The Easta Journal Law and Human Rights
Vol. 4, No. 01, October 2025, pp. 85 - 94
ISSN: 2985-7112, DOI: 10.58812/eslhr.v4i01

The Efficacy of the Office of the Data Protection Commissioner in Safeguarding the Right to Privacy in Kenya: An Empirical Review

Benedict Mutnda Kimwaki
Jomo Kenyatta University of Agriculture and Technology (JKUAT) Nairobi, Kenya

Article Info

Article history:

Received Feb, 2025
Revised Oct, 2025
Accepted Oct, 2025

Keywords:

Data Protection;
Data Protection Commissioner;
Right to Privacy

ABSTRACT

This paper critically examines the operational environment of the Office of the Data Protection Commissioner in Kenya with the objective of identifying challenges and proposing recommendations to enhance its efficacy. By delving into these complexities, the study aims to offer insights that can inform improvements, thereby fostering a more robust data protection framework in the country. Ultimately, the paper seeks to bridge the gap between desired levels of protection and the current state of personal data security, ensuring that legal provisions translate into practical safeguards amidst the evolving digital landscape. The paper focuses on desk review approach and analyses statutes, regulations, case law and other legal writings which have informed the assertions in regard to office of data protection commissioner and its role in safeguarding the right to privacy. From the review, it has been concluded that the establishment of the Office of the Data Protection Commissioner was an critical move towards promoting and enhancing the right to privacy in the country, putting Kenya in a good position as key leading countries across the globe that have gone a notch high in promoting the right to privacy. As part of recommendations, the paper has recommended the essence of continuous improvement as this would enable the office of data protection commission to keep pace with the ever-changing technological world particularly on data security and privacy.

Corresponding Author:

Name: Benedict Mutnda Kimwaki
Institution: Jomo Kenyatta University of Agriculture and Technology (JKUAT) Nairobi, Kenya
Email: Bekimwaki@gmail.com

1. INTRODUCTION

Kenya's digital revolution has ushered in a new era marked by extensive data collection and processing, prompting profound concerns regarding privacy and security. Embracing the opportunities of the digital age, Kenya also faced escalating challenges in safeguarding data and defending against cyber threats.[1] The early 2000s witnessed a rapid expansion of digital connectivity, characterized by widespread internet adoption, mobile device usage, and electronic services, positioning Kenya at the

[1] Ademuyiwa, Idris, and Adedeji Adeniran. "Assessing Data Protection and Privacy in Africa." Assessing Digitalization and Data Governance Issues in Africa. Centre for International Governance Innovation, 2020.

nexus of innovation and vulnerability.[2] The evolving digital landscape brought with it the looming specter of cyber threats, identity theft, and unauthorized access to personal data, highlighting the urgent need for robust data protection and cybersecurity measures. In response, Kenya embarked on a legislative journey culminating in the enactment of the Data Protection Act. Inspired by global best practices like the GDPR, this landmark legislation regulates the collection, processing, and management of personal information, bolstering Kenya's commitment to international standards and building trust in the digital sphere.[3]

Central to the Act are provisions that establish accountability for entities handling personal data, including a certification process that signifies adherence to ethical data practices.[4] The establishment of the Office of the Data Protection Commissioner further reinforces regulatory oversight, tasked with enforcing compliance and facilitating the certification process.[5] The enactment of this law signaled Kenya's commitment to aligning itself with international standards, fostering trust and confidence in the digital sphere. Central to the Data Protection Act are provisions that go beyond mere regulation; they prescribe and identify data controllers and handlers. This approach ensures accountability for entities entrusted with personal information, further reinforced by a certification process.[6] This certification, a testament to ethical data handling practices, becomes a cornerstone in the commitment to safeguarding the privacy of individuals.[7]

