International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

Privacy-Preserving Machine Learning: How Ai Drives Prosperity While Safeguarding Privacy.

Author: Motunrayo E. Adebayo

Date of Submission: 28-05-2025 Date of Acceptance: 08-06-2025

I. INTRODUCTION

According to Stryker and Kavlakoglu (2024), Artificial intelligence (AI) can be described as technology that allows computers and machines to reproduce human learning, comprehension, problem solving, decision making, creativity and autonomy.Applications and devices equipped with AI can see and identify objects, understand and respond to human language. They can also learn from new information and experience. They can make detailed recommendations to users and experts. They can act independently, replacing the need for human intelligence or intervention.

AI is always available anytime and is largely reliable in terms of delivery. Tools such as AI chatbots or virtual assistants can reduce demands for human staff service or support. AI can help maintain consistent work quality and output levels when used to complete repetitive or tedious tasks.

Closely following AI is machine learning, which involves creating models by training an algorithm to make predictions or decisions based on collected data. It encompasses techniques that enable computers to learn from and make conclusions based on data without being programmed for specific tasks.

There has been significant growth of Artificial Intelligence (AI), as AI systems are fast becoming a contemporary solution that many businesses adopt today. Its adoption into various sectors, from healthcare to finance, is driving massive shifts in changing how humans relate with data, which is used for decision-making. DigitalOcean (2023) points out that 49% of respondents in its survey utilize artificial intelligence and machine learning tools for business use.

One of the groundbreaking benefits of AI is that it can minimize human errors in various ways.It can be used to guide people through the proper steps of a process, identifying potential mistakes before they occur, and fully automating processes without any form of human intervention. This is especially important in industries such as healthcare where, for example, AI-guided surgical robotics can facilitate consistent precision.Machine learning algorithms can continually improve their accuracy and further reduce errors as they're exposed to more data and "learn" from experience

The rapid advancements in artificial intelligence and machine learning are stimulating a technological gold rush, transforming automation, predictive analytics, and data-driven decision-making. These technologies are not just streamlining operations but also serving as catalysts for innovation across various industries. As companies navigate the challenges of implementation, they unlock opportunities for growth and competitive advantage. Governments are not left behind in the race to influence the course of AI development. In January, 2025, President Trump announced a 500 billion dollar investment in AI infrastructure, which will be used to build several data centers, creating at least 100,000 jobs. AI systems require enormous computing power, pushing demand for specialized data centers that enable tech companies to link thousands of chips together in clusters.

However, hesitation around these technologies persists. Despite its widespread use, a lot of concerns remains present relating to ethical, legal, and security challenges.

The issue of privacy is one which has come with this significant advancement in information technology. This is because AI systems process vast amounts of personal information, the line between utility and intrusion becomes increasingly blurred. Companies using AI business tools or developing their own must carefully balance protecting sensitive information with maximizing the technology's capabilities. This study delves into the multifaceted issue of AI privacy, examining the risks, challenges, and strategies for mitigation that individuals, governments, and businesses must consider.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

PROBLEM STATEMENT

According to Kaur (2018), artificial Intelligence is a branch of science which deals with helping machines find solutions to complex problems in a more humanlike fashion. This generally involves borrowing characteristics from human intelligence and applying them as algorithms in a computer friendly way. Artificial Intelligence's scientific goal is to understand intelligence by building computer programs that exhibit intelligent behavior.

The theoretical origins of artificial intelligence, and the concept of intelligent machines may be traced to Greek Mythology (Jeffrey, 2022). Intelligent artifacts have appeared in journalism since then, with real mechanical devices actually indicating behavior with some degree of intelligence. The study of logic led directly to the discovery of the programmable digital electronic computer, based on the work of mathematician Alan Turing and others. Turing's theory of calculation suggested that a machine, by shuffling symbols as simple as "0" and "1", could replicate any imaginable mathematical act. This, along with simultaneous discoveries in neurology, information theory and cybernetics,inspired a small group of researchers to begin to seriously think about the possibility of an electronic brain.

Within 1950 – 1960,the first operational AI programs were written in 1951 to run on the Ferranti Mark I machine of the University of Manchester (UK): a draughts playing program written by Christopher Strachey and a chess-playing program written by Dietrich Prinz.

