Impact factor: 3.59

LOGAN JOURNAL OF EDUCATIONAL RESEARCH AND INNOVATION

11(1) 2024 LJERI

ISSN: 3067-1590

THE INTERSECTION OF ARTIFICIAL INTELLIGENCE AND DATA PRIVACY: EVALUATING LEGAL FRAMEWORKS AND TECHNOLOGICAL SOLUTIONS

[1]Ayodele Emmanuel Adebayo and [2]Ngozi Uchechi Okafor

[1]Department of Jurisprudence and International Law, Faculty of Law, Ekiti State University, Ado-Ekiti

[2]Data Privacy and AI Governance Counsel

Abstract: This paper examined the dual objectives of fostering innovation through AI while ensuring robust data privacy. The paper adopted the doctrinal method of research by relying on both primary and secondary sources of information or data. Primarily, it utilises a legal approach using data such as the European Union Artificial Intelligence Act, the General Data Protection Regulation, the California Consumer Protection Act and the Nigeria Data Protection Act. The secondary sources of data used include textbooks, online articles in learned journals, relevant materials from the internet, magazines, newspapers, other periodicals, dictionaries and reports. The study found that a multi-faceted approach is necessary to navigate the intersection of AI and data privacy, ensuring that technological progress does not compromise individual rights and trust in AI systems and finally make recommendations which include technical solutions such as differential privacy, federated learning, and homomorphic encryption which aim to balance data utility and privacy

Keywords: Data privacy, AI governance, Technology law, Innovation, Security

1.0 Introduction

Artificial intelligence (AI) is, simply put, a technology that allows machines and computer applications to mimic human intelligence, learning from experience via iterative processing and algorithmic training, it is a form of intelligence that is used to solve problems, come up with solutions, answer questions, make predictions, or offer strategic suggestions.[1] AI is transforming industries and reshaping the future with its remarkable capabilities in data analysis, automation, and decision-making. From personalized recommendations on streaming platforms to predictive analytics in healthcare, AI is driving innovation at an unprecedented pace. However, this rapid advancement brings with it significant concerns about data privacy. AI systems rely heavily on large datasets, often containing sensitive personal information, raising questions about how to balance the benefits of AI with the need to protect individual privacy. The intersection of AI and data privacy is a complex and evolving landscape. On one hand, AI's ability to process vast amounts of data enables breakthroughs in various fields, enhancing efficiency, accuracy, and personalization. On the other hand, the collection, storage, and analysis of

personal data by AI systems pose risks such as unauthorized access, misuse of information, and erosion of privacy. Striking a balance between fostering innovation in AI and ensuring robust data protection is a critical challenge for policymakers, technologists, and society as a whole. To address these challenges, it is essential to understand the principles of data privacy and the specific ways in which AI impacts these principles. This involves examining current data privacy laws, exploring ethical considerations, and developing frameworks that promote responsible AI use. Additionally, organizations must adopt privacy-enhancing technologies and practices, such as data anonymization, encryption, and transparent data handling policies, to mitigate privacy risks while leveraging AI's full potential. In this context, the ongoing dialogue between innovation and regulation becomes crucial. Governments and regulatory bodies worldwide are drafting and enacting laws and guidelines to protect data privacy without stifling technological advancement. Meanwhile, AI researchers and developers are exploring ways to integrate privacy-preserving techniques into AI systems from the ground up. This synergy between regulation and innovation aims to create an environment where AI can thrive responsibly, safeguarding individuals' rights and fostering trust in AI technologies. The journey towards balancing AI innovation with data privacy protection is ongoing and requires collaboration across multiple stakeholders. By addressing privacy concerns proactively and ethically, we can harness the power of AI to improve lives while respecting and protecting the fundamental right to privacy. This paper discusses the concept of Artificial Intelligence Governance, the interrelationship between AI and the use of data, and the ethical considerations in the use of data by AI, it analyses the current legal and institutional framework for the protection of data as it relates to its use by AI and make recommendations for further enhancement on the use of AI and the protection of data privacy.