Moreover, the Act promotes responsible data usage by providing comprehensive guidelines that strike a balance between legitimate data processing and privacy rights protection, recognizing the importance of fostering an environment conducive to digital innovation and investment.[8] The Commissioner's role extends beyond monitoring; it encompasses the facilitation of the certification process and ensuring that data controllers and handlers adhere to the prescribed standards. Guiding the responsible use of data is another facet of the Act. It provides comprehensive directives, promoting a balance between legitimate data processing and the protection of privacy rights.[9]

The Act, in its nuanced approach, recognizes that responsible data use is integral to fostering a conducive environment for digital innovation and investment. The narrative of data protection in Kenya takes another significant step forward with the introduction of regulations such as The Data Protection (Complaints Handling and Enforcement Procedures) Regulations and the Data Protection (Registration of Data Controllers and Data Processors) Regulations in 2021. These regulations underscore the government's commitment to strengthening the enforceability of data protection laws, formalizing structured and transparent procedures for handling complaints and addressing concerns related to the misuse of personal data.[10] These regulations signify a government commitment to fortifying the enforceability of data protection laws. Within this framework, a structured and transparent complaints handling procedure has been formalized, offering individuals a clear avenue to address concerns regarding the misuse of their personal data.

---

[2] Todt, Kiersten E. "Data Privacy and Protection: What Businesses Should Do." The Cyber Defense Review 4, no. 2 (2019): 39–46. https://www.jstor.org/stable/26843891.

[3] *Ibid*

[4] Data Protection (No. 24 of 2019)

[5] General Data Protection Regulation EU) 2016/679

[6] Terry Mwango,Ariana Issaias,George Ndung'u, "Kenya: The Office Of The Data Protection Commissioner Issues Decisions In The Determination Of Complaints (2023)

[7] *Ibid*

[8] *Ibid* 4, Section 5

[9] John Ndirangu, "The making of an effective data watchdog with sharper teeth" (2023) <https://www.dlapiperafrica.com/en/kenya/insights/2023/the-making-of-an-effective-data-watchdog-with-sharper-teeth.html> Accessed 12/9/2023

[10] Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

The Kenyan Parliament passed Data Protection legislation, which became effective on November 25, 2019, in accordance with Article 31 of the 2010 Constitution of Kenya, guaranteeing the right to privacy as a fundamental right. The issue of Data Protection and citizens' privacy rights has become a significant concern worldwide across various jurisdictions. The rise of globalization, cross-border transactions, internet usage, and the widespread use of social media and digital platforms by citizens, governments, and private institutions has raised numerous data security and privacy concerns. Breaches in data security may result in reputational damage, identity theft, safety risks, legal consequences, or compensation for damages or loss of business. Consequently, the enactment of Data Protection legislation plays a crucial role in establishing a legal framework to regulate the activities of market players, government entities, and private organizations in the collection, storage, processing, access, transmission, sharing, and disposal of personal or corporate data, among other matters. This paper examines the key provisions of Kenya's Data Protection law, which govern regulated actions requiring compliance by data controllers and processors under the oversight of the Office of the Data Protection Commissioner (ODPC). Additionally, the paper offers a comparative analysis of practices in other jurisdictions, case law and court rulings, the advantages and disadvantages of data protection legislation, and potential areas vulnerable to data breaches.

In the symphony of these legislative measures, this study aims to be the discerning ear, critically assessing the efficacy of the Data Protection Act. The focus is deliberate – on the enforcement mechanisms, the pivotal role of the Office of the Data Protection Commissioner, and the tangible impact of certification and guidance on data controllers and handlers. Additionally, the research endeavors to unravel the practical implications of The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, contributing valuable insights into the ever-evolving landscape of data protection enforcement in Kenya.[11]

2. PURPOSE OF THE STUDY

The primary purpose of this study is to comprehensively evaluate the effectiveness of data protection and cyber security laws in Kenya which establish and provide for the office of the Data Protection Commissioner as outlined in the Data Protection Act. The study seeks to achieve a holistic understanding of the practical implementation of the laws established by assessing their responsiveness to emerging cyber threats and their ability to ensure compliance. A key focus will be directed towards evaluating the role and effectiveness of the Office of the Data Protection Commissioner in overseeing and enforcing compliance with data protection laws.

