Academic Journal of Science and Technology
Vol. 6 (2023)
https://academicpinnacle.com/index.php/ajst

Balancing Innovation and Privacy: Ethical Implications of Artificial Intelligence

Mei Chen
Department of Computer Science, University of Electronic Science and Technology of China, China

Abstract:

The proliferation of Artificial Intelligence (AI) technologies has transformed various sectors, from healthcare to finance. However, the integration of AI into everyday life raises significant privacy concerns. This paper explores the key privacy issues associated with AI, examines regulatory and ethical frameworks, and proposes strategies to mitigate privacy risks while leveraging AI's benefits.

Keywords: Artificial Intelligence (AI), Privacy, Data Protection, Data Collection, Data Breaches, Surveillance, Profiling, Personal Data, Sensitive Data, Behavioral Data.

1. Introduction:

Artificial Intelligence (AI) has become a transformative force across diverse sectors, including healthcare, finance, education, and transportation. Technologies such as machine learning, natural language processing, and computer vision are increasingly embedded in applications ranging from automated medical diagnoses to personalized marketing strategies. As AI systems gather and analyze vast amounts of data, they offer significant benefits but also introduce substantial privacy risks. The importance of privacy in the digital age is underscored by growing concerns over data breaches, unauthorized surveillance, and the misuse of personal information. This paper aims to explore the intersection of AI and privacy, examining the inherent risks posed by AI technologies and evaluating current regulatory and ethical frameworks. It will also propose strategies for mitigating privacy concerns while harnessing the advantages of AI, ultimately seeking to balance technological advancement with the fundamental right to privacy[1].

In the digital age, privacy has emerged as a critical concern due to the pervasive nature of data collection and the increasing sophistication of data analytics. As individuals interact with digital platforms, they generate vast amounts of personal information, from browsing habits and location data to sensitive financial and health records[2]. This data, if inadequately protected, can be exploited for various purposes, including unauthorized surveillance, identity theft, and targeted manipulation. The erosion of privacy not only poses risks to personal security but also threatens the autonomy and dignity of individuals. In an era where personal data can be harvested and analyzed on an unprecedented scale, safeguarding privacy has become essential to maintaining trust in digital systems and ensuring that technological advancements do not come at the expense of fundamental rights. Privacy protection is therefore crucial not only for individual security but also for upholding democratic values and fostering a fair and respectful digital environment.

Artificial Intelligence (AI) encompasses a range of technologies designed to simulate human intelligence and perform tasks that typically require cognitive functions. Key AI technologies include machine learning, where algorithms improve their performance based on data; natural language processing (NLP), which enables machines to understand and generate human language; and computer vision, which allows computers to interpret and analyze visual information from the world. These technologies have found applications across various domains. In healthcare, AI aids in diagnosing diseases, personalizing treatment plans, and predicting patient outcomes. In finance, it is used for algorithmic trading, fraud detection, and risk management. AI-powered systems enhance customer experiences through chat bots and personalized recommendations in retail, while in transportation, autonomous vehicles and traffic management systems leverage AI to improve safety and efficiency. The broad applicability of AI underscores its transformative potential, but also highlights the need to address the associated challenges, including those related to privacy and data protection.

The purpose of this paper is to explore the complex interplay between Artificial Intelligence (AI) technologies and privacy concerns, focusing on how the deployment of AI impacts data protection and individual privacy. It aims to provide a comprehensive analysis of the privacy risks associated with AI, including issues related to data collection, unauthorized access, and potential misuse. By examining existing regulatory and ethical frameworks, this paper seeks to evaluate how current measures address these privacy challenges and identify gaps that need to be addressed.

Additionally, the paper will propose practical strategies and solutions for mitigating privacy risks while leveraging the benefits of AI, with a focus on privacy-preserving technologies and best practices for AI development. The scope includes a review of relevant case studies, emerging trends, and future directions, aiming to balance technological innovation with the imperative of protecting fundamental privacy rights.