2.0 Conceptual Analysis

2.1 Artificial Intelligence

Artificial Intelligence refers to the simulation of human intelligence processes by machines, particularly computer systems. These processes include learning, that is, the acquisition of information and rules for using the information, reasoning, that is, using rules to reach approximate or definite conclusions, and self-correction. AI encompasses a wide range of technologies and applications, all aimed at enabling machines to perform tasks that typically require human intelligence. Systems with artificial intelligence use data and algorithms to function. First, in a procedure called training, vast amounts of data are gathered and fed into mathematical models, or algorithms, which utilise the data to identify patterns and provide predictions. After training, algorithms are used in a variety of applications, where they continuously absorb new information and adjust to suit it. As a result, AI systems can eventually carry out difficult tasks like data analysis, language processing, and image identification with increased efficiency and accuracy. AI is applicable in virtually all aspects of professional and non-professional occupation2.2 Data Privacy to understand data privacy or data protection, it is imperative to have an understanding of what data is in this context. Data in this sense refers to a set of information about a person either expressly given or learnt through the activities engaged in by such person. Data is given, for instance, when a person voluntarily supplies their information by filling out a form, through an interview or by publishing such information, it is learnt where a person’s pattern of activities is used to determine some aspect of his life.

Data privacy refers to the right of an individual to protect sensitive information about him or information which such individual wishes to protect from the public from unauthorised access, use, or disclosure, ensuring that individuals have control over their personal data.

2.3 Data Protection

Data protection encompasses measures to safeguard data integrity, confidentiality, and availability against various threats such as cyberattacks, data breaches, and malicious activities. Where vast amounts of data are

generated, stored, and transmitted, ensuring robust data privacy and security measures is of utmost importance. These measures not only protect sensitive information but also uphold trust between organizations and their customers, comply with regulatory requirements, and mitigate financial and reputational risks associated with data breaches. Data protection is the duty of the organization, body or persons who collect data from another party, they are vested with the duty to protect the data being supplied by such other party from any use to which consent have not been given by the owner. Thus, where through the negligence or otherwise of the organization, data supplied by another party got used for a purpose for which it has not been approved, such organization may be liable to the extent of the use.

3.0 Literature Review

The performance of the AI and the veracity of its outputs are directly influenced by the amount and quality of training data imputed. For AI to effectively learn and imitate patterns, they need large, diverse datasets. Depending on the application, the data might be anything from text and pictures to more intricate data types like biometric data. Although useful, there is an inherent risk to privacy when this data incorporates personal information and maintaining the delicate Balance between innovation and security requires an understanding of the relationship between Artificial Intelligence (AI) and data privacy. Nguyen explored the current context surrounding AI and privacy, and the importance of maintaining control over data, highlighting the importance of protecting individuals' sensitive information such as respecting individual rights, building trust and social acceptance, and in order to be in compliance with regulations. The author recommends potential solutions such as assessing the system's decision-making processes to identify any potential biases or errors, monitoring the AI system's accuracy and other attributes over time to help identify potential issues or deviations, and ensuring that the AI system is fair, unbiased, and effective in solving real problems. According to Cate and Dockery, while compliance with existing data protection laws is important, it is imperative to confront the issue of privacy in the use of AI with a better longterm approach which will be to see the challenges presented by AI as another wake-up call that our current approach to data protection is growingly outdated, archaic and progressively ineffective. With this understanding, the author asserts that it is data protection law that must be improved if it is to protect privacy, effectively address the challenges presented by AI, and avoid creating unnecessary, bureaucratic barriers to AI's benefits. The authors recommend five areas of necessary reforms which are shifting from individual consent to data stewardship, a more systemic and well-developed use of risk management, a greater focus on data uses and impacts, a framework of harms, and transparency and redress. Rayhan and Rayhan conducted an in-depth study into the concept of AI and data privacy to understand the historical development of AI, its ethical implications, and the legal frameworks guiding its deployment. Using real-world case studies, their study analyzed instances where AI had both advanced and threatened human rights, one of such threats discussed is biases embedded in AI algorithms and that the reliance on biased historical data can perpetuate discrimination, leading to unfair treatment and decisions in various domains. The authors recommend the need for explainable and transparent AI, stressing the importance of ethically driven development and responsible deployment through a comprehensive re-examination of international and national regulatory efforts. Devineni explores the transformative impact of Artificial intelligence on data privacy and security by discussing traditional AI methodologies and their associated shortcomings. The discourse revolves around how AI with its 'automation and anomaly identification capabilities is transforming this field' and practical examples of real-world applications of AI in banking and health care to give an insight into how AI can be integrated into the security system, there are further discussions on ethical concerns that despite the immense benefits that may be derived from AI there is a significant concern on potential biases, surveillance energy as an Issue and data handling

issues is performed to have a comprehensive understanding of AI. The author underscores the significance of AI in progressing data privacy and security.