During the 1960s and 1970s Marvin Minsky and Seymour Papert issuedperceptrons, which are representative limits of simple neural nets, and AlainColmerauer developed the Pro log computer language. TedShortliffe established the power of rule-based systems for information representation and inference in medical diagnosis and therapy, in what is sometimes referred to as the first expert system. Hans Moravec developed the first computer-controlled vehicle to separately discuss cluttered barrier courses.

In the 1980s, neural networks became largelyadopted with the back broadcast algorithm, first described by Paul John Werbos in 1974. By 1985 the market for AI had reached over a billion dollars. At the same time, Japan's fifth generation computer project stimulated the U.S and British governments to return grant for academic research in the field. However, beginning with the fall of the Lisp Machine market in 1987.

In the 1990s and early 21st century, AI achieved its greatest successes, although it was largely hidden. Artificial intelligence is used for logistics, data mining, medical analysis and many other areas throughout the skill industry. The success was due to several factors: the rising importance of solving exact sub problems, the creation of new ties between AI and other fields working on similar problems, and a new assurance by researchers to hard mathematical methods and precise scientific standards

As promising and helpful as AI is, numerous challenges have been identified with this innovation which raises significant concerns. Rijmenam (2023) points out that AI systems require vast amounts of (personal) data, and if this data falls into the wrong hands it can be used for nefarious purposes, such as identity theft or cyberbullying. Also, AI systems could be used in discriminating against individuals, based on race, gender, religious affiliation, etc. This could be done by collecting biased information into AI systems, which could then exclude individuals based on these conditions.

AI systems have also been found to be used for bad data practices. AI can be used to create convincing fake images and videos, which can be used to spread misinformation or even manipulate public opinion. Also, AI can be used to conduct phishing attacks, which can trick individuals into revealing sensitive information or clicking on harmful web links.

Unregulated use of AI also impacts national security. For instance, the Chinese AI model known as ''DeepSeek'' stores users' data in China, which raises concerns about state-sponsored cyber activities. State-sponsored cyberattacks often target other countries' critical infrastructure, government agencies, and public sector units such as healthcare organizations. Consequently, ''DeepSeek'' has been banned on government devices in South Korea, Australia and Taiwan (Aljazeera, 2025). Similarly, the Italian Data Protection Authority known as the Garante banned the use of Deepseek, as concerns about data privacy, and storage of users' data were not addressed by the AI startup.

In addition, the methods highlightingsophisticated artificial intelligence systems are vulnerable to a new type of cybersecurity attack called an "artificial intelligence attack." Using this attack, adversaries can manipulate these systems to alter their behavior to achieve sinister objectives. As artificial intelligence systems are further integrated into

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

critical components of society, these artificial intelligence attacks represent an emerging and systematic vulnerability with the potential to have significant effects on the security of the country.

As AI systems become more sophisticated and can process and analyze vast amounts of data, the potential for misuse and abuse of this technology grows.In order to ensure that AI technology is developed and used in a way that respects individual rights and freedoms, it is essential that it be subject to effective regulation and oversight. This includes not only the collection and use of data by AI systems but also the design and development of these systems to ensure that they are transparent and neutral.

THE NEED FOR PRIVACY IN AI SYSTEMS

Privacy is an essential legal and social concept that gives people control over who has access to their sensitive information. Information privacy can be defined as the ability of the individual to control information about oneself. According to Beckers (2015) confidentiality is defined as ‘‘the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes’’. The examples of privacy definitions indicate a lack of a standard definition of privacy that explains the privacy requirements and risks in information systems. The complex and diverse nature of privacy risks in developing AI systems makes it even more challenging in addressing them. Therefore, a suitable framework for categorizing privacy risks considering AI development is needed. Organizing privacy risks into appropriate categories will help developers understand them better and make risk-informed decisions (Proske, 2019). Privacy risk categorization will also help developers integrate privacy-preserving solutions into AI development.

Corporate organizations are also advised to develop AI policy in order to comply with data regulatory frameworks and protect data. In addition, this will help to prevent data bias and discrimination, while helping to avoid conflicts of interest between the IT department and other departments using AI systems in an organization (Weaver, A).