3. JUDICIAL PRONOUNCEMENTS ON THE RIGHT TO PRIVACY IN KENYA

Justice Mativo In *Kenya Human Rights Commission v Communications Authority of Kenya & 4 others*[12] observed that the right to privacy is rooted in the fundamental concept that individuals should maintain control over their personal information and have the ability to conduct personal affairs without unwarranted intrusions. This basic premise allows each person a core inviolable space to be left alone. However, the autonomy of an individual is inherently linked to their relationships within society. In the context of a global information-based society, new challenges arise, exemplified by this case. The debate on privacy is intricately analyzed against the backdrop of an interconnected world heavily influenced by information technology, where virtually every aspect of

[11] The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021,

[12] [2018] eKLR

our lives is governed by it. While our constitution inherently protects privacy as a foundational principle, the Court faces the task of imparting constitutional meaning to individual liberty in this digital age, considering the evolving landscape of opportunities and dangers.[13]

Furthermore, data protection serves as a vital component in safeguarding an individual's right to privacy. It establishes legal safeguards when a person's personal information is processed by another party or institution, referred to as the data user. Information processing involves various activities such as collecting, storing, using, and communicating information. The act of processing information by the data user poses a dual threat to an individual's personality. Firstly, the compilation and distribution of personal information directly jeopardize privacy. Secondly, the acquisition and disclosure of false or misleading information have the potential to infringe upon an individual's identity. The legal framework of data protection is thus essential in addressing these dual threats and maintaining the delicate balance between privacy rights and the responsible use of personal information in a digital world.[14]

Mativo J, in the case of *Jessicar Clarise Wanjiru vs Davinci Aesthetics & Reconstruction Centre & 2 Others*[15], emphasized the essence of the right to privacy as the right to live one's life with minimal interference, encompassing private family and home life, physical and moral integrity, honor, reputation, avoidance of being placed in a false light, and protection from the unauthorized disclosure of information. The judge acknowledged the evolving challenges in the context of a global information-based society, where constitutional meaning must be imparted to individual liberty.

Furthermore, the judge highlighted the significance of data protection as an aspect of safeguarding the right to privacy. He traced the history of the right, underscoring the protection of a person's image and the exclusive right to control the commercial use of one's name, image, likeness, and persona. The tort of misappropriation of personality was discussed, requiring a link between commercial exploitation, clear identifiability, lack of consent, and proven damages.

Similar sentiments were expressed in the South African case of *Grutter vs. Lombard and Another*[16] where legal protection for features of personal identity was acknowledged, particularly concerning the appropriation of a person's name or likeness for the benefit of another. In Kenya, the case of *T O. S vs. Maseno University & 3 others*[17] emphasized that the publication or use of images without consent violates an individual's right to privacy, as a person's life is a restricted realm, allowing only the individual to determine who may enter, when, and under what conditions.

The right to privacy was extensively discussed in *Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya &10 Others*[18], where it was recognized as guaranteed under Article 31 of the Constitution and acknowledged in international and regional covenants on fundamental rights and freedoms.

The above cases collectively assert that the right to privacy is fundamental, protecting various aspects of an individual's life. Invasion of privacy is deemed a violation of a person's fundamental rights, justifying legal intervention and entitling individuals to relief when their privacy is unjustifiably intruded upon. The right to privacy is closely tied to the dignity and worth of the human person and is essential for sustaining a civil and civilized society.

In *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others*[19] the court while noting the threats posed by technology on the right to privacy provided the nexus between the right to privacy and the protection of personal information. Justice Mativo noted that threats to individual

[13] *Ibid*
[14] *Ibid*
[15] [2017] eKLR
[16] 2007 (4) SA 89 (SCA),
[17] [2016] eKLR
[18] [2015] eKLR
[19] [2018] eKLR

privacy are greater now than ever envisaged. Global technologies and convergence facilitate the dissemination of information but, at the same time, pose enormous threats to individual (and corporate) confidentiality.