4.0 Innovations and Artificial Intelligence

From the medical industry, customer services, education, finance, and human resources to manufacturing, security, legal services etc. AI has shown tremendous reformative capabilities through innovations that are not only transformative but also helpful in achieving the core goals of each field in which it has been applied. Several types of AI that are used in these fields include Natural Language Processing (NLP) which is used to interpret human language, translate content from one language to another, and understand request from users of assistants like Siri, Alexa, Cortana, etc. Other types are Machine Learning, Deep Learning, and Large Language Models. Machine Learning focuses on using data and algorithms to enable AI to imitate the way humans learn, gradually improving its accuracy while Deep Learning also uses data, it recognises complex patterns in pictures, sounds, text, and other data to generate accurate insights and predictions. Deep learning methods can automate tasks that typically require human intelligence, such as the description of images or transcribing a sound file into text. Large Language Models, on the other hand, make use of both ML and DL to process data and commands, it is used mostly in generative AI models and has the ability to structure responses in real-time. Some AI innovations in different fields of endeavor are discussed below in healthcare, AI is used in the diagnosis of several diseases by ML systems which were developed to detect, identify, and quantify microorganisms, diagnose and classify diseases, and predict clinical outcomes. Clinical laboratories have also made use of AI in automated techniques in blood cultures, susceptibility testing, and molecular platforms. AI has emerged as a valuable tool in advancing personalized treatment, as it offers the potential to analyze complex datasets, predict outcomes, and optimise treatment strategies. It is also capable of optimizing drugs according to patients' needs, thus prioritizing the health and safety of the patient by analyzing the data supplied. AI has been used in population health management, virtual healthcare assistant, mental health support, enhancing patient education and mitigating healthcare provider burnout. With the myriad of the usefulness of AI in healthcare comes its challenges, in the age of digital healthcare transformation, AI-driven systems are increasingly at the forefront of medical innovation which is primarily driven by data. The integration of AI in healthcare raises complex privacy challenges, especially in the area of data control and usage by private establishments. The increase in the handling of sensitive patient data by AI raises concerns regarding the management of these information by private entities. The potential for misuse or unauthorized exploitation of health data requires the establishment of transparent and accountable data governance frameworks that respect patient privacy. Customer Service Management has not remained the same since the integration of AI, customer segmentation is used by companies to fine-tune their strategies in the field of Marketing by classifying consumers into appropriate groups based on their demographics, needs and interests using Natural Language Processing which derives insights from consumer feedback, reviews, and social media interactions, assisting firms in understanding sentiment and feedback, improved personalisation, increased customer retention, and efficient resource allocation. AI is used in personalised marketing and customer engagement to improve conversion rates and revenue per customer and encourage customer loyalty and satisfaction. Chatbots powered by AI have transformed customer service by giving rapid replies and tailored assistance. These chatbots comprehend and reply to user inquiries using natural language processing. However, with these advancements, CRM systems powered by AI depend on massive volumes of consumer data. It is critical to ensure the privacy and security of this dat

AI has been used in legal practice for legal research and discovery to retrieve relevant case law, statutes, regulations, and legal articles to support attorneys in building strong legal arguments and staying up to date with

legal developments. It is also used in document automation, Virtual assistants equipped with NLP can automate repetitive and time-consuming operations like document review, contract analysis and generating legal documents, saving time, and reducing the risk of errors. Additionally, AI in predictive legal analysis examines past data to foresee case outcomes. However, among the various challenges posed by the use of AI in legal practice is the challenge of keeping client data private, integrating AI technologies into legal practice raises challenges related to privacy, confidentiality, and compliance with data protection laws. AI often requires access to sensitive legal data and documents. Ensuring proper data protection and preventing unauthorised access is crucial to maintaining client confidentiality and complying with privacy regulations. AI in Finance is used to improve credit decisions by helping lenders and credit-rating institutions assess a consumer's behaviour and verify their ability to repay a loan. It helps identify threats to financial institutions and help meet compliance obligations, AI-enabled compliance technology can reduce the cost for financial service providers to meet their KnowYour-Customer (KYC) requirements and decrease false positives generated in banks' monitoring efforts by sifting through millions of transactions quickly to spot signs of crime, establish links, detect anomalies, and crosscheck against external databases to establish identity using a diverse range of parameters; and it is also used to address financing gaps faced by businesses in emerging markets. AI in Security has proven to be advantageous as it is used in multiple fields to ensure security. One of its functions in security is threat detection by analysing patterns and identifying unusual activities that may lead to potential problems. With intrusion detection and prevention systems, AI can identify and respond to threats as soon as they are detected, thus, it prevents incidents And mitigates damage and loss. AI security also enables organisations to take a more proactive approach to cybersecurity by using historical data to predict future cyber threats and identify vulnerabilities.

