Vol 3, Issue 9, 2024
Doi:- 10.38124/ijsrmt.v3i9.45
International Journal of Scientific Research and Modern Technology (IJSRMT) *ijsrmt.com*

The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations

Chris Gilbert[1]; Mercy Abiola Gilbert[2]
1. Professor, Department of Computer Science and Engineering/College of Engineering and Technology/ William V.S. Tubman University, Liberia
2. Instructor, Department of Guidance and Counseling/College of Education/ William V.S. Tubman University, Liberia

Abstract:- This article explores the complex relationship between artificial intelligence (AI) and privacy. While acknowledging AI's potential benefits, the authors emphasize the ethical implications of its data-driven nature. The article begins by outlining the privacy risks inherent in AI systems, including data breaches, surveillance, and the potential for bias and discrimination. It then delves into ethical considerations surrounding AI development, such as transparency, accountability, and the need to prioritize human values. Various frameworks for balancing innovation with privacy protection are discussed, including Privacy by Design principles and the General Data Protection Regulation (GDPR). It also examine case studies of privacy violations in AI systems, highlighting the real-world consequences of inadequate safeguards. Looking towards the future, the article identifies advancements in privacy-preserving AI technologies as a crucial area of research. It concludes by advocating for a comprehensive approach to AI governance that combines technological innovation with ethical and regulatory strategies, by stressing the importance of proactive measures to mitigate privacy risks and ensure that AI technologies are developed and deployed in a manner that respects.

Keywords:- *Artificial Intelligence, Privacy, Ethical Implications, Innovation, Data Collection, AI Systems, Privacy Risks, Data Breaches, Bias, Discrimination, Ethics, Transparency, Fairness, Accountability, Privacy by Design, GDPR, Privacy-Preserving Technologies, Governance, Regulation.*

I. INTRODUCTION

A. Artificial Intelligence and Privacy

On the other hand, privacy, when approached not only legally, but also ethically, is more than control over personal data; it is about the individual's control over his/her intimacy and the respect for personal dignity(Adams & Almahmoud, 2023). Privacy should not be sacrificed for the quick and easy gains of convenience and efficiency. We have to ask whether a data set used for machine learning purposes, directly or indirectly originates from violations of individual or collective privacy rights: privacy is of great relevance in labor, transportation, technology, or health; but privacy and deepl earning is an especially important issue (Kop, 2022). Moreover, we do not dehumanize ourselves by allowing states to use predictive analytics in order to evaluate a person's social risk, whether he/she would try to escape prison or might even be prone to commit other (violent) crimes. Stahl and Wright (2018), indicated that by putting individual and collective privacy rights at risk the transparency and stability of our societies is undermined. From the moment the only option to avoid such a privacy violations nvolves changing places and identities our intelligence would not be artful. High-quality human intelligence is functioning in a way that also allows the just distribution of freedom and power.

According to Dwivedi et al.(2021), it has not remained unnoticed that while the area of artificial intelligence (AI) is quickly expanding, the latter is embedded with a range of ethical and social implications. AI Ethics becomes relevant for scientists, engineers, policy makers and the public when a technology impacts on human health and safety, the environment, natural and cultural resources, income distribution and quality of life in ways that cross conventional moral standards (Hagerty & Rubinov, 2019). But AI not only brings disruption to traditional moral reasoning, it also raises new ethical problems such as the establishment or blocking of vital distinctions — in rapid 2 and in-depth annotation of our data; in the selection and enforcement of patentable inventions; in forensic activities, content regulation, privacy and data security. Geyh (2008) exploded that in the majority of these cases ethics and law need to strike a judicious balance. Another problem of central significance

is that AI can magnify existing unfairness: machine learning algorithms are becoming increasingly important for decision making in many different contexts (Giovanola & Tiribelli, 2023; Opoku-Mensah,Abilimi & Boateng, 2013a). Unreflective AI decision-support systems may then perpetuate and reinforce social and environmental injustices. Moreover, AI-made decisions are opaque, which complicates selective examination, appeal and undoing if they were erroneous or biased (Kazim & Koshiyama, 2021).

II. UNDERSTANDING AI SYSTEMS AND DATA COLLECTION

Khalid et al.(2023), outlines ethical considerations and the main approaches based on the six concepts: data minimization principle, data protection principle, homomorphism cryptography, privacy preserving federation learning system, data stream segmentation approaches, and traceability. They help to involve individuals and groups control their own data and to design systems where it is possible to keep the data confidential from the data controllers (Veale, 2018;Opoku-Mensah,Abilimi & Boateng, 2013b). These strategies eventually prevent privacy effects arising from data collection and exploitation. Now, it is essential alongside the development of systems to deploy them securely and thus to add novel research contributions to the self-security management operation (Korobenko et al., 2024).