2. AI and Data Collection:

Data collection is a fundamental component of Artificial Intelligence (AI) systems, serving as the foundation for training and optimizing machine learning models. AI technologies rely on vast quantities of data to identify patterns, make predictions, and generate insights. This data can include personal information, such as demographic details, browsing history, and even biometric data. The methods of data collection are diverse, ranging from user interactions with online platforms and mobile applications to sensors embedded in IoT devices. While data collection enables AI to deliver personalized experiences and enhance decision-making processes, it also raises significant privacy concerns[3]. The extensive gathering and processing of personal data can lead to issues such as data breaches, unauthorized access, and the potential for misuse. Furthermore, the aggregation of data from multiple sources can lead to detailed profiling, which may infringe upon individual privacy and autonomy. As AI systems become increasingly sophisticated, addressing the challenges of responsible data collection and ensuring robust privacy safeguards are essential to maintaining trust and protecting individuals' rights in the digital age.

In AI systems, data collection is facilitated through a variety of mechanisms designed to gather, process, and analyze information from diverse sources. These mechanisms include user interactions with digital platforms, such as websites, mobile apps, and social media, where data is captured through clickstreams, search queries, and user-generated content. Additionally, AI systems utilize sensors and devices embedded in the Internet of Things (IoT) to collect data from physical environments, such as smart home devices, wearable technology, and autonomous vehicles. Data is also aggregated from public and private databases, including online records, transactional data, and demographic information. Machine learning algorithms rely on this extensive data to train models, identify patterns, and make predictions. While these mechanisms enable AI systems to deliver tailored and efficient services, they also pose privacy risks if data is collected without adequate consent, transparency, or security measures. Ensuring that data collection practices are ethical and compliant with privacy regulations is crucial to safeguarding user information and maintaining trust in AI technologies[4].

3. Types of Data Collected: Personal, Sensitive, and Behavioral

AI systems collect a range of data types, each with distinct implications for privacy and security. Personal data refers to information that can identify an individual, such as names, email addresses, and phone numbers. This type of data is often collected through user registrations, transactions, and interactions with digital platforms. Sensitive data includes information that requires higher levels of protection due to its nature, such as health records, financial information, and biometric data like fingerprints or facial recognition patterns. The exposure of sensitive data can have serious repercussions, including identity theft and unauthorized access to personal services[5]. Behavioral data, on the other hand, encompasses information about an individual's actions and patterns, such as browsing history, search queries, and usage habits. This type of data is used to create detailed user profiles and deliver personalized experiences but can also lead to intrusive tracking and profiling. The collection and use of these data types require stringent privacy measures to ensure that individuals' rights are respected and that their information is handled securely and ethically. The fig.1 shows personal, Behavioral and Technical data.