5.0 Analysis of Legal Framework on Artificial Intelligence Governance and Data Protection 5.1 the European Union Artificial Intelligence Act

In April 2021, the European Commission presented the first EU regulatory framework for artificial intelligence. It states that AI systems that can be employed in a variety of applications are evaluated and classified based on the risk they bring to users. The varying risk levels will result in more or less regulation. The underlying premise of the bill was to regulate AI based on its capacity to cause harm. The Act outlined various AI use cases and applications and then classified them with an appropriate degree of AI risk from minimal to high. Some AI systems were deemed to have an unacceptable level of risk and would be banned outright, except for a few for law enforcement. These included:

a) AI systems deploying subliminal techniques
b) AI practices exploiting vulnerabilities
c) Social scoring systems
d) 'Real-time' remote biometric identification systems

Risks are categorised into unacceptable risks, high risks, limited risks, and minimal or no risk. Unacceptable risk AI systems are prohibited because they are deemed a threat to human safety. Amongst these are: Cognitive behavioural manipulation of individuals or particularly vulnerable groups, for example, voice-activated toys that incite dangerous behaviour in children; Social scoring which is the process of categorising individuals according to their socioeconomic background, behaviour, or personal traits; People's biometric identification and classification; and Biometric identification systems that operate in real-time and remotely, such as facial recognition. Some exceptions are, however, allowed for the purpose of law enforcement, for example, Real-time remote biometric identification systems will be permitted in a limited number of serious cases. AI systems that negatively affect safety or fundamental rights are considered high risk and All AI systems with high risk are to

be assessed before it's released to the public this assessment shall continue throughout their lifecycle. The Act grant people the right to file complaints about AI systems to designated national authorities. AI Systems with a limited risk, are systems that pose risk to individuals but with limited impact, and therefore only required to fulfil specific transparency obligations. Examples include chatbots, which means that the user must be informed that they are interacting with a machine rather than a human. AI systems with no or minimal risks are systems that will have no additional obligations for these AI systems, such as AI-enabled video games or spam filters. According to the EU Commission, the majority of the AI systems will fall within the category of minimal or no risk.

5.2 The European Union General Data Protection Regulation (GDPR) [28]

The GDPR is the highest form of regulation of Data in the world, one of the purposes of the GDPR is to protect individuals' fundamental rights and freedoms, particularly their right to the protection of their personal data, it is an extension of the right to one's private life as laid down in the European Convention on Human Rights (ECHR). In order to prevent obstacles to the free flow of personal data throughout the Union, it also aims to establish a consistent and harmonized level of personal data protection throughout the EU. This is made possible by the regulation's direct application in each of the member states as well as the uniform application of the rules across the Union. The Regulation lays down rules relating to the protection of natural persons concerning the processing of personal data, it laid down rules relating to the free movement of personal data, it protects fundamental rights and freedoms of natural persons and in particular, their right to the protection of personal data, the regulation further made provision that the free movement of personal data within the Union shall not be hindered due to the protection of personal data.[30] The Regulation applies to the processing of personal data wholly or partly by automated means and non-automated means of personal data which form part of a filing system or are intended to form part of a filing system by an establishment referred to as 'controller' or 'processor' in the territory of the Union, regardless of whether the processing takes place in the Union or not, where the processing activities are related to the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the Union. The Regulation made provision for the rights of individuals to the protection of their data and the duties or obligations of businesses that collect and use data to protect such data. A controller of data is only allowed to process data lawfully, this means compliance with the provision of the regulation by being transparent, use for legitimate purposes only and collection of data that are only necessary and adequate. Processing is deemed to be lawful where such processing is done with the consent of the 'data subject', where it is necessary for compliance with legal Obligation, to protect the interest of the data subject or a third party, or where it is necessary to process such data in the interest of the public. Consent by the data subject is however not an absolute or total surrender of their interest in their personal data, the data subject retain the right to withdraw consent at any time, the withdrawal shall not nullify any process that has been done by the controller or processor. The controller on the other hand is obligated to ensure that the data subject is notified of the use to which the data will be put, notify the data subject of its identity and its contact details, the purpose of the processing and details of the recipients of the data. The Regulation provided data subjects with various rights which include the right to rectify inaccurate data without delay upon request and to complete any incomplete data supplied to the controller, right to erasure, right to restrict the processing of data, right to be notified of any alteration made to personal data by the controller, right to port data, and right to object.