AI PRIVACY AND DATA COLLECTION METHODS

Generally, data privacy encompasses those practices which ensure that the data shared by information providers is only used for the purpose for which it was provided. The right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which says:

a. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.
b. Everyone has the right to the protection of the law against such interference or attacks.

Specifically, AI privacy can bedescribed as a set of practices which is focused on ethical collection, storage, and usage of personal information by artificial intelligence systems. It is designed to meet the need for protection of individual data rights, while retaining the element of confidentiality, as AI algorithms process and learn from vast quantities of personal data. Ensuring AI privacy has to do with finding a balance between technological innovation and the preservation of personal privacy, especially when data is a highly valuable commodity as it is in recent years.

Largely artificial intelligence systems such as ChatGPT derive their capabilities from vast quantities of data sourced from all sections of the internet, including content from blogs, social media platforms, forums and many others. The volume of data content makes it difficult to ascertain its authenticity, which raises serious, lasting questions around potential biases and irregular responses.

Methods of AI data collection that impact data privacy include the following:

- AI systems can accumulate vast amounts of information by automatically harvesting data from websites. While some of this data is public, web scraping can also capture personal details, potentially without the approval of the data owner subject.
- AI systems that use facial recognition, fingerprinting, and other biometric technologies can intrude into personal privacy, collecting sensitive data that is unique to individuals and, if compromised, irreplaceable.
- Devices connected to the Internet of Things (IoT) provide AI systems with real-time data from our homes, workplaces, and public spaces. This data can reveal intimate details of our daily lives, creating a continuous stream of information about our habits and behaviors.
- AI algorithms can analyze social media activity, capturing demographic information, preferences, and even emotional states, without user awareness or consent.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

AI PRIVACY CHALLENGES

In its most basic form, privacy is the right to not be observed. People often act in a manner to increase their own privacy. For instance, shutting doors, wearing sunglasses, or clothing that is less revealing are simply subtle ways that humans actively moderate their own privacy. Privacy is valuable for several important reasons: It allows people to make their own, non-coerced decisions, to better calculate their behavior and be strategic in their social interactions, and also to take decisions and actions that do not conform to certain social norms (Bartneck et al., 2021)

According to Glasner (2023), AI introduces privacy challenges that are complex and multifaceted, different from those posed by traditional data processing. To begin with, AI systems have potential to digest and analyze more data at a higher frequency than traditional data processing systems, thereby increasing the risk of exposing personal data. AI can infer personal behaviors and preferences, often without the individual's knowledge or consentthrough pattern recognition and predictive modeling.

While the availability of users' private data enables AI systems to perform better, there are also considerable risks associated with this data collection. Bartneck et al., (2021) argue that the usage of data for non-intended purposes is a significant challenge in this regard. Users are often unaware how their data will be processed, used and even sold. The success of programmatic advertisement demonstrates how personal data can be used to make people buy products. This specific form of marketing has in general been accepted by society, and people have developed protection mechanisms. We know that advertisements can only be trusted to some degree. But we have not yet developed such a critical awareness towards AI. We might not even be aware of manipulation taking place. But there are serious forms of manipulation that use the exact same mechanisms that marketing experts applied so successfully: AI systems and social robots can be used to manipulate opinions on anything, including political views

In addition, the need for large data sets, which is required for AI systems to function effectively makes it attractive targets for cyber threats, subsequently heightening the possibility of breaches that could endanger personal privacy. In the absence of strict regulations, AI systems can extend the bias in the data collected into it, which may cause discriminatory outcomes.

These challenges underscore the necessity for robust privacy protection measures in AI. Balancing the benefits of AI with the right to privacy requires vigilant design, implementation, and governance to prevent misuse of personal data.

AI PRIVACY REGULATIONS

Globally, prominent regulatory frameworks on AI data privacy include the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the United States, and China's Personal Information Protection Law (PIPL). Each framework imposes its own form of guidelines on data collection, processing, and storage of data, placing great emphasis on user consent and transparency. The GDPR enactedin 2018 is viewed as often considered the best modelfor laws on data privacy. The framework guaranteesextensive measures for data protection, including the right to access, rectify, and delete personal data (Mbah, 2024).

