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

Muli Mutuku

https://doi.org/10.62049/jkncu.v5i1.170

Abstract

The Artificial Intelligence (AI) cooperation 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 the systematic search on Scopus, Web of Science and ERIC repositories, 25 paper were listed out from the year 2020 to 2024. The method of data collection involved a comprehensive systematic literature review from secondary sources which included periodicals, published articles and books, followed by a qualitative analysis of the collected data to identify patterns and insights related to data privacy issues. 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.

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

Introduction

The 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.

Naik *et al*. (2022) examines the legal and ethical considerations of AI in healthcare, raising important questions about responsibility and accountability in global perspective. 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.

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 in a global perspective. 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.

Peltz and Street (2020) discuss the ethical dilemmas involving privacy in AI, particularly in the 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.

Lacroix (2019) discusses the privacy challenges associated with big data, particularly in healthcare in Europe Countries, 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 of the privacy solitude of students while allowing the benefits of AI to be realized.

Hoxhaj, Halilaj, and Harizi (2023) explores the ethical implications and human rights concerns associated with AI in Europe. 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.

Aina (2024) provides a global perspective on the ethical implications and legal frameworks for privacy in AI. The study that was conducted in Malasyia highlighted 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.

Shaltout (2024), in a study conducted in Egypt, examines the legal aspects of using AI in digital identity and authentication within banking, highlighting the challenges and risks associated with AI-driven processes, such as digital payments. The research underscores the need for comprehensive legal frameworks to ensure the secure handling of sensitive data, a concern that resonates in the Kenyan context, where educational institutions are adopting AI technologies for administrative and instructional purposes.

Liywalii (2023) explores the implications of AI for children in Africa, analyzing its impact on childhood experiences through a normative ethics lens. The research emphasizes the vulnerabilities of children to data privacy breaches, calling for ethical safeguards tailored to the unique needs of this demographic. This perspective is particularly relevant for Kenyan secondary schools, where the integration of AI tools raises similar concerns about protecting students' personal information.

Gaffley, Adams, and Shyllon (2022) provide a pan-African insight into the ethical and human rights implications of AI. Their research highlights the inadequacy of existing legal frameworks in addressing the ethical dilemmas posed by AI, emphasizing the need for African-specific strategies to ensure data privacy and compliance. These findings offer a foundation for understanding the broader challenges faced by Kenyan educational institutions in safeguarding student data.

Kumbo, Nkwera, and Mero (2024) investigate ethical practices in the development of AI and machine learning systems in Tanzania, drawing attention to the gaps in ethical oversight during system development. Their findings stress the importance of incorporating ethical principles in AI design, a recommendation that can guide Kenyan stakeholders in mitigating privacy risks associated with AI in schools.

Kitili and Karanja (2023) focus on the intersection of AI and privacy concerns in eHealth in Kenya. Their case study highlights the vulnerabilities in managing sensitive data and the critical role of legal frameworks in ensuring data protection. Their findings directly inform the Kenyan secondary school context, where similar vulnerabilities may arise as AI technologies are deployed for educational purposes.

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:

i. What are the current legal frameworks and policies governing data privacy in Kenyan secondary schools?
ii. How do ethical considerations relate to the use of AI technologies impact students' privacy in Kenyan secondary schools?

iii. What are the best practices for enhancing data protection in the context of AI use in Kenyan secondary schools?

Theoretical Framework

The study will be guided by the following human rights theory. Human Rights Theory is rooted in the philosophical and legal understanding that every individual possesses inherent rights that must be respected and protected. These rights are enshrined in foundational documents such as the Universal Declaration of Human Rights (UDHR) adopted by the United Nations in 1948, often attributed to contributions by Eleanor Roosevelt and other members of the drafting committee. While the concept of human rights has historical precedents, its formal modern articulation emerged post-World War II to ensure the protection of individual freedoms and dignity globally.

Artificial intelligence (AI) and data privacy, Human Rights Theory provides a critical lens for examining how AI systems interact with individuals' rights, particularly the right to privacy as stipulated in Article 12 of the UDHR. This framework is increasingly relevant as AI technologies are integrated into various domains, including education, where sensitive personal data is often collected and processed.