5.3 The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act is a data privacy law that enhances privacy rights and consumer protection for residents of California. The Act applies to most businesses that process the personal data of California

residents, it gives California residents a certain amount of control over the personal data that businesses collect about them. The CCPA made it an obligation for businesses to disclose their data collection practices, including the categories of personal information collected, the sources of the information, the business or commercial purpose for collecting the information, and the categories of third parties with whom the information is shared. It is a requirement, for businesses, to implement reasonable security measures to protect consumer data. Consumers' rights are equally protected, these include the right to know, that is, consumers have the right to know what personal information is being collected about them, the purposes for which it is being used, and with whom it is being shared; right to delete, consumers can request the deletion of their personal information held by businesses; right to opt-out, consumers have the right to opt-out of the sale of their personal information; and right to non-discrimination, that is consumers are protected from discrimination for exercising their privacy rights under the CCPA.

5.4 The Illinois Biometric Information Privacy Act (BIPA)

The law requires entities, businesses or bodies that use and store biometric identifiers to comply with specific requirements for the protection of biometric data collected by such entities. The law also provides a private right of action for recovering statutory damages when the requirements are not complied with. According to BIPA, biometrics are unlike other unique identifiers used to access finances or sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. BIPA also defines a "biometric identifier," in part, as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

5.5 The Nigerian Data Protection Act[51] (NDPA)

The NDPA was enacted to safeguard the fundamental rights and freedoms, and the interests of data subjects, to provide for the regulation of the processing of personal data; the promotion of data processing practices that safeguard the security of personal data and privacy of data subjects; to ensure that personal data is processed in a fair, lawful and accountable manner; to protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights; to ensure that data controllers and data processors fulfil their obligations to data subjects; to establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors; and to strengthen the legal foundations of the national digital economy. The Act is applicable to a controller who is resident in Nigeria and processes data in Nigeria or who neither resides in Nigeria nor processes data in Nigeria but processes data of Nigerians. The NDPA draws heavily from the European Union GDPR in terms of the rights of data subject and obligations of controller and processor. The Act provided for the rights of data to have their data protected and secured and the duties of controllers that collect and use data to protect such data. A controller of data is only allowed to process data lawfully, this means compliance with the provision of the regulation by being transparent, use for legitimate purposes only and collection of data that are only necessary and adequate. Processing is deemed to be lawful where such processing is done with the consent of the data subject, where it is necessary for compliance with legal obligation, to protect the interest of the data subject or a third party, or where it is necessary to process such data in the interest of the public. Consent by the data subject is however not an absolute or total surrender of their interest in their personal data, the data subject retains the right to withdraw consent at any time, and the withdrawal shall not nullify any process that has been done by the controller or processor. The controller on the other hand is obligated to ensure that the data subject is notified of

the use to which the data will be put as the burden of proof rests on the data controller to establish that the data subject was notified.

6.0 Analysis of Technical Regulations for Data Privacy

While the private data never leaves its owner, the exchanged models are prone to memorisation of the private training dataset. Some sensitive information may be inferred from the shared information using well-known attacks like gradient inversion, reconstruction attacks, membership inference, and property inference attacks. One way to mitigate this attack is to use privacy-preserving techniques like differential privacy (DP) and homomorphic encryption (HE). Such may be in the form of technical solutions as follows:

1. Federated Learning

Federated Learning (FL) is a machine learning setting where many clients collaborate to train a centralised machine learning model. Only updates required for immediate aggregation are communicated with the central server; raw data from each client is kept locally and is not shared with third parties.