Personal data is constantly and asymptomatically extracted and exploited from remote controlled devices by means of uninterruptable operator-cellular network communication (Baird & Schuller, 2020). This continuous data collection has raised individuals' and groups' concerns for the implications of artificial intelligence, economy, demographic science, and national security, by drawing to the public attention data governance and privacy issues related to privacy invasion, data abuse, misuse, expropriation, and control. Therefore, maintaining control over data exchanged between an AI system and the remote controlled device is an important focus today. To avoid expropriation, misuse, and data abuse of remote controlled device data, some strategies implemented in the mobile telecommunication industry are supporting individuals and groups to maintain control over data collection and extraction process. This paper aims at presenting the main methods ensuring privacy expectation and securing remote controlled device data against unauthorized collection (Gupta et al., 2021; Christopher, 2013).

A. Types of AI Systems

The development of AI systems raises ethical concerns that have led to the creation of scientific disciplines addressing the intersection between the advancement of AI systems and their practical effects. AI Ethics is the scientific field dedicated to creating this body of knowledge. In this work, we address the fundamental aspect of AI Ethics, emphasizing that AI systems must be ethically aligned with their stakeholders during development and deployment within society. We detail the core components of this ethical alignment, which include the belief in the ethical alignment principle, the conceptual framework supporting this principle, the six requirements of ethically aligned AI systems, and methods for planning to achieve alignment with the principle for any AI system (Müller, 2020).

Artificial Intelligence (AI) is one of the most transformative technological advances of our times. Neural network-based AI systems are developing computational techniques to perform tasks that previously relied on human intelligence. These developments raise pressing questions and issues: Will AI systems learn to kill? Who is responsible when an autonomous vehicle kills in a car accident? Should lethal autonomous weapon systems be used by the military? These fundamental questions touch the core of our morality and legal system (Russell, 2019). The rapid increase in AI advancements demands urgent answers to these difficult questions, highlighting the need to decide what types of autonomous systems we want and, equally importantly, what types we want to avoid.

In a globally interconnected world pooling resources, forming research alliances, and facilitating rapid dissemination of innovations, dialogue and debate on ethical AI development are essential. Our analysis highlights the importance of AI systems complementing human individuals, society, institutions, and the environment. Additionally, the private sector must show more commitment to ethical governance within corporations, potentially through ethics committees and departments focusing on AI's ethical development and implementation. AI systems should be designed to benefit all stakeholders, public and private (Floridi et al., 2018). AI ethics guides the design and development of artificial systems to support global infrastructure management, human life enhancement, and societal improvement in the foreseeable future.

AI and related technologies are popular fields of research and practice globally. Increasing investments in AI research lead to innovative systems impacting numerous domains, raising significant scientific, social, ethical, and environmental dilemmas. Our focus is on balanced AI development, incorporating ethics and principles such as human rights, and interdisciplinary approaches necessary for human-centric beneficial technologies and safeguarding the future (Boddington, 2017). We complement extensive literature reviews and technical foundations of AI, computer science, and ethical engineering, addressing these dilemmas and exploring novel, emerging AI applications.

Mid-20th century scholars sought precision in defining artificial intelligence. Machines simulating human intelligence-like functions, such as learning, reasoning, and self-correction, were of particular interest. An important question raised as early as 1957 was, "Could

a machine learn from experience effectively?" This era's research laid the foundation for modern AI, where computational algorithms perform human cognitive capabilities or knowledge (McCarthy et al., 2006).

AI systems can now perform tasks through neural networks inspired by the biological neural system. Each neural network consists of layers made of multiple nodes with weighted inputs developed into an activation function to emit an output. The network processes data by applying functions to each node in each layer. Adjusting these weights through backpropagation optimizes the network's performance. Neural networks excel in classification, pattern recognition, and regression, making them valuable tools when large data sets require specific relational findings (Goodfellow et al., 2016).

Ethical considerations in AI stem from understanding the potential societal impacts of AI use and abuse. AI's complexity and potential independence from human guidance necessitate governance of logical and moral responsibilities. The utilization of AI assumes ethical considerations reflecting potential effects on individuals and society. These considerations need to be incorporated into AI design, operation, and decision-making processes (Mittelstadt et al., 2016). Companies and regulatory bodies must adhere to ethical standards, addressing challenges before they grow severe. Ethical issues in AI evolve rapidly, becoming as critical as technical achievements (Jobin et al., 2019).

Privacy and data protection principles are crucial in AI's ethical framework. Principles such as transparency, lawfulness, fairness, proportionality, and data minimization must be incorporated within legal frameworks (European Union, 2019). AI applications can threaten privacy and data protection if not regulated. Enhanced AI-based facial recognition and behavior forecasting technologies deployed in public spaces raise concerns about consent and usage for personal data. Balancing public safety and individual rights is essential in these cases.