One of the core principles of the GDPR isthe principle of Consent.GDPR mandates explicit, informed, and revocable consent from users before processing their data. Organizations must clearly outline the purpose of data collection and provide mechanisms for users to withdraw consent at any time. Similarly, Data Minimization is another principle emphasized by the GDPR (Mbah, 2024). This principle requires that only the data necessary for a specific purpose is collected and processed. Excessive data collection is prohibited, ensuring that user privacy is preserved by design. Furthermore, the GDPR emphasizesthe Right to Be Forgotten, as another principle of data privacy. Under this principle,users can request the deletion of their personal data under certain circumstances, e.g. when the data is no longer necessary or when consent has been withdrawn (Mbah, 2024).

However, the GDPR presents unique challenges for AI systems. AI models require vast datasets for training, often conflicting with GDPR's principles of data minimization and purpose limitation. For example, training an AI system to recognize medical anomalies may require extensive patient data, yet GDPR restricts the use of sensitive health data without explicit consent [22]. Another challenge lies in algorithmic explainability. GDPR mandates that users have the right to understand how automated decisions impacting them are made, often referred to as the "right to explanation". However, many AI systems, particularly those based on deep learning, operate as black boxes, making it difficult to provide meaningful explanations.

Similarly, the CCPA gives residents of California the right to control their dataandprovides

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

sanctions in the case of violations.One notable aspect of the CCPA is its emphasis on data monetization. Companies are required to disclose whether they sell personal data and provide users with an option to opt out. For example, websites must prominently display a "Do Not Sell My Personal Information" link for compliance.

Additionally, the PIPL reflects China's emphasis on data sovereignty and imposes stringent requirements for cross-border data transfers. Despite their benefits, fragmented regulations pose challenges for global businesses. Companies operating in multiple jurisdictions must navigate varying compliance requirements, leading to increased operational complexity and costs. For example, while GDPR prioritizes user consent, PIPL mandates stricter localization of data, creating conflicts for multinational organizations. Addressing these challenges requires harmonized global standards and innovative compliance strategies to enable seamless data governance across borders.

While comparing the GDPR, CCPA, and PIPL, it reveals significant differences in their scope and enforcement mechanisms. GDPR has a global impact, applying to any organization processing the data of EU residents, regardless of location. In contrast, the CCPA is limited to businesses operating in California or handling the data of California residents. PIPL extends its reach to entities processing Chinese citizens' data, with stringent localization requirements. Penalties also vary significantly. GDPR imposes the heaviest fines, with penalties reaching up to 4% of global turnover, while CCPA's maximum fine is $7,500 per violation. PIPL strikes a middle ground, with fines up to 5% of annual revenue, along with additional measures like operational suspensions. Enforcement mechanisms further differentiate these frameworks. GDPR's Data Protection Authorities (DPAs) actively pursue violations, as evidenced by high-profile fines against companies like Google and Amazon. CCPA enforcement, managed by the California Attorney General, is comparatively less aggressive. PIPL, on the other hand, reflects China's strict regulatory environment, with robust oversight and severe penalties for non-compliance (Mbah, 2024).

MITIGATING AI PRIVACY RISKS

From a Delloite survey in 2023, a significant number of individuals are either unaware or uncertain about the existence of ethical guidelines for generative AI usage. Mitigating AI privacy risks involves combining technical solutions, ethical guidelines, and robust data governance policies.

DigitalOcean (2025) argues that data privacy risks in AI systems can be mitigated by adopting the following strategies.

1. Embed privacy in AI design

To mitigate AI privacy risks, there is need for the integration of privacy considerations at the commencing stages of AI system development. This involves adopting "privacy by design" principles, which guarantees that data protection is a foundational component of the AI system being developed. This necessary safeguard helps to limit unnecessary data exposure and provide robust security from the beginning. Encryption should be standard to protect data at rest and in transit, while regular audits can ensure ongoing compliance with privacy policies.

2. Anonymizing and aggregating data

Using anonymization techniques can shield individual identities by removing identifiable information from the data sets AI systems use. This process involves altering, encrypting, or removing personal identifiers, ensuring that the data cannot be traced back to an individual. In addition to anonymization, data aggregation combines individual data points into larger datasets, which can be analyzed without revealing personal details. These strategies reduce the risk of privacy breaches by preventing data association with specific individuals during AI analysis.