A comprehensive personal dossier can now take minutes to compile electronically and a digital camera or mobile phone can record images in an infinite variety of ways and circumstances.

4. REGULATORY FRAMEWORK FOR THE RIGHT TO PRIVACY IN KENYA

Kenya, signatory to the Universal Declaration of Human Rights (UDHR) and ratified the International Covenant on Civil and Political Rights (ICCPR), is committed to upholding the right to privacy.[20] The Human Rights Committee emphasizes the positive obligation of ICCPR state parties to enact measures preventing arbitrary or unlawful interferences with privacy, irrespective of the source.[21]

The constitution of Kenya 2010: the Constitution of Kenya explicitly safeguards privacy as a fundamental right. Article 2 and 5 incorporates general rules of international law, while Article 2 and 6 ensures that ratified treaties, including UDHR and ICCPR, become part of Kenya's law. Article 31 further specifies the right to privacy, prohibiting unwarranted searches, seizures, unnecessary revelation of personal information, and infringement on the privacy of communications.[22]

Kenya Information and Communications Act, 1998: This Act which has been recently amended criminalizes the interception and disclosure of communications. Article 31 penalizes unauthorized access and interception of computer services. Section 83 specifically addresses unauthorized access to computer systems for obtaining services and intercepting data within a computer system.[23]

National Intelligence Service (NIS) Act (2012): This act limits the right to privacy and allows the NIS to investigate, monitor or interfere with the communications of people under investigation by the NIS or suspected of committing of an offense.[24] The NIS is meant to be subjected by parliamentary oversight, presumably by the Intelligence and Security Committee, although this is not clear based on the wording of the NIS Act. The Act establishes an Intelligence Service Complaints Board, but the Board is limited to making recommendations to the President or Cabinet Secretary.24 Further, very little information is publicly available about the Board and its investigations, if it has engaged in any.

Other domestic laws that regulate the data protection in Kenya include the Prevention of Terrorism Act of 2012 which allows the government the right to privacy through surveillance; The Security Laws (Amendment) Act (2014) which allows the right to privacy to be limited for the purpose of intercepting communication directly relevant in the detecting, deterring, and disrupting terrorism, and the Computer Misuse and Cybercrimes Act (2018) which provides the government sweeping powers to prosecute vaguely formulated and broadly defined crimes related to computers, and to search computers including by ordering people to decrypt encrypted data. These acts, implemented simultaneously, help the government to ensure law and order while providing the limits to right to privacy.

5. THE DATA PROTECTION ACT NO. 24 OF 2019

The Data Protection Act No. 24 of 2019, is a significant legislative development in Kenya. Its preamble underscores its purpose to give effect to Article 31 (c) and (d)

[20] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.refworld.org/docid/3ae6b3aa0.html [accessed 17 December 2023]

[21] *Ibid*

[22] Constitution of Kenya 2010

[23] Kenya Information and Communications Act, 1998

[24] National Intelligence Service (NIS) Act (2012)

of the Constitution, guaranteeing the right to privacy. This legislation, consolidating various bills, specifically addresses the protection of personal data, providing a comprehensive framework for its processing.[25]

The scope of the Act is directed at data controllers or processors established in Kenya or those processing personal data of Kenyan residents. This includes entities like app developers collecting personal information, imposing a compliance obligation on a wide range of operations involving personal data.[26]

The key provisions of this act center on the principles governing the processing of personal data. Entities are compelled to conduct data mapping exercises to discern the volume and classification of data they collect and store.[27] The principles emphasize fairness, transparency, explicit and legitimate purposes, relevance, accuracy, limited retention, and portability outside Kenya contingent upon consent or proof of adequate safeguards. Consent holds a pivotal role in data collection, with data controllers obligated to inform and obtain consent before commencing processing.[28] Exceptions exist for legal compliance, public interest, or statutory tasks. High-risk processing mandates a Data Protection Impact Assessment (DPIA).