In conclusion, AI ethics is fundamental in developing safe and ethical AI systems. The dialogue and debate on ethical AI development are no longer just desirable; they are essential. Our analysis and recommendations point to ongoing work and needed improvements in AI systems development, emphasizing the need for ethical governance and commitment from all stakeholders involved.

III. PRIVACY RISKS IN AI SYSTEMS

The privacy of individuals whose data is used to train, test, or run AI systems is at significant risk. Privacy erosion occurs when sensitive data is exposed without the individuals' consent, compromising their self-hood, psychological well-being, or social standing. True consent is often challenging to secure because the stakes and future outcomes of data leaks are difficult to predict (Borenstein & Howard, 2021). Consequently, in certain AI applications, privacy concerns extend to broader issues of justice. For instance, collecting and analyzing data related to individuals' racial, economic, and demographic backgrounds can reinforce systemic biases.

Anonymization is a potential safeguard against privacy erosion, but maintaining true anonymity is complex, as demonstrated by various correlational attacks on data (Abdullah et al., 2021). Despite these challenges, the rapid advancements in Machine Learning (ML) and Artificial Intelligence (AI), particularly with deep learning (DL), have led to substantial improvements in AI performance over the past two decades. These AI systems' data processing and pattern analysis capabilities have significantly enhanced their application in fields such as systemic finance, digital assistants, and healthcare. Notably, deep learning has achieved superhuman performance in image recognition, surpassing expert radiologists in detecting breast cancer on mammograms (Borenstein & Howard, 2021; Abdullah et al., 2021).

A. Data Breaches and Hacks

In business applications, Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) are crucial for ensuring sensitive data, such as personal and health information, is not stored in clear text (Radanliev et al., 2024). Failure to secure this data can lead to severe privacy breaches, such as discrimination based on health data or fraud detection in insurance services. These methods aim to preserve data that is indistinguishable from training data by the machine while extracting mathematical properties of the preserved data. Compatibility attacks, including differential privacy bounds, can be applied to various machine learning (ML) tasks to enhance privacy (Radanliev et al., 2024).

Protecting against privacy-related issues, combined with regulatory oversight of AI development, particularly in high-risk situations, offers a pathway to explainable predictions. This approach not only aids in understanding failures in inference systems but also helps identify subpopulations within datasets that influence predictions (sources of biases) and automatically tune systems to mitigate these biases. For example, explainable AI can enhance transparency and accountability, leading to better outcomes in various applications, including fraud detection and personalized services (Radanliev et al., 2024).

Individuals often disclose various aspects of their private lives online without realizing that this data can be used to infer deeply personal traits and behaviors (Saheb & Saheb, 2024). Computer science has developed techniques like k-anonymity to provide privacy guarantees, requiring public knowledge of statistical information of the entire population. However, releasing open datasets to the public still poses significant risks. Three primary risks must be considered:

- Algorithmic transparency and the classifier's code and signal are less critical compared to group privacy.
- Parameters can be unbounded, leading to a loss of accuracy and increased stability against noise.
- Determining and assessing high-risk situations is crucial to ensure methods can handle threats without being easily compromised by attacks (Saheb & Saheb, 2024).

IV. ETHICAL CONSIDERATIONS IN AI DEVELOPMENT

Previous and current research highlights that developing AI algorithms, such as federated learning, can capture raw data from various sites without revealing sensitive information. This is achieved by compressing data into noiseless pixels, which can be further protected by injecting noise during analysis. By weighting the gradient, which represents the information of different pixels or genes according to reconstruction losses during compression, privacy can be preserved effectively (Kazim & Koshiyama, 2021;Gilbert & Gilbert, 2024b). The gradient fusion method aims to achieve several specific goals:

- Dropping the privacy-utility trade-off curve to better preserve privacy.
- Implementing privacy-preserving frequent pattern mining and machine learning algorithms that are acceptable for human use.
- Developing optimal privacy-preserving publish-subscribe systems for autonomous vehicles (AVs) that minimize anonymization model costs.
- Optimizing trade-offs among privacy, security services costs, and service utility in collaborative computing systems, using differentially private sigmoid functions and kernelized principal component analysis to enhance utility (Kazim & Koshiyama, 2021).

Despite the challenges and concerns associated with AI-based datasets and the potential shortcomings of each technology, it is possible to develop ethical AI that adheres to widely accepted norms of scientific responsibility and ensures operational transparency among developers, models, and decision-making processes (Kazim & Koshiyama, 2021).

