Legal and Ethical Implications of Data Privacy in Artificial Intelligence: A Review of Data Privacy among Learners in Kenyan Secondary Schools

Muli Mutuku

Abstract:- The Artificial Intelligence (AI) incooperation in educational settings sparked significant discussions regarding data privacy, especially in secondary schools in Kenya. As AI technologies became increasingly prevalent, the oversight and guiding of students' individual information raised important legal and ethical concerns. This study explored the legal and ethical implications of data privacy in AI applications within Kenyan secondary schools, focusing on the unique challenges faced in this context. The problem statement addressed the growing concerns over the adequacy of current data privacy protections and the potential risks posed by AI systems handling sensitive student information. The study had three primary objectives: first, to assess the current legal frameworks and policies governing data privacy in Kenyan secondary schools; second, to evaluate the ethical considerations related to the use of AI technologies and their impact on students' privacy; and third, to identify best practices for enhancing data protection. The scope of the study was confined to secondary schools across Kenya, examining the intersection of legal regulations and ethical practices in managing student data within these institutions. The justification for this study lay in the increasing reliance on AI tools in education and the need to ensure that data privacy standards were robust enough to protect students' personal information. Data for this review was collected from secondary sources, including existing literature, policy documents, and previous research findings. The method of data collection involved a comprehensive literature review, followed by a qualitative analysis of the collected data to identify patterns and insights related to data privacy issues. The reason for the inquiry of the study was to provide a thorough review of the current state of data privacy among learners in Kenyan secondary schools and to offer recommendations for improving legal and ethical practices. By analyzing secondary sources, the study aimed to contribute to the development of more effective data privacy strategies and ensure that AI technologies were executed in a manner that safeguarded students' rights and interests.

Keywords: *Artificial Intelligence (AI), Data Privacy, Legal Frameworks, Ethical Implications, Data Protection.*

I. INTRODUCTION

The increasing in cooperation of artificial intelligence (AI) into educational units worldwide has brought about numerous benefits, including personalized learning experiences and improved administrative efficiency. However, this technological advancement has also introduced significant legal and ethical challenges, particularly concerning data privacy among learners. In Kenya, where AI is gradually being adopted in secondary schools, the privacy of students' data has become a critical issue that requires careful consideration. This research examines the legal and ethical implications of data privacy in AI, focusing on learners in Kenyan secondary schools.

Lacroix (2019) discusses the privacy challenges associated with big data, particularly in healthcare, where the collection of vast amounts of data can lead to ethical dilemmas. Although the focus is on healthcare, the issues highlighted by Lacroix, such as consent, data ownership, and the potential for misuse, are equally relevant in the educational sector. In the context of Kenyan secondary schools, the putting together and processing of student data by AI systems raise similar concerns. There is a pressing need for legal frameworks that take care the privacy solitude of students while allowing the benefits of AI to be realized (Lacroix, 2019).

Ishii (2019) provides a comparative legal analysis of privacy and data protection in AI-equipped robots, emphasizing the importance of considering both functional and technological aspects. The study's insights are pertinent to the educational sector, where AI technologies are increasingly used to monitor student performance and behavior. Ishii's research highlights the shortcomings of current legal frameworks in effectively addressing the specific challenges that AI presents, especially in safeguarding minors' data within educational environments (Ishii, 2019).

Hoxhaj, Halilaj, and Harizi (2023) explore the ethical implications and human rights concerns associated with AI. They argue that AI's deployment can lead to significant ethical dilemmas, including privacy violations and increased surveillance. In Kenyan secondary schools, the use of AI to track student activities could potentially infringe on students' privacy rights, making it imperative to establish strong legal protections and ethical guidelines to prevent misuse (Hoxhaj, Halilaj, & Harizi, 2023).

Aina (2024) provides a global perspective on the ethical implications and legal frameworks for privacy in AI. The study highlights the varying approaches taken by different countries to regulate AI and protect data privacy. In Kenya, where data protection laws are still evolving, Aina's work suggests that more robust legal frameworks are needed to safeguard student data from potential abuses associated with AI technologies (Aina, 2024).

Naik et al. (2022) examine the legal and ethical considerations of AI in healthcare, raising important questions about responsibility and accountability. While the focus is on healthcare, the issues discussed are applicable to the educational sector, where AI systems increasingly influence decision-making processes. The question of who is responsible when AI systems in schools violate students' privacy is particularly relevant, highlighting the need for clear legal guidelines (Naik et al., 2022).