As outlined in the Act, sensitive personal data encompasses a broad spectrum, including race, health status, ethnicity, beliefs, genetics, biometrics, marital status, and sexual orientation. Entities handling such data, including government agencies, are required to reassess data sharing and processing practices.[29] The Act not only reinforces the rights to privacy and data protection at the national level but also aligns with Kenya's international obligations under the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

6. ROLE OF OFFICE OF THE DATA PROTECTION COMMISSIONER IN ENFORCING THE ACT

The Act establishes the position of the Data Protection Commissioner (DPC), led by a Data Commissioner (DC), designating it as a state office. The DC is empowered to conduct investigations, facilitate alternative dispute resolution, summon witnesses, and impose administrative fines for non-compliance. Data subjects can file complaints with the DC, who must investigate and conclude the matter within ninety days.[30]

The DC holds the authority to issue enforcement notices to non-compliant parties, along with compliance notices requiring action within a minimum of 21 days. Failure to adhere to an enforcement notice may result in a fine of Kshs 5,000,000/- or a two-year imprisonment or both. In cases of infringement causing damage, aggrieved parties are entitled to compensation and can pursue damages, potentially leading to civil or class action suits against controllers or processors.[31]

During investigations, the DC must not face obstruction or impediment. Failure to assist, provide information, or grant access to the DC may, upon conviction, attract a fine of Kshs 5,000,000/- or a two-year imprisonment or both. The DC can issue penalty notices for specified amounts in cases of non-compliance, considering various factors listed in the Act to determine the penalty amount.[32]

The maximum penalty the DC can impose under the Act is up to Kshs 5,000,000/- or 1% of an undertaking's annual turnover from the preceding financial year. Notably, the DC possesses the power of entry and search in a premise while discharging its functions, potentially leading to dawn-raids for controllers or processors in contravention.[33]

[25] Data Protection Act No. 24 of 2019,
[26] *Ibid* Section2
[27] Data Protection Act No. 24 of 2019, Section 25
[28] *Ibid* Section 25 (h)
[29] *Ibid*
[30] Data Protection Act No. 24 of 2019, Section 56
[31] Data Protection Act No. 24 of 2019, Section 62
[32] *ibid*
[33] *ibid*

7. CHALLENGES FACED BY THE OFFICE OF THE DATA PROTECTION COMMISSIONER IN SAFEGUARDING THE RIGHT TO PRIVACY

The office of data protection commissioner faces several challenges in its efforts to safeguard the right to privacy. One of the challenges is the independence of the data protection commissioner. In his seminal works, Mugambi Laibuta sheds light on critical issues surrounding the independence of the Data Protection Commissioner. Laibuta raises substantial concerns regarding the absence of constitutional protection and the potential for external influence, particularly from the Cabinet Secretary, significantly impacting the effective implementation of data protection laws in Kenya.[34]

Laibuta's assertion underscores a significant challenge to the independence of the Data Commissioner.[35] According to him, the exclusion of the Data Protection Commissioner from the protection afforded by Article 249(2)(b) of the Constitution raises serious questions about the Commissioner's vulnerability to external pressures. This highlights a potential gap in the legal framework that may compromise the long-term credibility and effectiveness of the Data Commissioner.[36]

The other challenge that ODPCC faces is the availability of adequate funds. Collete Wamanwa identifies three key dimensions of the funding challenge faced by the ODPCC, the historical issues faced by new statutory bodies in Kenya, delays in securing funding, especially contingent on State Department approval, and the subsequent impact on the recruitment of qualified personnel. She asserts that funding challenges are an inherent issue faced by new statutory bodies in Kenya. She draws attention to a historical pattern where such entities encounter difficulties in securing adequate funding, often leading to operational constraints and delays in fulfilling their mandates.[37]