3. Limit data retention times

Implementing strict data retention policies minimizes the privacy risks associated with AI. Setting clear limits on how long data can be stored prevents unnecessary long-term accumulation of personal information and diminishes the likelihood of a breach. Policies such as this compel organizations to regularly review and purge outdated or irrelevant data, streamlining databases and minimizing the amount of data at risk.

4. Increase transparency and user control

Enhancing transparency around AI systems' data practices creates user trust and accountability. IT companies should communicate which data types are being collected, how AI algorithms process them, and for what purposes. Providing users with control over their data—such as options to view, edit, or delete their information—empowers individuals and fosters a

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

sense of agency over their digital footprint. These align with ethical standards and ensure compliance with evolving data protection regulations, which increasingly mandate user consent and governance.

5. The impact of regulations

Understanding the implications of regulations such as the General Data Protection Regulation (GDPR) and similar regulations is essential for mitigating AI privacy risks, as these laws set stringent standards for data protection, granting individuals significant control over their personal information. These regulations mandate that organizations must be transparent about their AI processing activities and ensure that individuals' data rights are upheld, including the right to explanation of algorithmic decisions.

One of such regulations is the EU AI Act. The AI Act is a European regulation on artificial intelligence (AI) – the first comprehensive regulation on AI by a major regulator. The Act assigns applications of AI to three risk categories. First, applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned. Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.Like the EU's General Data Protection Regulation (GDPR) in 2018, the EU AI Act could become a global standard, determining to what extent AI has a positive rather than negative effect on individuals across the globe.

Similarly, in March 2025, the American National Institute of Standards and Technology (NIST) completed guidelines for evaluating differential privacy guarantees to de-identify data, known as NIST SP 800-226. The document is a call to action for standardization and certification of differential privacy systems. NIST SP 800-226 is a foundational resource for understanding and applying differential privacy in a world increasingly reliant on data analytics. By outlining strengths and weaknesses, it empowers practitioners to deploy privacy-preserving solutions that genuinely protect individuals.

As data privacy concerns grow, this guide marks a significant step toward robust, standardized protection, ensuring that the benefits of data analysis don't come at the cost of personal privacy.The publication targets technical practitioners with a background in data science or computer science, but its executive summary, privacy pyramid, and flowcharts are accessible to less technical decision-makers. It's particularly relevant for organizations handling sensitive data—government agencies, healthcare providers, tech companies, and researchers—who need to balance privacy with actionable insights.

Companies must implement measures that guarantee the accuracy, fairness, and accountability of their AI systems, particularly when decisions have a legal or significant effect on individuals. Failure to adhere to such regulatory standards can lead to substantial penalties.

Zaruhi Aslanyan and Panagiotis Vasilikos (2020) further points out that workable strategies include:

DATA ANONYMIZATION

Data anonymization aims at protecting the privacy of an individual in a given dataset. Basicallythis involves eliminating all direct identifiers, such as name, address and phone numbers. However, in most cases this proves insufficient. Removing the direct identifiers may still allow an attacker to re-identify an individual in the dataset by linking the data with other additional information that may be available. To forestall this, additional layers of anonymization should be created and enforced, to make it difficultfor an adversary to learn anything about an individual from an anonymized dataset.

DIFFERENTIAL PRIVACY

Differential privacy is a privacy method that helps reveal useful information about a dataset without revealing any private information about an individual in the dataset. The method guarantees that even if an attacker knows all records in a dataset, he/she will not be able to link a specific record to an individual on the basis of the output of a differentially private method. In other words, the outcome of the analysis is not (significantly) dependent on an individual's record being in the dataset. Hence, the privacy risk is essentially the same with or without the individual's participation in the dataset.

Differential privacy is achieved by adding random noise to the result, which can be done through various differentially private mechanisms, such as the Laplace mechanism, the exponential mechanism and the randomized response mechanism.

MULTI-PARTY COMPUTATION

Multi-Party Computation (MPC) is a technology that allows multiple parties to compute a function on their private inputs without revealing

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

them. The parties are independent and do not trust each other. The main idea is to allow users to perform a computation on private data while keeping the data secret. MPC guarantees that all participants learn nothing more than what they can learn from the output and their own input.