2. Homomorphic Encryption

While homomorphic encryption (HE) allows computations over an encrypted domain, it is a promising option for joint model training in FL that involves collaboration. HE can be used in the FL framework in a variety of ways. Using HIM in FL to conceal client updates from the server is one use case. The server performs the aggregations in the encrypted domain and only accesses the final result instead of accessing the client's updates directly. An extra layer of protection against data breaches and spying is offered by this method. By encrypting the changes, the raw data and the model updates will remain unreadable even in the unlikely event that someone uninvited intercepts the data.

3. Differential Privacy

Differential privacy (DP) is a widely used standard to guarantee privacy in data analysisThe basic idea behind DP is to examine a thought experiment where we compare the behavior of an algorithm on a real dataset to that of a hypothetical dataset where one person's record has been added or removed. These two datasets are considered "neighbours" in the dataset space. Hence, we say that an algorithm is differentially private if running the algorithm on two neighbouring datasets yields roughly the same distribution of outcomes. In other words, differential privacy ensures that the outcomes of 'Data A' are approximately the same whether or not the person 'Data B' joins the dataset.

7.0 The Interplay between AI Governance and Data Protection Laws

With the evolution of AI, its applicability to all spheres of human work and its capability in the usage of data, it is imperative to analyse the interplay between AI and Data Privacy and Consequentially figure out how the application of AI in our daily lives will not lead to data loss, infringement on citizen's data privacy and how AI governance has, so far, been a useful instrument in the protection of data and to ensure that the development and deployment of AI technologies are ethical, transparent, and respect individuals' privacy rights. AI governance refers to the control and regulation of the usage of AI systems, frameworks, regulations, standards, and legal requirements put in place to safeguard people's fundamental rights, particularly their right to data privacy. Thus, since AI systems handle personal data processing, they must also abide by current data protection rules. Data quality and data privacy are of utmost importance in AI applications in order to generate accurate and reliable results, to gain users' trust and confidence in AI applications, for addressing bias and ensuring fairness in AI, enabling accurate data sharing and collaboration between organisations, and to compliance with regulations. AI systems usually require huge amounts of data to function effectively. Data protection laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the US set

out principles that AI systems must adhere to. AI systems are required to process data in a manner that is lawful, fair, and transparent to the data subjects. Data shouldn't be processed in a way that is inconsistent with its intended uses; instead, it should be gathered with clear, stated, and legitimate objectives in mind. AI systems should only gather information that is required for the tasks for which they are designed. Ensuring the accuracy and timeliness of the data that AI systems use. Personal data should be retained for only as long as it's required for the reasons for which it's processed. To protect data, appropriate security measures must be implemented.

8.0 Challenges of Data Privacy and Protection in the Usage of AI

Data is the foundation of AI. In a similar vein, it's increasingly obvious that data governance forms the basis of AI governance. The term "utility-privacy trade-off" suggests that there is undoubtedly a conflict between protecting privacy and mining user data for useful insights. However, achieving a balance between privacy and usefulness is also feasible.

1. Violation of Data Privacy

AI systems often require large datasets to function effectively, which may involve collecting extensive personal information. Ensuring that data collection practices comply with privacy regulations such as GDPR, and CCPA is crucial but impracticable due to the volume of data processed and obtaining and managing user consent for data collection and processing becomes complex, particularly when data is used for multiple purposes or shared across different AI systems. Also, while anonymising data can protect individual identities, sophisticated AI algorithms may re-identify individuals from anonymized datasets, posing a risk to privacy.

2. Supply of Potentially Identifiable Information (PII) by Data Subjects Leading to Data Breach

Users sometimes include potentially identifiable information in their query while using AI applications without realising it, this increases the risk of PII exposure and compliance issues. For example, an employee using generative AI to help create an internal report may input confidential financial statements or personnel or corporate information that could be leaked. AI systems are as vulnerable to data breaches as traditional IT systems. Protecting data from unauthorized access is critical, especially when handling sensitive or personal information. Ensuring that data is securely stored and transmitted between systems is essential to prevent unauthorized access and tampering.

3. Difficulty in Compliance due to Various Cross-Broder Data Protection Laws

AI algorithms collect datasets and training data across the globe in multiple languages. This means that AI developers and operators have to make sure they comply with all applicable, local data privacy laws, such as the CCPA in California or the new AI Act in the European Union, this sometimes becomes difficult as tracing and identification of the origin of a particular data may not be possible. Data protection laws and regulations are continually evolving and keeping up with these changes and ensuring compliance across different jurisdictions is a bit of a challenge. Many AI systems operate across borders, complicating compliance with regional data protection laws, which may have conflicting requirements.