Peltz and Street (2020) discuss the ethical dilemmas involving privacy in AI, particularly in the context of global security. Their work emphasizes the need for ethical considerations to be at the forefront of AI development. In Kenyan secondary schools, where AI is used to enhance security and monitor students, there is a risk that privacy rights could be compromised. Therefore, it is crucial to ensure that ethical considerations are integrated into the development and deployment of AI systems in educational settings (Peltz & Street, 2020).

Cath (2018) addresses the governance of AI, focusing on the ethical, legal, and technical challenges that need to be addressed to ensure responsible AI development. Cath's insights are valuable for understanding the complexities of AI governance in educational contexts, particularly in relation to protecting students' data privacy. The study underscores the importance of developing comprehensive legal and ethical frameworks to govern the use of AI in schools (Cath, 2018).

Despite the extensive research on the legal and ethical implications of data privacy in AI, there remains a significant gap in understanding how these issues manifest in the educational sector, particularly among secondary school learners in Kenya. Most existing studies have focused on healthcare or global perspectives, with limited attention given to the unique challenges faced by educational institutions in developing countries. This research aims to fill this gap by examining the specific legal and ethical challenges associated with data privacy in AI as it relates to secondary school students in Kenya. By focusing on this underexplored area, the study seeks to contribute to a more comprehensive understanding of the legal and ethical frameworks needed to protect student data in the context of AI adoption in Kenyan schools. The study was guided by the following research questions:

- What are the current legal frameworks and policies governing data privacy in Kenyan secondary schools?
- How do ethical considerations relate to the use of AI technologies impact students' privacy in Kenyan secondary schools?
- What are the best practices for enhancing data protection in the context of AI use in Kenyan secondary schools?

This study focused on the legal and ethical implications of data privacy related to the use of AI technologies in Kenyan secondary schools. It aimed to explore existing legal frameworks, assess ethical considerations, and identify best practices for enhancing data protection. Through qualitative research, including interviews and literature reviews, the study examined how AI was implemented in Kenyan schools and the associated privacy concerns. The research was justified by the increasing adoption of AI in education and the need for robust legal and ethical safeguards to protect student data. It contributed valuable insights and practical recommendations for improving data privacy in the educational sector.

II. LITERATURE REVIEW

➢ *Global Data Privacy Standards*

Rustad and Koenig (2019) argue for the need for a global data privacy standard, given the transnational nature of data flows. They highlight that existing national and regional framework, such as the General Data Protection Regulation (GDPR) in the European Union, are often inadequate when dealing with cross-border data issues. The authors advocate for a harmonized global framework that can ensure consistent data protection while respecting the cultural and legal differences of individual nations.

Bennett and Raab (2020) revisit the governance of privacy by analyzing contemporary policy instruments within a global context. They observe that while data privacy regulations have become more stringent, there is significant variation in how these policies are implemented across different jurisdictions. Their work emphasizes the need for a balance between protecting individual privacy and enabling the free flow of information, particularly in the context of emerging technologies such as artificial intelligence.

Sharma (2019) provides an in-depth analysis of the GDPR, which has set a high standard for data privacy worldwide. The GDPR's principles of data protection by design and by default, along with its strict consent requirements and rights for data subjects, have influenced many countries to adopt similar regulations. Sharma discusses the challenges organizations face in complying with the

GDPR, especially in terms of implementing appropriate technical and organizational measures to protect personal data.

Scheibner et al. (2020) examine the specific challenges of data protection in multisite research involving health data. Their comparative study of legislative governance frameworks highlights the complexities of ensuring data privacy in research that spans multiple jurisdictions. The authors emphasize the role of data protection technologies, such as encryption and anonymization, in meeting the ethical and legal requirements of data privacy. They argue that while legislation provides the necessary legal framework, technology plays a crucial role in operationalizing these requirements in practice.

III. RESEARCH METHODOLOGY

The data collection was from secondary sources which primarily involved reviewing and synthesizing existing legal, regulatory, and academic materials. The study leveraged a combination of legal texts, policy documents, reports, and scholarly articles to address their respective research questions and objectives. This approach allowed the researcher to build on existing knowledge and provide insights into data privacy and governance challenges.

IV. FINDINGS

The findings from the reviewed articles provide a comprehensive view of the current data privacy landscape. Rustad and Koenig (2019) identified the need for a global data privacy standard due to inconsistencies in national frameworks, arguing that a harmonized regulatory approach is necessary to effectively manage cross-border data issues. Bennett and Raab (2020) found significant variation in privacy governance across countries, noting that while privacy regulations are becoming more stringent, their effectiveness varies based on implementation practices. Sharma (2019) highlighted that the GDPR sets a high standard for data privacy, but organizations frequently face challenges in achieving compliance with these rigorous requirements. Scheibner et al. (2020) examined diverse legislative frameworks for multisite health research, emphasizing the importance of data protection technologies, such as encryption, in meeting both ethical and legal data protection requirements. These studies collectively underscore the need for cohesive global standards, effective policy implementation, and technological advancements to address current data privacy challenges.

