encourage customers to utilize new goods and services because they will feel more confident that their data is being used properly.

Western ideas of individual autonomy and liberty have a strong influence on the concept of consent. Governments and businesses rarely accept that consent is a weak instrument for data protection (Bhandari, 2021). However, in a positive development, the Australia Competition and Consumer Protection Commission recommended in 2019 that the Australian government take into account transferring accountability for data protection and privacy from consumers to entities collecting, using, and disclosing personal information.

Personal information about customers should be handled in a manner that is consistent with the reasonable expectations they have developed as a result of their interactions with service providers. Providers should be restricted to gathering, producing, utilizing, and exchanging data compatible with or required for the services being offered. In keeping with this, the Privacy Commissioner for New Zealand has emphasized that, unlike other countries, its law does not rely on consent as the basic authority for collecting, using, and disclosing personal information. Although the primary motivator is the holder of the information's legitimate business purpose, consent undoubtedly plays a part (Parn, 2019). Therefore, the data should not be kept in an identifiable form when they are no longer required for legal purposes.

The Australian Competition and Consumer Commission (ACCC) weighed the pros and cons of using consent versus legitimate interest, noting that "Google submits that legitimate interests can be an effective alternative to consent that balances the impact of data processing against the legitimate interests of the entity processing the information" (Medine, 2020). The ACCC does point out that the very open-ended and flexible formulation of the GDPR's "legitimate interests" basis for processing personal data is a source of significant uncertainty and worry. The ACCC does not advise that the proposed consent requirements be waived in order to exempt personal information that is acquired, used, or disclosed for legitimate interests. The individual whose data are being collected and utilized should be the center of data protection law, and a legitimate purposes approach would be better protective of that individual's interests.

Lehto (2018) claims that technological advancements in Finland have created new information system security controls as well as new dangers to data security. Universities in Europe have been dealing with this problem for many years. Lehto (2018) uses embedded systems as an illustration of a brand-new difficulty in ensuring security. Wang (2018) asserts that high competency levels are necessary for data security, even though they may be present in highly developed countries. Wang (2018) continues by saying that there should be purposeful risk assessment and review because emerging technologies like smart campuses, which extensively rely on the internet and internet of things to share data, create a danger of unwanted access.

Comparatively to the rest of the world, Africa has generally trailed behind in the adoption of data protection regulations (Abdulrauf & Fombad, 2017). Fighting violations of information

privacy in African nations still requires a lot of work (Tshiani, 2018). By ratifying the African Union Convention on Cybersecurity and Personal Data Protection (AU Convention), Africa showed its commitment to protecting citizens' personal information (2014). The aim of the AU Convention is to compel members to create a legislative framework to safeguard personal data. The AU Convention further stipulates that the legal framework must guarantee that when personal information is processed, persons' fundamental rights and freedoms are upheld. The African Union Agreement aims to harmonize earlier regional and municipal data privacy measures (Abdulrauf & Fombad, 2017).

The Protection of Personal Information Act 4 of 2013 (POPIA) (RSA Government, 2013) was passed in South Africa, offering relief to customers whose personal information was being used by businesses without their permission for things like direct marketing of services and goods (Cassim, 2015). Unless there is consent, new customers may only be contacted once, and existing customers are given the option to opt out when they are contacted for similar products or services, the use of collected personal information as a source of information for direct marketing of goods and services is prohibited. Thus, it is crucial that legal requirements for the protection of personal information be taken into account while using personal information for marketing reasons (Zenda, 2020). Although there is now privacy legislation in South Africa to protect the personal information that businesses process, it is still necessary to determine whether the businesses are abiding by the privacy requirements outlined in this Act when marketing to individuals.

The duty to safeguard data protection should establish regulations that do so without violating a person's constitutional rights (Parks, 2020). The Tanzanian government increased limits on the freedom of the press and expression by enacting four laws between 2015 and 2016. (Parks, 2020). The Access to Information Act, the Statistics Act, the Cybercrimes Act, and the Media Services Act all came into effect in 2015. (2016). Since independence, the government has been led by Chama cha Mapinduzi, which has pushed for the approval of the Statistics Act and the Cybercrimes Act. Nevertheless, these laws do not clearly define the types of crimes that can be committed online.

Theoretical Framework

This study is will be guide by Adaptive Structuration Theory which was proposed by Anthony Giddens in 1984 and Neo-liberalism theory that was proposed by Cohen and Levinthal in 1990.

Adaptive Structuration Theory

Anthony Giddens first suggested the Adaptive Structuration Hypothesis in 1984. This theory investigates how members of social systems use rules and resources to interact, leading to the evolution and replication of those systems. Organizations that use information technology for their operations dynamically shape perceptions about the technology's function and usefulness, as well as how it might be applied to their operations. This theory holds that laws and regulations are made based on opinions about how technology should be used. In order to build administrative controls that are formulated based on the nature of interactions among the members of the organizations and the expected use of technology, institutions of higher learning apply this idea. Policies for password management, secondary data storage, and responsibility sharing are a few examples of these measures. Since people's perspectives and interpersonal interactions vary from one organization to the next, so do these policies. At organizations where there is a culture of not protecting data from unauthorized access, such

restrictions are found to be more stringent. With the growth of technology, this theory will assist in comprehending the significance of laws and regulations in data protection.