PRINCIPLES OF RESPONSIBLE AI USAGE

According to the United Nations, proper use of artificial intelligence is defined as one that is consistent with the Charter of the United Nations, respecting human rights laws, including the right to privacy. The principles as posited by UNESCO (2021)seek to provide a basis for organizations to make decisions about how to develop, design, deploy and use AI systems.

a. **Safety and Security**: Safety and security risks should be identified, addressed and mitigated throughout the AI system lifecycle to prevent where possible, and/or limit, any potential or actual harm to humans, the environment and ecosystems. Safe and secure AI systems should be enabled through robust frameworks.
b. **Purposefulness**: The use of AI systems, including the specific AI method(s) employed, should be justified, appropriate in the context and not exceed what is necessary and proportionate to achieve legitimate aims that are in accordance with each United Nations system organization's mandates and their respective governing instruments, rules, regulations and procedures.
c. **Data Privacy**: Privacy of individuals and their rights as data subjects must be respected, protected and promoted throughout the lifecycle of AI systems. When considering the use of AI systems, adequate data protection frameworks and data governance mechanisms should be established or enhanced in line with the United Nations Personal Data Protection and Privacy Principles also to ensure the integrity of the data used.
d. **Harmlessness**: AI systems should not be used in ways that cause harm, whether individual or collective, and including harm to social, cultural, economic, natural, and political environments. All stages of an AI system lifecycle should operate in accordance with the purposes, principles and commitments of the Charter of the United Nations. All stages of an AI system lifecycle should be designed, developed, deployed and operated in ways that respect, protect and promote human rights and fundamental freedoms. The intended and unintended impact of AI systems, at any stage in their lifecycle, should be monitored in order to avoid causing or contributing to harm, including violations of human rights and fundamental freedoms.
e. **Human Oversight**: Organizations should have in place appropriate oversight, impact assessment, audit and due diligence mechanisms, including whistle-blowers' protection, to ensure accountability for the impacts of the use of AI systems throughout their lifecycle. Appropriate governance structures should be established or enhanced which attribute the ethical and legal responsibility and accountability for AI-based decisions to humans or legal entities, at any stage of the AI system's lifecycle. Harms caused by and/or through AI systems should be investigated and appropriate action taken in response. Accountability mechanisms should be communicated broadly throughout the United Nations system to build shared knowledge resources and capacities.
f. **Fairness**: Organizations should aim to promote fairness to ensure the equal and just distribution of the benefits, risks and costs, and to prevent bias, discrimination and stigmatization of any kind, in compliance with international law. AI systems should not lead to individuals being deceived or unjustifiably impaired in their human rights and fundamental freedoms.
g. **Transparency**: The transparency and explainability of AI systems are often essential preconditions to ensure respect, protection and promotion of human rights, fundamental freedoms and ethical principles. Transparency is necessary for relevant national and international liability regimes to work effectively. A lack of transparency could also undermine the possibility of effectively challenging decisions based on outcomes produced by AI systems and may thereby infringe the right to a fair trial and effective remedy andlimit the areas in which these systems can be legally used.Transparency contributes to more peaceful, just, democratic and inclusive societies. It allows for public scrutiny that can decrease corruption and discrimination and can also help detect and prevent negative impacts on human rights. Specific to the AI system, transparency can enable people to understand how each stage of an AI system is put in place, appropriate to the context and sensitivity of the AI system.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 177-185www.ijaem.net ISSN: 2395-5252

II. CONCLUSION

The impact of artificial intelligence in the growth of industries like healthcare, retail businesses, and finance has shown the ability of AI to resolve challenges such as fraud detection and rendering personalized services. However, these benefits come with responsibilities, which includeeliminating biases, protecting sensitive data, and ensuring fairness. Emerging privacy-enhancing technologies such as federated learning, quantum cryptography, and blockchain can help to provide solutions to these challenges, while also enabling innovation.

One major factor addressed is the importance of aligning AI development with compliance and ethical principles. Organizations must integrate privacy elements into their AI systems from the foundation, establish robust data governance frameworks, and promote a consciousness of privacy among its workers. Collaborative efforts between public and private sectors can further promote the development of accessible solutions that respect the privacy of users, while also being compliant with regulatory requirements. Ultimately, businesses that proactively embrace ethical AI practices and prioritize privacy stand to gain a competitive edge. By fostering trust, enhancing operational transparency, and adhering to evolving regulations, organizations can position themselves as leaders in the rapidly evolving digital landscape.