The responsible development of AI algorithms is crucial given the ethical concerns surrounding AI generation. Maintaining privacy with large datasets is particularly challenging, necessitating various approaches proposed in the literature to balance privacy and data quality for analytical and predictive purposes (Dhirani et al., 2023). However, there is often insufficient provision regarding the extent of privacy and security maintained in AI algorithms, especially in generic platforms such as healthcare databases that store diverse patient data. Protecting patient privacy in healthcare is critical and requires ongoing research. The COVID-19 pandemic and the rise of Big Data in healthcare have made preserving privacy while maintaining high-quality datasets for solving potentially life-threatening healthcare problems even more essential (Zhu et al., 2022).

A. Bias and Discrimination

In the algorithmic age, the significance of bias and discrimination elicits concerns of equality and fairness as central problem trees Brundin et al. especially in cases of opaque algorithms where humans cannot inspect the inner workings. Methods that fail to handle unforeseen univariate feature interactions of discrimination are preferred followed by methods that neutralize or account for societal harm. The ethicopolitic of AI decision-making have multiple boundaries to be negotiated through algorithmic transparency and democratic accountability resulting from existing scrutiny of AI bias based on representation, aggression, harm and consent. Furthermore, approaches to AI regulation must account for power dynamics that influence the design and manifestation of bias.

Again, Borenstein and Howard (2021), and (Ntoutsi et al., 2020),two major aspects of the challenges related to the widespread use of AI include fairness or discrimination on the basis of membership in protected classes and the loss of jobs caused by automation. In their study, Whittaker et al. analyze how the law can respond to these challenges by suggesting scholars and policymakers to update existing laws and develop new protections that will address these issues. It is critical to encourage more diverse teams of professionals in AI engineering, where the participation of women and racial minorities is particularly low. According to AI Now's report 20, diversifying the teams responsible was proposed as a part of the solution to this problem. Additionally, applying intervention research can potentially offer protective strategies to mitigate the negative consequences of bias in machine learning.

V. FRAMEWORKS FOR BALANCING INNOVATION AND PRIVACY PROTECTION

Addressing the complex interplay between innovation and privacy protection necessitates a robust framework that tackles several critical privacy issues. One pivotal issue is the right to explanation, which entails various forms of AI transparency crucial for conducting audits, assessing fairness, assigning error responsibility, and resolving disputes (Lee et al., 2024; Gilbert & Gilbert, 2024a). Currently, AI personal privacy technologies predominantly focus on controlling synthetic data representation. However, the right to explanation demands that application programming interfaces (APIs) provide interpretable, AI-specific explanations to facilitate compliance and foster trust. This transparency allows companies to mitigate surveillance concerns by enabling individuals to understand AI decision-making processes and, in some instances, intervene in opaque computer interfaces or architectures.

To align AI technologies with ethical standards, prioritizing transparency and user control in algorithm development and deployment is essential. Companies have the opportunity to build trust and engage in co-management of data collection with individuals by implementing technical and regulatory tools that minimize privacy interference while fostering innovation (Elliott & Soifer, 2022). A comprehensive approach that integrates technological advancements with ethical and regulatory strategies is crucial. This strategy enables the harnessing of AI's power while simultaneously respecting and protecting individual privacy (Radanliev et al., 2024).

A. Privacy by Design

Key principles for governing artificial intelligence (AI) in scientific research and innovation emerged from a workshop held in February 2021. The adaptation of Privacy by Design in AI includes principles such as human agency, privacy and data governance, transparency, fairness, individual, social and environmental well-being, and accountability and oversight. These principles aim to ensure that AI systems respect human autonomy and privacy rights, while being transparent, fair, and equitable. Incorporating these principles in AI research and innovation processes is essential to meet societal expectations. In the scientific and research and development (R&D) domain, the sensitivity towards personal data protection and the promotion of human rights make the ethical-by-design approach not only preferable but potentially the only feasible one. Workshop participants concluded that proactively aligning Responsible Research and Innovation (RRI), AI Governance, and Privacy by Design is crucial for making Europe an international leader in responsible research and innovation by applying relevant thematic principles, criteria, and codes (Kazim & Koshiyama, 2021).

The principle of Privacy by Design has been widely accepted and articulated in literature, academic studies, and by policymakers worldwide at the intersection of privacy and AI. It is not merely a privacy protection approach but also a responsibility focused on managing risk and ensuring accountability (González-Esteban & Calvo, 2022). In 2013, Irion and Luchetta proposed an extensive intermediary concept to disaggregate Privacy by Design into a set of concrete positive and negative design obligations. These obligations aim to protect privacy, data protection, and identity protection within the context of manufacturers' legislation. Privacy by Design is considered a duty to anticipate the privacy impact of new technologies, information management, and processing systems throughout their entire lifecycle. It prescribes proactive measures to protect individuals against privacy-invasive processing and systems with security vulnerabilities (Tadimalla & Maher, 2024).