Absorptive Capacity Theory

Cohen and Levinthal created this theory in 1990. According to the notion, businesses differ in their ability to identify and incorporate innovations into their applications to boost performance. Innovations include the use of information technologies, such as technical information system security controls, in accordance with Cooper and systems and associated technology Molla (2017). According to the notion, organizations will always be exposed to new ideas and information from the outside world, but they will internalize, transform, and use it in different ways. The majority of technical controls implemented in information systems knowledge is found outside of institutions. Nevertheless, not every company uses every piece of information that exists to protect data to safeguard their information system. Institutions employ this knowledge while weighing the cost of implementation of controls and their level of expertise. This idea will make it easier to comprehend how important data protection is.

Empirical Review

Ngethe (2021) studied the impact of information systems security measures on data security at the Kiriri Women's University of Science and Technology in Kenya. The research design used in the study was descriptive. 122 information system users made up the study's sample, which consisted of 55 respondents. Data were gathered by the researcher using a questionnaire. The Statistical Packages of Social Sciences 21 (SPSS) program was used to examine the data that had been gathered. The research showed a correlation between administrative, technical, and physical controls and data security in university-related information systems. According to the study's findings, improving information system controls significantly aid in reducing data insecurity in information systems used at Kiriri University.

Zenda (2020) examined whether the direct marketing rules of the Protection of Personal Information Act 4 of 2013 (POPI) are being followed by the South African insurance sector. Using fresh e-mail addresses and phone numbers, an experiment was run to track the flow of personal information sent to 20 insurance companies seeking quotes for short-term insurance. The experiment's findings show that 92% of the marketing communications recipients received lacked prior consent. Companies outside the sample made contact with one another, indicating third-party sharing. Receiving an unwanted short message service (SMS) communication that demanded clients pay to stop receiving SMSs is against legal standards. In order to help the insurance industry comprehend how personal information can be processed in accordance with the Act's standards, the study recommended that a personal information processing management structure be necessary.

Guracha (2019) investigated how some commercial state-owned businesses in Nairobi City County, Kenya, delivered security services after outsourcing cash protection, body guarding, property protection, and information/data protection services. The Functionalist Model and Securitization Theory served as the study's guiding theories. The chosen research design was descriptive. Questionnaires were utilized in the study to gather information. The study came to the conclusion that the provision of security services by commercial state-owned firms in Kenya was positively and significantly impacted by the outsourcing of cash protection, body guarding, property guarding, and information security services. The study suggested that private data security officers should have access to IT skills, private security companies should

maintain data on any property that enters and leaves the business's premises, and private security companies should keep records on the personnel that they are supposed to protect.

Tikkinen-Piri (2018) investigated how the NDPR rules might affect Data Controllers and Processors in important Nigerian economic sectors. The institutional theory served as a guide for the study's qualitative methodology. A standardization of procedures, policies, and IT assets to demonstrate conformity and achieve legitimacy is only one of the substantial structural changes that the study reveals the NDPR can push, inspire, or encourage firms to make. These conclusions suggest a route for policy in strengthening the institutionalization of NDPR measures across important sectors. It will also educate businesses on the steps that must be taken and modifications that must be made in order to secure the privacy of the personal information that has been gathered from data subjects.

Schwartz (2017) examined how the EU and the US have crafted their distinct legal identities around data privacy. An exploratory research design was adopted in the study. The investigation reveals significant variations between the two systems' conceptions of the individual as the holder of legal interests. According to the study, the EU has developed a privacy culture centered on discussions about data subjects' rights. Moreover, in the EU, the creation of a European citizen's identity is a crucial component of the postwar European project. It also showed that, in contrast, in the United States, the emphasis is on a commercial discourse regarding personal information and the protection of consumers' privacy. The report also shows that in the US, consumer protection in a data marketplace is the main emphasis of data privacy regulation.

Githige (2015) investigated the elements affecting Kenyan broadcasting stations' adherence to the watershed period laws. Data collection methods include questionnaires. A survey research approach was used in the study. A representative sample of Nairobi-based licensed broadcasting television and radio stations participated in the poll. The Kenya Films Classification Board, a watershed regulator, provided statistics on law enforcement (KFCB). According to the study, the factors affecting compliance include the cost of compliance and how strictly the law is enforced. The amount of compliance with the watershed regulation was found to be negatively correlated with the cost of compliance; as the cost of compliance increased, the level of compliance decreased. The study found that the Kenya Films Classification Board, a regulating body, only monitored and inspected a small number of media outlets because it lacked the means to monitor and inspect a significant number of broadcasters. The report advocated using a wider range of enforcement tactics in addition to warning letters and persuasion for broadcasters that disobeyed.