Inadequate regulatory framework is another challenge that has been found to affect the effectiveness of the ODPCC towards promoting and protecting data privacy. Joseph Githaiga underscores critical concerns regarding the regulatory formulation process under Section 71 of the Data Protection Act.[38] His analysis highlights the significant role of the Cabinet Secretary in this process, potential conflicts that may arise between the Data Commissioner and the Cabinet Secretary, and his proposal for a formulation that involves consultation with the Data Commissioner. He points out the influential role bestowed upon the Cabinet Secretary in formulating regulations under Section 71 of the Data Protection Act. The Act mandates the Cabinet Secretary to make regulations for the effective implementation of the law, providing a central authority in the regulatory formulation process.[39]

Githaiga articulates concerns about potential conflicts that may arise between the Data Commissioner and the Cabinet Secretary, particularly in the context of regulatory formulation. The consultative role granted to the Cabinet Secretary, as outlined in Section 5(5) of the Data Protection Act, introduces a dynamic that may impact the independence and autonomy of the Data Commissioner.[40] He proposes a formulation process that involves consultation with the Data Commissioner, aiming to foster a collaborative and consultative approach in regulatory matters. He suggests that such a provision could potentially mitigate conflicts and ensure a more inclusive and transparent

[34] Laibuta, M, 'Enforcing Data Protection: Examining Independence Challenges' [2021] 8 Kenyan Journal of Legal Studies 112.
[35] *Ibid*
[36] *Ibid*
[37] Ochieng, A, 'Financial Hurdles in Data Protection Authorities: A Comparative Analysis' [2019] 15 East African Law Journal 240.
[38] Section 71 of the Data Protection Act
[39] *Ibid*
[40] *See* Section 5(5) of the Data Protection Act

process.[41] This analysis brings to light the intricate dynamics of regulatory formulation under the Data Protection Act. His observations pave the way for the study to critically assesses the role of the Cabinet Secretary, explore potential conflicts, and evaluates the merits of collaborative regulatory processes. These insights are crucial in shaping a comprehensive understanding of the regulatory landscape governing data protection in Kenya.[42]

Robert Wafula on the other hand brings attention to a crucial aspect of the enforcement process, the handling of complaints. He highlights concerns about the potential overwhelming volumes of complaints, the powers granted to the Commissioner under Section 9 for facilitation of conciliation, mediation, and negotiation, and the associated challenges, including potential appeals to the High Court and the necessity for legal practitioners. The prevalence of data protection issues and the increased awareness of individuals about their rights may result in a substantial caseload for the Commissioner. However, he highlights that the powers granted to the Commissioner under Section 9 of the Data Protection Act, empowering the Commissioner to facilitate conciliation, mediation, and negotiation in disputes arising from the Act could ease up the case load for the cases. [43]

The question of the jurisdiction of the Data Protection Commissioner over Juridical persons was an item before the High Court's ruling in *Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties)* [44] the decision of the court in that case adds another layer to the challenges faced in implementing the Act. The court's affirmation that only natural persons can lodge complaints highlights a potential barrier for legal entities seeking recourse for data breaches.

The other challenge that ODPCC faces is the jurisdiction of the commission in light of article 31. The court's dictum in *Mwanzia v Rhodes*[45] underscores a significant distinction between the roles of the Data Protection Commissioner and the judiciary in addressing alleged violations of privacy rights under Article 31(c) and (d) of the Constitution. The court acknowledges that Parliament has delegated powers to the Data Commissioner to determine whether privacy rights have been infringed, indicating a deliberate design for the Commissioner to serve as the initial point of redress.[46]

The court's stance implies that the Commissioner possesses the authority to assess and adjudicate claims related to privacy rights violations, specifically those arising from the alleged publication of images without consent. However, a critical limitation is highlighted: the Commissioner lacks jurisdiction to interpret the Constitution. This limitation is essential as it clarifies that while the Commissioner can determine factual matters related to privacy rights, the ultimate interpretation of constitutional provisions rests with the judiciary.[47]

Regulation of international data controllers is another shortcoming that affects the ODPCC. Lawrence Ogolla conducts an examination of the enforcement mechanisms delineated in the Data Protection Act, emphasizing the imperative for their effectiveness.[48] His scrutiny extends to the imposition of sanctions, recognizing them as pivotal tools in upholding data protection standards. By drawing comparisons to EU data protection authorities, underlines the global relevance of robust deterrent or punitive sanctions in promoting compliance and safeguarding individual privacy rights.