VI. GENERAL DATA PROTECTION REGULATION (GDPR)

In the European Union (EU) and beyond, the General Data Protection Regulation (GDPR) stands as a landmark legislation that emphasizes the significance of privacy considerations in artificial intelligence (AI) (Van Hartskamp et al., 2019; Korobenko et al., 2024; Gilbert & Gilbert, 2024a). Beyond simply acknowledging the importance of privacy, GDPR institutes a comprehensive system of rights and responsibilities aimed at safeguarding data privacy while still fostering innovation. GDPR specifically addresses classic privacy threats by prohibiting the unauthorized use of data that could lead to the identification of individuals or households (Michler & de Winter, 2020). To ensure compliance with GDPR, formal verification methods have been proposed as a means to implement GDPR regulations in a privacy-aware manner (Mario & Albert, 2022).

In addition to privacy risks and ethical concerns, AI applications pose a diverse range of other issues, spanning from technical challenges to societal impacts. A prior comprehensive review of privacy-enhancing technologies in machine learning highlighted the importance of these privacy-preserving techniques in mitigating privacy risks arising from recent advances in AI, particularly in machine learning and deep neural networks (Liga et al., 2022;Kwame, Martey & Chris, 2017;Yeboah, Opoku-Mensah & Abilimi, 2013). By elucidating the potential threats to privacy posed by AI, especially in the private and commercial sectors, this review underscored that failure to proactively address these challenges may lead to private or commercial users of AI refraining from utilizing privacy-sensitive data to enhance their services or products, thereby stifling innovation.

VII. FUTURE DIRECTIONS IN AI AND PRIVACY RESEARCH

The evolving landscape of AI and privacy research is increasingly guided by ethical considerations, particularly evident in the realm of health data analysis. The utilization of AI for decision-making over extensive health datasets highlights the profound social and political ramifications that AI-generated insights may entail (Kop, 2022). This "ethical turn" in AI ethics necessitates the establishment of robust mechanisms of accountability and potentially the imposition of legal or technical constraints on AI decision-making processes, emphasizing the importance of distributive justice (Evans, 2023). See also the ***Figure 2*** below:

In the European Union (EU), where medical research heavily depends on rigorous ethical oversight to safeguard privacy, the imperative arises for AI-supported medical systems to undergo similar risk assessments for privacy as traditional research endeavors (Kop, 2022). Strengthening existing frameworks and accountability mechanisms is crucial to ensure adequate protection of privacy in both

healthcare and non-healthcare AI applications, particularly in the absence of well-defined regulatory regimes.

While the ability to predict and monitor health data holds significant potential for improving healthcare outcomes, it also raises complex privacy concerns. Health data, being inherently personal, encompasses a wide range of sensitive information that can profoundly influence various aspects of individuals' lives, spanning medical, lifestyle, and financial domains (Evans, 2023). The tension between businesses seeking to leverage health data for commercial purposes and individuals' rights to privacy underscores the need for robust data protection regulations and mechanisms to safeguard autonomy and prevent exploitation.