METHODOLOGY

This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries

RESULTS

The results were analyzed into various research gap categories, that is, contextual and methodological gaps.

Contextual and Methodological Gaps

Zenda (2020); Ngethe (2021); Githige (2015) and Guracha (2019) posit a conceptual gap as none of these studies addresses the challenges faced in implementing data protection laws. Schwartz (2017) and Tikkinen-Piri (2018) present a methodological gap as these studies used exploratory and qualitative research design while the current study adopts desktop study research design.

CONCLUSION AD RECOMMENDATIONS

Conclusion

The study comes to the conclusion that marketing communications display personal information with the consumers' consent and charge the customers to unsubscribe. Also, it was determined that strengthening information system controls significantly aid in reducing data vulnerability in those systems. The investigation comes to the conclusion that the regulatory agencies' monitoring and inspections are not carried out correctly because they lack the necessary resources.

Recommendations

To help the industries comprehend how personal information can be processed in accordance with the Act's standards, the study proposed that a personal information processing management framework be required. The study advocated using a wider range of enforcement tactics in addition to persuasion and sending warning letters to non-compliant parties. The report suggests that laws be passed to strengthen the institutionalization of data regulating bodies' actions across important industries.

REFERENCES

Abdulrauf, L. A., & Fombad, C. M. (2017). Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms. *Liverpool Law Review*, *38*, 105-134.

Ang, P. H., & Nadarajan, B. (1996). Censorship and the Internet: A Singapore perspective. *Communications of the ACM*, *39*(6), 72-78.

Balkin, J. M. (2020). The fiduciary model of privacy. *Harv. L. Rev. F.*, *134*, 11.

Bhandari, V., Bailey, R., Parsheera, S., & Rahman, F. (2021). Comments on the (draft) Personal Data Protection Bill, 2019. *Available at SSRN 4051127*.

Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *18*(2), 68-110.

Dobkin, A. (2018). Information fiduciaries in practice: data privacy and user expectations. *Berkeley Technology Law Journal*, *33*(1), 1-52.

Eboibi, F. E. (2021). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, *47*(1), 113-142.

Froomkin, M., & Colangelo, Z. (2020). Privacy as Safety. *Wash. L. Rev.*, *95*, 141.

Githige (2015), Factors influencing compliance with the Watershed Period among broadcasters in Kenya

Guracha, A., & Kiruthu, F. (2019). Attitudes towards Outsourcing Security Services on Service Delivery in Commercial State Owned Enterprises in Nairobi City County, Kenya. *International Journal of Current Aspects*, *3*, 1-13.

Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, 1687.

Jones, P., Wynn, M., Hillier, D., & Comfort, D. (2017). The sustainable development goals and information and communication technologies. *Indonesian Journal of Sustainability Accounting and Management*, *1*(1), 1â-15.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns—Why do customers (not) grant permissions?. *Journal of interactive marketing*, *39*(1), 39-54.

Lehto, M. (2018). Cyber security education and research in the Finland's universities and universities of applied sciences. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 248-267). IGI Global.

Manjoo, F. (2015). Right to be forgotten online could spread. *New York Times*.

Maras, M. H., & Wandt, A. S. (2019). Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, *4*(2), 160-177.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current opinion in psychology*, *31*, 116-121.

Medine, D., & Murthy, G. (2020). Making data work for the poor. *CGAP, January*, *1*.

Neo, R. (2020). The securitisation of fake news in Singapore. *International Politics*, *57*(4), 724-740.

NGETHE, N. S. (2021). *INFORMATION SYSTEM SECURITY CONTROLS AND DATA SECURITY IN KIRIRI WOMEN'S UNIVERSITY OF SCIENCE AND TECHNOLOGY, KENYA* (Doctoral dissertation, KENYATTA UNIVERSITY).

Parks, L., & Thompson, R. (2020). The Slow Shutdown: Information and Internet Regulation in Tanzania From 2010 to 2018 and Impacts on Online Content Creators. *International Journal of Communication (19328036)*, *14*.

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*.

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human genetics*, *137*, 575-582.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Geo. LJ*, *106*, 115.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Geo. LJ*, *106*, 115.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic markets*, *25*, 161-167.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Tshiani, V., & Tanner, M. (2018). South Africa's Quest for Smart Cities: Privacy Concerns of Digital Natives of Cape Town, South Africa. *Interdisciplinary Journal of E-Learning & Learning Objects*, *14*.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, 494.

Yeh, C. L. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*(4), 282-292.

Zenda, B., Vorster, R., & Da Viega, A. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal*, *32*(1), 113-132.

Zenda, B., Vorster, R., & Da Viega, A. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal*, *32*(1), 113-132.