8.0 Summary of Findings

With the wide use of AI comes the fear of loss of data security, AI however bring with it indispensable innovations that are used in various aspects of life and enable development, this indispensability has however translated to breach of data security. This study found that despite the usefulness of AI, it is very important that personal data of be secured from illegal use and that consent must be sought and obtained before any such data must be used by a controller or processor whether human controller of Artificial Intelligence Application. The study further found that governments all over the world have enacted laws for the protection of the right to data privacy and the enforcement of the same and that the new EU AI Act is a useful instrument in governing the operation of

Artificial Intelligence and ensuring its compliance with regulatory laws. The study further finds that despite the number of Laws to ensure data security and the EU AI Act, there are still in existence some challenges that make total compliance with regulations on Data Privacy almost unattainable.

9.0 Conclusion and Recommendations

Artificial Intelligence has come to stay, and so is Data Privacy and the right to data protection. Thus, this paper concludes that ensuring the privacy, security, and integrity of data within AI systems requires a multi-level approach. This includes robust data governance, adherence to Evolving regulations, and the implementation of privacy-preserving techniques. It is hereby recommended as follows:

1. Implementation of robust data governance frameworks by organisations is encouraged to establish comprehensive data governance policies to oversee the entire lifecycle of data within AI systems. This includes data collection, storage, usage, sharing, and deletion, ensuring compliance with relevant data protection laws and regulations. Also, the implementation of comprehensive data security protocols to protect against data breaches and unauthorised access should be prioritised, this includes secure data storage, encryption, and secure data transmission practices.
2. Adopting and utilising advanced privacy-preserving techniques such as differential privacy, federated learning, and homomorphic encryption. These technologies can help protect sensitive data while enabling AI systems to function effectively without compromising privacy.
3. Development of transparent AI systems with clear and explainable decision-making processes can help enhance transparency and accountability to ensure that AI systems can be audited and scrutinised for compliance with ethical and legal standards.
4. Ensure regulatory compliance and stay informed about evolving data protection regulations and ensure that AI systems comply with applicable laws such as GDPR, CCPA, and other regional regulations. This includes managing cross-border data transfers in accordance with international data protection standards. Foster collaboration between technologists, legal experts, ethicists, and policymakers to develop comprehensive solutions that address the challenges of AI and data privacy.
5. Promote ethical AI practices by engaging stakeholders, including users, in discussions about data use and AI system design to respect user autonomy by obtaining informed consent and giving individuals control over their data and implement ethical guidelines to govern the development and deployment of AI technologies. It is also recommended that ongoing education and training for AI practitioners on data privacy and protection issues should be organised to promote a culture of continuous learning to adapt to new challenges and advancements in AI and data protection, and support for research and development in the field of AI and data privacy to innovate new methods and tools that enhance data protection while maximising the benefits of AI technologies is highly recommended.
6. Organisations are implored to employ technical solutions such as differential privacy, federated learning, and homomorphic encryption which aim to balance data utility and privacy. Federated learning is a promising technique that allows multiple parties to collaboratively train a model without sharing their data, Homomorphic encryption and differential privacy are two techniques that can be used to address these privacy concerns. Homomorphic encryption allows secure computations on encrypted data, while differential privacy provides strong privacy guarantees by adding noise to the data. However, depending solely on one technique leaves potential gaps in security coverage. Therefore, an integrated approach, combining DP and HE, might offer a comprehensive solution. This hybrid model attempts to leverage the strengths of both DP and HE, offering accuracy from HE and plausible deniability from DP.

7. Data Minimization: Collect and keep just the data required for CRM, reducing the risk of data breaches.

References

McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282

Rezak Aziz, Soumya Banaeree, Samia Bouzefrane, and Thinh Lee Vinh 'Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm' (2023) 15 (9) Future Internet

Education Securiti, 'Overview: AI Governance and its Intersection with Data Privacy Law' https://education.securiti.ai/certifications/ai-governance/ai-governance-and-its-intersection-with-data-privacylaws/overview-ai-governance-and-its-intersection-with-data-privacy-laws/ accessed 24 June 2024 See generally the GDPR and the CCPA

Hao Zhung, Khaifeng Bu, 'Privacy-Utility Tradeoff' (2022) Cornell University Information Theory https://arxiv.org/abs/2204.12057 accessed 24 June 2024.