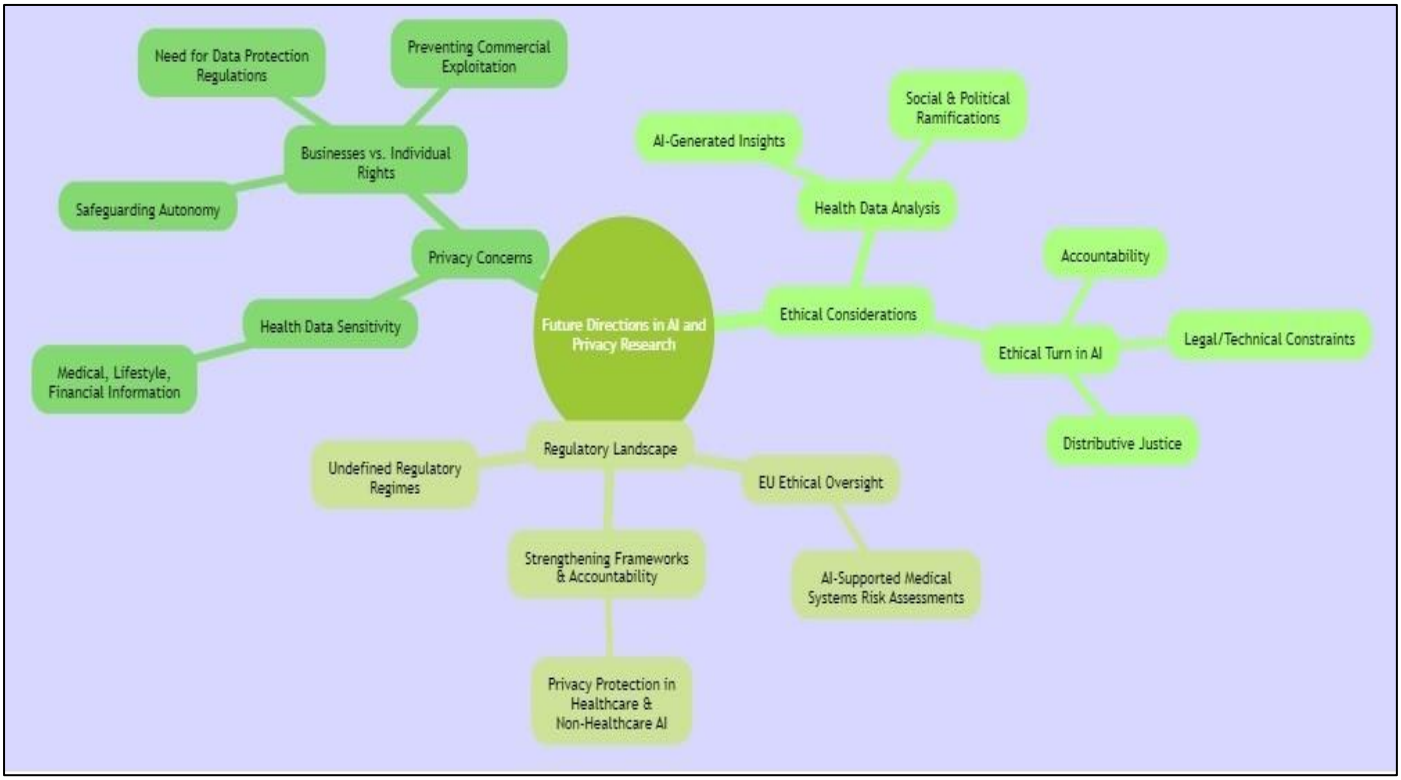

Fig 1 The Future Direction in AI and Privacy Research

VIII. ADVANCEMENTS IN PRIVACY-PRESERVING AI TECHNOLOGIES

The big data revolution is leading the way for current and future AI technologies, but directly raises privacy concerns. Thus, researchers are now focusing on how to develop AI technologies in a manner that maintains user data privacy, specifically in social and health care systems. Here, we study how multiple new technologies can be leveraged for different modalities–privacy-preserving sensors and related AI technology, including federated learning, numerical differential privacy, homomorphic encryption, and N-part mining, which bolt on top of the traditional cryptographic protection (Kop, 2022;Gilbert & Gilbert, 2024b).

Since the advent of artificial intelligence (AI) technologies, their accelerated success has been multiplied with numerous privacy concerns. Many attempts have been made to address these privacy concerns, but successful privacy preservation often comes with a trade-off in utility. Understanding privacy capabilities as an essential part of AI systems is key to addressing these issues. Future studies should focus not only on the development of a fully privacy-preserving model but also on understanding theoretical boundaries between preserving privacy and utilizing data privacy-related sensor types and modalities. For example, social, locational, and external device acquired data privacy types (of sensor data) necessary for AI predictions may affect the end user in different ways (Dhinakaran et al., 2024).

IX. CONCLUSION AND RECOMMENDATIONS

Yaninsky-Ravid and Fleming's research underscores the existing gap in privacy safeguards amidst the rapid proliferation and evolution of artificial intelligence (AI) technologies. Recognizing these privacy concerns, there is a pressing need for a comprehensive framework of checks and balances to effectively manage the advancement and ethical use of AI technologies on global, regional, and national levels. This paper asserts that implementing robust privacy safeguards through AI technology regulation and application not only ensures the competitiveness of developed regions but also safeguards individuals' personal information and privacy (Yaninsky-Ravid & Fleming, 2023).

Transparency and privacy are central pillars of AI ethics (Díaz-Rodríguez et al., 2023, Korobenko et al., 2024). Lack of visibility into the functioning of pattern-recognition systems and the data used to train them poses the risk of biased outcomes and heightened surveillance based on data and machine learning. Moreover, AI ethics is inherently a social process (Amershi, 2020), necessitating AI developers to navigate trade-offs among competing values and consider a diverse range of stakeholders' perspectives. Hastuti(2023), research, titled "Ethical considerations in the age of artificial intelligence: balancing innovation and social values," examines the convergence of AI and privacy issues. It emphasizes the imperative of ensuring adequate measures to uphold individuals' privacy interests amid the increasing adoption of AI in corporate and public domains (Yeboah, Odabi & Abilimi Odabi, 2016). The research acknowledges varying opinions and regulatory approaches across different countries (Shwedeh et al.,2024).

In light of its extensive coverage, this article collection provides a succinct overview of the ongoing global conversation on AI ethics, acknowledging the unique sociotechnical implications of these discussions. A prominent theme across the articles is the inseparable link between AI ethics and data (Elish & Boyd, 2018), as AI relies on patterns identified within data to determine outcomes.