Miao (2019) emphasizes the importance of human rights ethics in AI research, arguing that technologies should be designed and deployed in ways that respect fundamental human rights, including data privacy and security. This perspective is particularly applicable to Kenyan secondary schools, where students' data privacy might be at risk due to insufficient safeguards in AI systems. Ensuring compliance with human rights principles can mitigate risks of misuse or exploitation of student data.

Kumar and Choudhury (2023) further explore the intersection of normative ethics and human rights in AI, highlighting the potential for AI systems to either uphold or infringe on human rights depending on their design and regulation. Their research underscores the need for ethical frameworks aligned with human rights to guide AI implementation, especially in sensitive environments like schools. This aligns with the necessity of legal and ethical standards in Kenya to ensure that AI-driven educational technologies protect students' personal information.

Sartor (2020) examines the legal and ethical dimensions of human rights in the age of AI, emphasizing the tension between technological advancement and the safeguarding of individual rights. In regions like Kenya, where AI adoption in education is growing, the application of human rights theory can serve as a foundation for developing robust data privacy laws and ethical guidelines. Such measures would help ensure that the deployment of AI in schools prioritizes the dignity, autonomy, and privacy of learners.

Human Rights Theory, therefore, serves as a foundational framework for understanding and addressing the legal and ethical implications of data privacy in AI. By grounding AI practices in human rights principles, stakeholders can balance technological innovation with the protection of students' rights, fostering a safer and more equitable educational environment in Kenyan secondary schools.

Literature Review

Data privacy for Artificial Intelligence (AI) has garnered significant attention due to its potential impact on personal privacy, particularly in educational settings. This literature review examines the legal and ethical implications of AI technologies, focusing on the protection of data privacy for learners in Kenyan secondary schools. Drawing on international and local perspectives, this review discusses the key challenges and frameworks that govern AI's use in educational environments and highlights the ethical considerations necessary to protect students' privacy.

James (2024) explores the ethical and legal implications of using big data and AI in public relations campaigns in the United States, emphasizing the significant concerns around data privacy when leveraging AI for large-scale data processing. Although this study focuses on the public relations sector, it highlights the risks of data misuse and the need for robust privacy protection, which can be extended to the educational sector in Kenya. In particular, James (2024) underscores the necessity of establishing clear legal frameworks to regulate AI's use of personal data, ensuring that consent is obtained, and data is securely managed.

Gerke, Minssen, and Cohen (2020) examine the ethical and legal challenges of AI in healthcare, which offers valuable insights into the broader implications of AI technologies in sectors like education. Their work stresses the importance of developing comprehensive legal frameworks that align with ethical principles to safeguard personal data from AI exploitation. For Kenyan secondary schools, this underscores the need to adopt such frameworks that consider the unique vulnerabilities of student data, particularly as AI tools are increasingly used for academic performance tracking and behavioral analysis.

Aina (2024) takes a global perspective on privacy concerns related to AI, discussing the diverse regulatory responses across countries. In particular, Aina highlights the varying legal approaches to AI-driven privacy concerns, suggesting that while some countries have comprehensive privacy laws, others, including Kenya, are still in the process of developing or refining their frameworks. This review suggests that Kenya could benefit from integrating global best practices, such as those proposed by the European Union's General Data Protection Regulation (GDPR), to better protect student privacy in the context of AI usage in schools.

Huang (2023) addresses the ethics of AI in education, focusing on student privacy and data protection. Conducted in an educational context, Huang's research is particularly relevant to the Kenyan secondary school setting, where AI technologies are being used for personalized learning, administrative functions, and even surveillance. Huang emphasizes the need for strong ethical frameworks that prioritize students' rights to privacy, highlighting the importance of transparency and accountability in AI's use of student data. This is a crucial concern for Kenyan policymakers, who must balance technological innovation with the ethical obligation to protect young learners' personal information.

Che (2024) analyzes the legal and ethical implications of digital technologies, including AI, on businesses in Cameroon, providing valuable insights into data privacy challenges faced by developing countries. Although focused on business environments, Che's findings are applicable to the Kenyan context, where AI technologies are increasingly integrated into educational settings. Che argues for the development of localized legal frameworks that consider the socio-economic realities of developing countries, which could guide Kenya in drafting policies that protect student data without stifling technological advancements.

Chikotie, Watson, and Watson (2023) explore privacy and ethical considerations in AI-enabled systems for syndromic surveillance in Southern Africa, an area with significant under-resourced countries. Their work highlights the challenges of implementing AI technologies in environments with limited resources, suggesting that countries like Kenya must prioritize the development of ethical guidelines that ensure the protection of privacy, particularly when AI is used to monitor students' behaviors or academic performance.