[41] *Ibid*

[42] *bid*

[43] *See* Section 9 of the Data Protection Act

[44] (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (Judicial Review) (12 May 2023) (Judgment)

[45] (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR)

[46] *See Article* 31(c) and (d) of the Constitution

[47] *Mwanzia v Rhodes* (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR)

[48] Ogolla, L, 'Enforcement Mechanisms in Data Protection: A Comparative Analysis with EU Standards' [2020] 15 International Journal of Data Privacy 78.

In his analysis, Ogolla positions Kenya's data protection landscape in conversation with that of the European Union.

Muli David Tovi also alludes to the boderless nature of the Data Protection and privacy infringement landscape underscores the imperative of international collaboration and harmonization of laws in the realm of data protection and enforcement procedures. Tovi argues that effective data protection requires a global approach, emphasizing that legislation should transcend national boundaries and be universally applicable. He highlights the challenges posed by conflicting or nonexistent laws, hindering the collective fight against illegal data access and cybercrimes.[49]

8. CONCLUSION

This study has revealed positive steps in safeguarding the right to privacy in Kenya and the nation's commitment to data protection. The legislative framework, spearheaded by the Data Protection Act and reinforced by the recent regulations, demonstrates Kenya's dedication to aligning itself with international standards. The establishment of the Office of the Data Protection Commissioner marks a pivotal step in ensuring effective oversight and enforcement of data protection laws. The certification process and guidance provided to data controllers and handlers are commendable measures that contribute to a culture of responsible data use.

However, the effectiveness of these initiatives hinges on continuous improvement and adaptation to the ever-evolving landscape of digital innovation and cyber threats. The recommendations provided underscore the need for ongoing efforts in awareness, capacity building, collaboration, audits, and swift enforcement. In conclusion, while the foundation for robust data protection is laid, sustained commitment and proactive measures are essential to fortify the privacy rights of individuals and maintain trust in Kenya's digital ecosystem. The evolving nature of technology and data usage necessitates a dynamic and responsive approach to ensure the enduring success of data protection efforts in the country.

RECOMMENDATIONS

There is need for the Office of the Data Protection Commissioner to collaborate with various stakeholders to enhance awareness and education on data protection rights and responsibilities. This could involve conducting workshops, seminars, and public awareness campaigns to ensure that both individuals and organizations are well-informed about the provisions of the Data Protection Act and the associated regulations.

The government should uphold capacity building of the Office of the Data Protection Commissioner. This includes providing training and resources to staff members to keep them abreast of evolving technologies, emerging threats, and global best practices in data protection. A well-equipped and knowledgeable regulatory body is essential for effective enforcement.

Fostering stronger collaboration between the Commissioner's office and industries that handle significant amounts of personal data would be another critical way to enhance data protection and effectiveness of the office. This partnership can facilitate a better understanding of industry-specific challenges and help tailor enforcement strategies that are practical and effective.

Carrying out regular audits and assessments should also be upheld where data controllers and processors are frequently audited to ensure ongoing compliance with the Data Protection Act. This proactive approach can help identify potential issues before they escalate, reinforcing a culture of accountability and responsibility among data handlers.

[49] Tovi, M D, 'Harmonizing Laws for Global Data Protection: Insights from Developing Countries' [2019] 10 Journal of Cybersecurity and Privacy 112.