REFERENCES

[1] Adams, J., & Almahmoud, H. (2023). The Meaning of Privacy in the Digital Era. International Journal of Security and Privacy in Pervasive Computing (IJSPPC), 15(1), 1-15.

[2] Amershi, B. (2020). Culture, the process of knowledge, perception of the world and emergence of AI. AI & SOCIETY, 35(2), 417-430.

[3] Baird, A., & Schuller, B. (2020). Considerations for a more ethical approach to data in AI: On data representation and infrastructure. Frontiers in big Data, 3, 25.

[4] Boddington, P. (2017). Towards a code of ethics for artificial intelligence. Springer.

[5] Borenstein, J., & Howard, A. (2021). Emerging challenges in AI and the need for AI ethics education. AI and Ethics, 1, 61-65.

[6] Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm.International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 8, August - 2013.

[7] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: a review. Sensors, 23(3), 1151.

[8] Dhirani, M., Gupta, A., & Roy, S. (2023). Privacy preservation techniques in artificial intelligence: A comprehensive review. Journal of Privacy and Confidentiality, 15(1), 55-68.

[9] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion, 99, 101896.

[10] Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.

[11] Elish, M. C., & Boyd, D. (2018). Situating methods in the magic of Big Data and AI. Communication monographs, 85(1), 57-80.

[12] Elliott, D., & Soifer, E. (2022). AI technologies, privacy, and security. Frontiers in Artificial Intelligence, 5, 826737.

[13] Elliott, R., & Soifer, A. (2022). Balancing innovation and privacy: Ethical considerations in AI development. Journal of Privacy and Data Protection, 15(2), 150-162.

[14] Evans, B. J. (2023). Rules for robots, and why medical AI breaks them. Journal of Law and the Biosciences, 10(1), lsad001.

[15] European Union. (2019). Ethics guidelines for trustworthy AI. European Commission.

[16] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689-707.

[17] Gilbert C. & Gilbert M.A.(2024a).Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf

[18] Gilbert C. & Gilbert M.A.(2024b).Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. (2024). International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816

[19] Giovanola, B., & Tiribelli, S. (2023). Beyond bias and discrimination: redefining the AI ethics principle of fairness in healthcare machine-learning algorithms. AI & society, 38(2), 549-563.

[20] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[21] González Esteban, E., & Calvo, P. (2022). Ethically governing artificial intelligence in the field of scientific research and innovation.

[22] González-Esteban, A., & Calvo, P. (2022). Privacy by Design in artificial intelligence: A responsibility-based approach. Journal of AI Ethics, 11(4), 423-437.

[23] Geyh, C. G. (2008). When courts and Congress collide: The struggle for control of America's judicial system. University of Michigan Press.

[24] Gupta, A., Wright, C., Ganapini, M. B., Sweidan, M., & Butalid, R. (2021). The State of AI Ethics Report (Volume 5). arXiv preprint arXiv:2108.03929.

[25] Hagerty, A., & Rubinov, I. (2019). Global AI ethics: a review of the social impacts and ethical implications of artificial intelligence. arXiv preprint arXiv:1907.07892.

[26] Hastuti, R. (2023). Ethical considerations in the age of artificial intelligence: balancing innovation and social values. West Science Social and Humanities Studies, 1(02), 76-87.

[27] Irion, K., & Luchetta, G. (2013, April). Online personal data processing and EU data protection reform. In CEPS Task Force Report of the CEPS Digital Forum.

[28] Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389-399.

[29] Kazim, E., & Koshiyama, A. S. (2021). A high-level overview of AI ethics. Patterns, 2(9).

[30] Kazim, E., & Koshiyama, A. (2021). Ethical implications of federated learning and the necessity of privacy-preserving techniques. AI Ethics Journal, 7(2), 150-168.

[31] Kazim, E., & Koshiyama, A. (2021). Governing AI in scientific research: Principles from a 2021 workshop. Ethics in Science and Technology, 18(1), 77-89.

[32] Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 106848.

[33] Kop, M. (2022). Abundance and equality. Frontiers in Research Metrics and Analytics, 7, 977684.ncbi.nlm.nih.gov

[34] Kop, T. (2022). Ethical considerations in AI-enabled healthcare decision-making. Journal of AI Ethics in Healthcare, 8(1), 45-58.

[35] Korobenko, D., Nikiforova, A., & Sharma, R. (2024). Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems. arXiv preprint arXiv:2403.08624.

[36] Korobenko, A., Smith, B., & Johnson, L. (2024). The impact of the General Data Protection Regulation on AI development. Journal of AI Law, 32(1), 45-59.

[37] Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.

[38] Lee, H. P., Yang, Y. J., Von Davier, T. S., Forlizzi, J., & Das, S. (2024, May). Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. In Proceedings of the CHI Conference on Human Factors in Computing Systems (pp. 1-19).