V. DISCUSSION

The findings from the reviewed articles offer important insights into the current legal frameworks and policies governing data privacy, particularly relevant to Kenyan secondary schools. Rustad and Koenig (2019) emphasize the need for a global data privacy standard due to inconsistencies in national laws, which reflects the challenges Kenya faces with implementing its Data Protection Act, 2019, in a way that aligns with global standards. Bennett and Raab (2020) highlight the variation in privacy governance effectiveness, a concern that may be evident in Kenyan schools where the application of data protection measures can differ significantly. Ethical considerations related to AI technologies, as discussed by Sharma (2019), stress the importance of adhering to high data protection standards, which is crucial for safeguarding students' privacy in Kenyan schools. Scheibner et al. (2020) further underline the need for robust data protection technologies and legislative frameworks, suggesting that Kenyan schools should integrate advanced security measures such as encryption and regular audits to address the challenges of AI data use. These findings collectively underscore the importance of adapting international best practices to the local context, ensuring that Kenyan secondary schools effectively protect student privacy while leveraging AI technologies.

VI. CONCLUSIONS

In conclusion, the findings from the reviewed articles underscore the critical need for effective data privacy frameworks and ethical considerations, particularly in the context of Kenyan secondary schools. The global perspective offered by Rustad and Koenig (2019) highlights the importance of aligning local policies with international standards, addressing the inconsistencies and gaps that may affect data privacy in Kenya. Bennett and Raab's (2020) insights on the variability of privacy governance emphasize the need for robust implementation and compliance measures. Sharma's (2019) discussion on GDPR standards and Scheibner et al. (2020) on data protection technologies point to best practices that Kenyan schools should adopt, including advanced security measures and adherence to ethical guidelines for AI technologies. By integrating these global best practices with local regulations and focusing on comprehensive data protection strategies, Kenyan secondary schools can enhance their approach to safeguarding student privacy and ensure ethical use of AI technologies. This holistic approach is essential for creating a secure and responsible data management environment in educational settings.

RECOMMENDATIONS

To enhance data privacy and ethical use of AI technologies in Kenyan secondary schools, several key recommendations emerge from the findings. Schools should align local data privacy policies with international standards, such as those proposed by Rustad and Koenig (2019), to address inconsistencies and improve protection. Strengthening the implementation and compliance of privacy measures, as highlighted by Bennett and Raab (2020), is crucial, involving regular audits and staff training. Investing in advanced data protection technologies, including encryption and anonymization, is essential, as suggested by Sharma (2019) and Scheibner et al. (2020). Ethical considerations in AI use must be carefully addressed, ensuring informed consent and robust data security. Finally, promoting continuous monitoring and evaluation of data privacy practices will help adapt to new challenges and maintain compliance. These steps will significantly improve data protection and ethical AI use in Kenyan secondary schools.

REFERENCES

[1]. Aina, N. (2024). Ethical implications and legal frameworks for privacy in artificial intelligence: A global perspective. *International Journal of Social Analytics, 9*(5), 1-10.

[2]. Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance, 14*(3), 447-464. https://doi.org/10.1111/rego.12229

[3]. Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

[4]. Hoxhaj, O., Halilaj, B., & Harizi, A. (2023). Ethical implications and human rights violations in the age of artificial intelligence. *Balkan Social Science Review, 22*(22), 153-171.

[5]. Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: Looking at functional and technological aspects. *AI & Society, 34*, 509-533. https://doi.org/10.1007/s00146-018-0849-7

[6]. Lacroix, P. (2019). Big data privacy and ethical challenges. In *Big Data, Big Challenges: A Healthcare Perspective: Background, Issues, Solutions and Research Directions* (pp. 101-111). Springer.

[7]. Naik, N., Hameed, B. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., ... & Somani, B. K. (2022). Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? *Frontiers in Surgery, 9*, 862322. https://doi.org/10.3389/fsurg.2022.862322

[8]. Peltz, J., & Street, A. C. (2020). Artificial intelligence and ethical dilemmas involving privacy. In *Artificial Intelligence and Global Security: Future Trends, Threats and Considerations* (pp. 95-120). Emerald Publishing Limited.

[9]. Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Florida Law Review, 71*(1), 365-411.

[10]. Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J. R., Raisaro, J. L., Hubaux, J. P., & Vayena, E. (2020). Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences, 7*(1), lsaa010. https://doi.org/10.1093/jlb/lsaa010

[11]. Sharma, S. (2019). *Data privacy and GDPR handbook*. John Wiley & Sons.