Gaffley, Adams, and Shyllon (2022) provide a comprehensive summary of the ethical and human rights implications of AI in Africa, emphasizing the need for Africa-specific legal frameworks that address privacy concerns. Their research advocates for a regionally tailored approach to data protection in the context of AI, which could help Kenya navigate the complexities of AI usage in schools while safeguarding student privacy. Gaffley *et al*. (2022) argue that AI's ability to process vast amounts of personal data necessitates stronger protections, particularly in educational settings where students' vulnerability to privacy breaches is heightened.

Kitili and Karanja (2023) conduct a case study on the use of AI in eHealth in Kenya, exploring the privacy concerns associated with digital health tools. This study offers critical insights for educational settings where AI is similarly used to track student performance and behavior. Kitili and Karanja (2023) emphasize the need for robust data protection mechanisms and clear consent protocols to ensure that personal data is handled ethically and securely.

Kisio and wa Teresia (2024) examine the ethical implications of advanced surveillance technologies used by law enforcement in Kenya. While their research focuses on surveillance in a security context, it offers important lessons for educational institutions in Kenya, where AI-driven surveillance technologies are increasingly used to monitor students. Their work advocates for transparent policies that ensure surveillance technologies are used responsibly and do not infringe on individuals' privacy rights.

The literature reveals significant gaps in data privacy protection in AI usage in schools. Although international and regional frameworks provide a foundation, Kenya must develop specific legal and ethical guidelines tailored to their educational system. The implementation of these frameworks should prioritize transparency, informed consent, and the use of secure technologies to safeguard student privacy.

Research Methodology

The data collection was from secondary sources which primarily involved reviewing and synthesizing existing legal, regulatory, and academic materials. Systematic review design was employed to methodically collect and analyze all relevant studies on a defined research questions for the study. Through the systematic search on Scopus, Web of Science and ERIC repositories, 25 paper were listed out from the year 2020 to 2024. 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.

Findings

What Are the Current Legal Frameworks and Policies Governing Data Privacy in Kenyan Secondary Schools?

The reviewed findings provide insight into the challenges and opportunities in aligning Kenya's data privacy frameworks with global standards. Rustad and Koenig (2019) emphasize the need for harmonized global data privacy regulations, suggesting that inconsistencies in national frameworks could pose challenges for Kenya. While Kenya has enacted the Data Protection Act (2019), its implementation in secondary schools may face hurdles similar to those noted by Bennett and Raab (2020), who found that the effectiveness of privacy regulations varies based on governance and execution. Furthermore, Sharma (2019) highlights the stringent benchmarks set by frameworks such as the GDPR, which could serve as a model for improving Kenya's policies. However, adopting such high standards requires addressing local constraints, including resource limitations and awareness gaps in educational institutions. These findings collectively underscore the need for a robust, relevant regulatory framework needs to be implemented to ensure effective data privacy governance in Kenyan secondary schools.

How Do Ethical Considerations Related to the Use of AI Technologies Impact Students' Privacy in Kenyan Secondary Schools?

The integration of AI technologies in Kenyan secondary schools raises critical ethical concerns, particularly in safeguarding student privacy. Scheibner *et al*. (2020) stresses the importance of embedding ethical and legal safeguards, such as encryption, to ensure compliance with privacy standards when implementing AI technologies. Bennett and Raab (2020) further highlight the need for stringent governance and effective implementation, suggesting that ethical issues, such as informed consent and transparency, are often neglected in the rush to adopt new technologies. In Kenya, these considerations are especially relevant as schools increasingly adopt AI systems for administrative and educational purposes. The findings indicate that without clear ethical frameworks, privacy risks for students may escalate, potentially undermining trust in technology. Addressing these risks requires balancing innovation with ethical obligations to protect student data, ensuring AI deployment in schools adheres to principles of accountability and transparency.

What Are the Best Practices for Enhancing Data Protection in the Context of AI Use in Kenyan Secondary Schools?