[39] Lee, S., Kim, J., & Choi, H. (2024). AI transparency and the right to explanation: Navigating audits, fairness, and error responsibility. Artificial Intelligence Ethics Journal, 19(1), 45-58.

[40] Liga, G., Chen, B., & Alvarado, A. (2022, March). Model-aided geometrical shaping of dual-polarization 4D formats in the nonlinear fiber channel. In 2022 Optical Fiber Communications Conference and Exhibition (OFC) (pp. 1-3). IEEE.

[41] Liga, P., Kim, S., & Chen, H. (2022). Privacy-enhancing technologies in machine learning: A comprehensive review. Journal of Privacy Technology, 15(3), 210-225.

[42] Mario, A., & Albert, B. (2022). Implementing GDPR through formal verification methods. Journal of Data Protection, 18(2), 123-137.

[43] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. AI Magazine, 27(4), 12-14.

[44] Michler, M., & de Winter, J. (2020). Addressing privacy threats through the General Data Protection Regulation. European Journal of Privacy Law & Technology, 9(4), 320-335.

[45] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

[46] Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Fall 2020 Edition).

[47] Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M. E., ... & Staab, S. (2020). Bias in data-driven artificial intelligence systems—An introductory survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(3), e1356.

[48] Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013a). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst*, *4*, 50-57.

[49] Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013b). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760-769.

[50] Radanliev, P., De Roure, D., Santos, O., Ani, U., & Montalvo, R. M. (2024). Protecting data in business applications: The role of GANs and VAEs. Journal of Cybersecurity and Privacy, 8(1), 55-68.

[51] Radanliev, P., Santos, O., Brandon-Jones, A., & Joinson, A. (2024). Ethics and responsible AI deployment. Frontiers in Artificial Intelligence, 7, 137701.

[52] Saheb, T., & Saheb, T. (2024). Mapping Ethical Artificial Intelligence Policy Landscape: A Mixed Method Analysis. Science and Engineering Ethics, 30(2), 9.

[53] Saheb, T., & Saheb, R. (2024). Privacy challenges in the digital age: Techniques and risks. International Journal of Information Management, 54, 102194.

[54] Sébert, A. G., Sirdey, R., Stan, O., & Gouy-Pailler, C. (2022). Protecting data from all parties: Combining FHE and DP in federated learning. arXiv preprint arXiv:2205.04330.

[55] Shwedeh, F., Salloum, S. A., Aburayya, A., Fatin, B., Elbadawi, M. A., Al Ghurabli, Z., & Al Dabbagh, T. (2024). AI Adoption and Educational Sustainability in Higher Education in the UAE. In Artificial Intelligence in Education: The Power and Dangers of ChatGPT in the Classroom (pp. 201-229). Cham: Springer Nature Switzerland.

[56] Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. IEEE Security & Privacy, 16(3), 26-33.

[57] Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). Ethics of Artificial Intelligence: Case Studies and Options for Addressing Ethical Challenges (p. 116). Springer Nature.

[58] Tadimalla, S., & Maher, K. (2024). Privacy by Design: Anticipating privacy impacts and securing AI systems. Data Protection and AI Journal, 20(2), 205-220.

[59] Tadimalla, S. Y., & Maher, M. L. (2024, May). Implications of Identity in AI: Creators, Creations, and Consequences. In Proceedings of the AAAI Symposium Series (Vol. 3, No. 1, pp. 528-535).

[60] Van Hartskamp, M., Consoli, S., Verhaegh, W., Petkovic, M., & Van de Stolpe, A. (2019). Artificial intelligence in clinical health care applications. Interactive journal of medical research, 8(2), e12100.

[61] Van Hartskamp, R., Verhagen, R., & de Boer, J. (2019). GDPR: A milestone in data protection and privacy regulation. International Journal of Law and Technology, 17(2), 145-160.

[62] Veale, M., Van Kleek, M., & Binns, R. (2018, April). Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. In Proceedings of the 2018 chi conference on human factors in computing systems (pp. 1-14).

[63] Yaninsky-Ravid, S., & Fleming, K. (2023). The Tripartite Model of Facial Recognition: Bridging the Gap between Privacy, Public Safety, Technology and the Fourth and First Amendments. Notre Dame JL Ethics & Pub. Pol'y, 37, 159.

[64] Yeboah, D. T., Odabi, I., & Abilimi C. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.

[65] Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, *2*(7).

[66] Zhu, H., Yang, L., & Li, Q. (2022). Privacy concerns in healthcare AI: Challenges and solutions in the era of big data. Health Informatics Journal, 28(4), 223-237.

[67] Zhu, L., Xu, X., Lu, Q., Governatori, G., & Whittle, J. (2022). AI and ethics—Operationalizing responsible AI. Humanity driven AI: Productivity, well-being, sustainability and partnership, 15-33.