Due to increased individual and organizational use, the necessity of protecting sensitive data has become a major issue. Solutions such as differential privacy offer promising solutions to enhance data protection while enabling innovative applications. At the same time, evolving regulations, such as the General Data Protection Regulation (GDPR) and EU AI Act underscores the need for organizations to prioritize transparency and accountability in their data practices. As regulatory frameworks become more stringent, businesses must navigate a complex compliance environment while striving to build consumer trust. Organizations can thrive by adopting ethical data practices and investing in privacy-preserving technologies, which will help toguarantee compliance with data regulations, while also gaining a competitive edge in the industry, as users are more likely to engage platforms that provide a higher assurance of data privacy. The future of data security in AI largely depends on collaboration between businesses, regulators, and consumers.

REFERENCES

[1]. Aljazeera (2025). Which countries have banned DeepSeek and why?. URL: https://www.aljazeera.com/news/2025/2/6/which-countries-have-banned-deepseek-and-why. This article identifies the new Chinese AI system, its challenges, and why it has been prohibited in certain countries.

[2]. Aslanyan, Z, & Vasilikos, P (2020).Privacy Preserving Machine Learning, Alexandra Institute Textbook. Available at https://www.alexandra.dk/wp-content/uploads/2020/10/Alexandra-Instituttet-whitepaper-Privacy-Preserving-Machine-Learning-A-Practical-Guide.pdf. This whitepaper serves as a guide to IT specialists and other readers without previous knowledge of data privacy. It introduces concepts related to privacy-preserving machine learning, as well as techniques to combine machine learning and preserve privacy.

[3]. Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). An Introduction to Ethics in Robotics and AI. Springer Nature. https://doi.org/10.1007/978-3-030-51110-4_1

[4]. Beckers, K (2015).Pattern and Security Requirements: Engineering Based Establishment of SecurityStandards. Cham, Switzerland: Springer.

[5]. Proske, D. (2019).Categorization of Safety and Risk, in Perceived Safety: A Multidisciplinary Perspective (Risk Engineering), M. Raue, B. Streicher, and E. Lermer, Eds. Cham, Switzer.

[6]. DigitalOcean (2023). Currents: Overview of 2023 startup and SMB trends. Available at https://anchor.digitalocean.com/rs/113-DTN-266/images/DigitalOcean-Currents_November-2023.pdf. The study examines startups as they are affected by recent developments in the tech ecosystem, and the implications of these developments on businesses.

[7]. Glasner, J. (2023).AI's Share of US Startup Funding Doubled In 2023. URL: https://news.crunchbase.com/ai-robotics/us-startup-funding-doubled-openai-anthropic-2023/.

[8]. Kaur, A. (2018). Emergence of Artificial Intelligence: A Review. Journal of Emerging Technologies and Innovative

Research (JETIR) Volume 5(2) pp 96 – 99.

[9]. Mbah G. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. International Journal of Science and Research Archive, 2024, 13(02), 2040–2058. DOI: https://doi.org/10.30574/ijsra.2024.13.2.2396.

[10]. Near J.P, Darais D, Lefkovitz N, Howarth GS (2025).Guidelines for Evaluating Differential Privacy Guarantees. National Institute of Standards and Technology, Gaithersburg, NIST Special Publication (SP) NIST SP 800-226. https://doi.org/10.6028/NIST.SP.800-226. This guide focuses on how to help organizations extract information from databases in a way that ensures that individual privacy is not compromised.

[11]. Stryker, C. & Kavlakoglu, E. (2024). What is artificial intelligence (AI)?URL: https://www.ibm.com/think/topics/artificial-intelligence. This article introduces the concepts of Artificial Intelligence, deep learning, as well as generative AI from a historical perspective. In addition, it also clarifies risks to artificial intelligence, ethics and governance related issues.

[12]. UNESCO (2021). Recommendation on the ethics of artificial intelligence. UNESCO General Conference. Paris.

[13]. Van Rijmenam, M. (2023). Privacy in the Age of AI: Risks, Challenges and Solutions. URL: https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/. The author emphasizes the evolution of information technology, while pointing out the necessity of AI as an important technological advancement. Furthermore, he highlights the challenges, risks, as well as workable solutions to maintaining privacy in the AI world.