The findings suggest several best practices that Kenyan secondary schools can adopt to strengthen data protection in of AI use. Rustad and Koenig (2019) advocate for a harmonized regulatory approach, which could guide Kenya in standardizing its data protection practices while considering local needs. Sharma (2019) highlights the challenges organizations face in achieving compliance with rigorous standards such as the GDPR, suggesting that Kenyan schools must prioritize capacity-building initiatives, including staff training and regular audits. Scheibner *et al*. (2020) emphasize the role of advanced technological solutions, such as encryption and secure data storage, in safeguarding sensitive information. Applying these insights, best practices for Kenyan schools should include the adoption of secure technologies, the development of context-specific policies for AI use, and ongoing efforts to enhance awareness and compliance with data protection standards. These measures can help ensure that the integration of AI technologies in schools is both secure and ethically sound.

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 underlines 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.

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 recommendations are proposed. Schools should align their data privacy frameworks with international standards, such as the GDPR, as suggested by Rustad and Koenig (2019), to address inconsistencies and improve protections for student data. Policymakers must adapt these guidelines to suit the local context for practical implementation. Strengthening compliance through regular audits and staff training, as emphasized by Bennett and Raab (2020), is essential to bridge the gap between policy creation and execution. Schools should also invest in advanced data protection technologies, such as encryption and anonymization, to safeguard sensitive information, following the recommendations of Sharma (2019) and Scheibner *et al*. (2020). Ethical considerations must be a priority when deploying AI technologies, with informed consent, transparency, and robust data security measures ensuring trust and accountability. Finally, continuous monitoring and evaluation of data privacy practices are crucial to address emerging challenges and maintain compliance with evolving standards. These steps will significantly enhance data protection and promote the ethical use of AI in Kenyan secondary schools.

References

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.

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.

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

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

Che, C. V. (2024). Analyzing the legal and ethical implications of digital technologies on businesses in Cameroon as a developing country. *Open Access Library Journal, 11*(6), 1-18.

Chikotie, T. T., Watson, B. W., & Watson, L. R. (2023, October). Systems thinking application to ethical and privacy considerations in AI-enabled syndromic surveillance systems: Requirements for under-resourced countries in Southern Africa. In *Pan African Conference on Artificial Intelligence* (pp. 197-218). Cham: Springer Nature Switzerland.

Gaffley, M., Adams, R., & Shyllon, O. (2022). Artificial intelligence. *African Insight.* A research summary of the ethical and human rights implications of AI in Africa.

Gaffley, M., Adams, R., & Shyllon, O. (2022). Artificial intelligence. *African insight.* A research summary of the ethical and human rights implications of AI in Africa.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

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.

Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers, 16*(2), 2577-2587.

James, M. (2024). The ethical and legal implications of using big data and artificial intelligence for public relations campaigns in the United States. *International Journal of Communication and Public Relations, 9*(1), 38-52.

Kisio, B., & wa Teresia, N. (2024). Ethical implications of advanced surveillance technologies on law enforcement: A case study of National Police Service in the County of Nairobi, Kenya. *East African Journal of Information Technology, 7*(1), 68-80.

Kitili, J., & Karanja, N. (2023). The new wave of eHealth: AI and privacy concerns? A case study of Kenya. *Journal of Technology in Health, 15*(3), 199-210.

Kitili, J., & Karanja, N. (2023). The new wave of eHealth: AI and privacy concerns? A case study of Kenya. *Journal of Technology in Health, 15*(3), 199-210.

Kumar, S., & Choudhury, S. (2023). Normative ethics, human rights, and artificial intelligence. *AI and Ethics, 3*(2), 441-450.

Kumbo, L. I., Nkwera, V. S., & Mero, R. F. (2024). Evaluating the ethical practices in developing AI and ML systems in Tanzania. *ABUAD Journal of Engineering Research and Development (AJERD), 7*(2), 340-351.

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.

Liywalii, E. (2023). Artificial intelligence (AI) and children in Africa: A sandboxed childhood and a normative ethics point of view (No. 10967). *EasyChair*.

Miao, Z. (2019). Investigation on human rights ethics in artificial intelligence researches with library literature analysis method. *The Electronic Library, 37*(5), 914-926.

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

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.

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

Sartor, G. (2020). Artificial intelligence and human rights: Between law and ethics. *Maastricht Journal of European and Comparative Law, 27*(6), 705-719.

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

Shaltout, M. A. (2024). Legal aspects on the use of AI in digital identity and authentication in banks, its impact on the digital payment process: Research for investigating the adaptation of open banking concepts in Egypt.

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