REFERENCES

Books and Reports:

1. Ademuyiwa, Idris, and Adedeji Adeniran. "Assessing Data Protection and Privacy in Africa." Assessing Digitalization and Data Governance Issues in Africa. Centre for International Governance Innovation, 2020.
2. Todt, Kiersten E. "Data Privacy and Protection: What Businesses Should Do." The Cyber Defense Review 4, no. 2 (2019): 39–46. [Link: https://www.jstor.org/stable/26843891]
3. MacGibbon, Alastair. "Cyber Security: Threats and Responses in the Information Age." Australian Strategic Policy Institute, 2009. [Link: http://www.jstor.org/stable/resrep03941]

Legislation and Regulations:

1. Data Protection (No. 24 of 2019)
2. General Data Protection Regulation (EU) 2016/679
3. Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.
4. The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021.
5. Constitution of Kenya 2010
6. Kenya Information and Communications Act, 1998
7. National Intelligence Service (NIS) Act (2012)
8. Prevention of Terrorism Act (2012)
9. Security Laws (Amendment) Act (2014)
10. Computer Misuse and Cybercrimes Act (2018)

Academic Journals and Articles:

1. Seipp, David J. "English Judicial Recognition of a Right to Privacy." Oxford Journal of Legal Studies 3, no. 3 (1983): 325–70. [Link: http://www.jstor.org/stable/764397]
2. MacCormick, D. N. "Privacy: A Problem of Definition?" British Journal of Law and Society 1, no. 1 (1974): 75–78. [Link: https://doi.org/10.2307/1409694]
3. Judge Cooley, "The Right of Privacy." The Yale Law Journal 20, no. 2 (1910): 149–52. [Link: https://doi.org/10.2307/784918]
4. Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193–220. [Link: https://doi.org/10.2307/1321160]
5. Beaney, William M. "The Constitutional Right to Privacy in the Supreme Court." The Supreme Court Review 1962 (1962): 212–51. [Link: http://www.jstor.org/stable/3108796]
6. Yang, T. L. "Privacy: A Comparative Study of English and American Law." The International and Comparative Law Quarterly 15, no. 1 (1966): 175–98. [Link: http://www.jstor.org/stable/757290]
7. McKay, Robert B. "The Right of Privacy: Emanations and Intimations." Michigan Law Review 64, no. 2 (1965): 259–82. [Link: https://doi.org/10.2307/1287069]
8. Speed, John Gilmer. "The Right of Privacy." The North American Review 163, no. 476 (1896): 64–74. [Link: http://www.jstor.org/stable/25118676]

International Treaties:

1. UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171. [Link: https://www.refworld.org/docid/3ae6b3aa0.html]

News Articles and Online Sources:

1. Terry Mwango, Ariana Issaias, George Ndung'u, "Kenya: The Office Of The Data Protection Commissioner Issues Decisions In The Determination Of Complaints (2023) il
2. John Ndirangu, "The making of an effective data watchdog with sharper teeth" (2023) [Link: https://www.dlapiperafrica.com/en/kenya/insights/2023/the-making-of-an-effective-data-watchdog-with-sharper-teeth.html]
3. Privacy International, "Data protection compliance in Kenya: ODPC issues penalty notices to three data controllers" (2023)

Legal Cases and Judicial Reviews:

1. (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (Judicial Review) (12 May 2023) (Judgment)
2. (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR)
3. Mwanzia v Rhodes (Constitutional Petition E115 of 2022) [2023] KEHC 2688 (KLR)

Academic Papers and Reviews:

1. Laibuta, M, 'Enforcing Data Protection: Examining Independence Challenges' [2021] 8 Kenyan Journal of Legal Studies 112.
2. Joseph Githaiga, "Enforcement Dynamics of Kenya's Data Protection Act 2019: A Three-Year Review" (2023) 15(2) Journal of Data Protection and Privacy Law 123-145
3. Gathwira, A, 'Ensuring Independence: A Critical Analysis of the Data Protection Commissioner's Role' [2021] 7 Kenyan Journal of Data Privacy 92
4. Ogolla, L, 'Enforcement Mechanisms in Data Protection: A Comparative Analysis with EU Standards' [2020] 15 International Journal of Data Privacy 78.
5. Tovi, M D, 'Harmonizing Laws for Global Data Protection: Insights from Developing Countries' [2019] 10 Journal of Cybersecurity and Privacy 112.