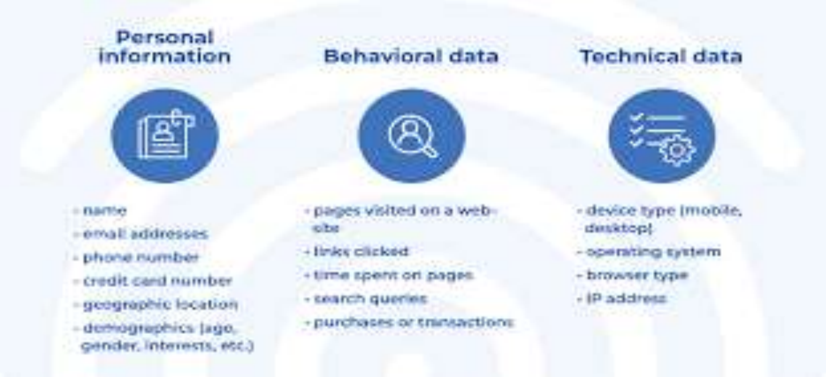

Fig.1: Personal, Behavioral and Technical data

Several case studies illustrate the complexities and privacy concerns associated with AI applications that involve extensive data collection. One prominent example is the use of AI in personalized advertising. Platforms like Facebook and Google utilize AI algorithms to analyze users' online behavior, including search queries, website visits, and social media interactions. This data enables them to deliver highly targeted ads, but it has also led to concerns about user consent and data security. Another case is the deployment of AI-powered health monitoring devices, such as wearable fitness trackers. These devices collect sensitive health data, including heart rate, activity levels, and sleep patterns, which can provide valuable insights for users but also pose risks if the data is mishandled or exposed. A third example is the use of facial recognition technology in public surveillance systems. While this technology can enhance security and law enforcement efforts, it has raised significant privacy issues, particularly regarding the potential for mass surveillance and the lack of transparency in how collected data is used. These case studies highlight the need for robust privacy protections and ethical considerations in AI data collection practices to address the associated risks and maintain public trust.

4. Privacy Risks Associated with AI

The integration of Artificial Intelligence (AI) into various applications presents several privacy risks that can significantly impact individuals and society. One major risk is the potential for data breaches, where unauthorized parties gain access to sensitive personal information stored by AI systems. These breaches can result in identity theft, financial loss, and damage to personal reputation. Another concern is profiling and surveillance as AI technologies can analyze large datasets to create detailed user profiles, which may be used for targeted advertising or monitoring, often without explicit consent. Data retention practices also pose risks, as the accumulation of data over time increases the likelihood of exposure and misuse. As AI systems continue to evolve, addressing these privacy risks through robust security measures, transparent data practices, and ethical guidelines is crucial to protecting individual rights and ensuring responsible AI deployment.

Data breaches and unauthorized access represent critical privacy risks associated with AI systems, where sensitive personal information can be exposed to malicious actors or inadvertently accessed by unauthorized parties[6]. In the context of AI, these breaches often result from vulnerabilities in data storage, transmission, or processing systems. For example, if an AI system is compromised, attackers can access large volumes of personal data, including financial details, health records, and private communications. The fig.2 represents AI system privacy risks and harm reduction.

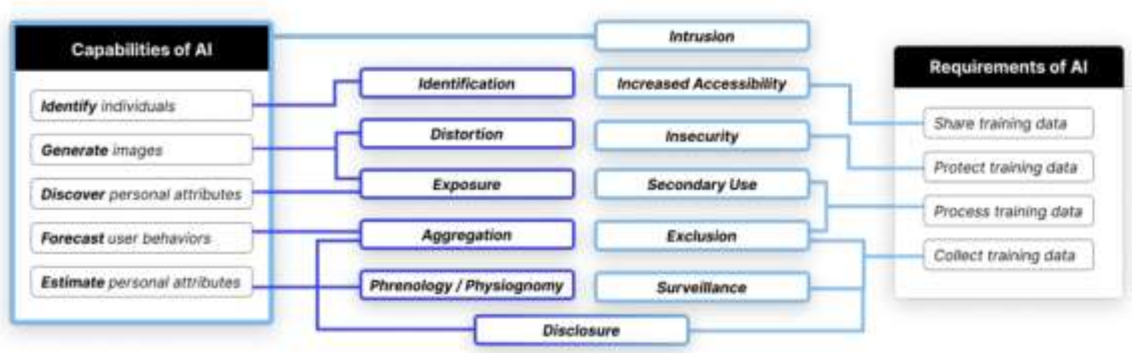

Fig.2: AI system privacy risks and harm reduction

Unauthorized access can also occur through inadequate security measures or flaws in software, leading to the exploitation of sensitive information. The consequences of such breaches are profound, including financial loss, identity theft, and severe damage to personal and organizational reputations. Additionally, breaches can undermine public trust in AI technologies and their providers, highlighting the need for robust security protocols, encryption, and continuous monitoring to prevent unauthorized access and ensure the integrity and confidentiality of data.

Profiling and surveillance concerns are significant privacy issues associated with AI technologies, as they involve the collection and analysis of personal data to create detailed user profiles and monitor individuals' activities. AI-driven profiling can aggregate data from various sources, such as online behaviors, social media interactions, and transactional records, to develop comprehensive insights into individuals' preferences, habits, and characteristics. While this can enhance personalization and service efficiency, it also raises concerns about intrusive surveillance and the potential misuse of such data. Profiling can lead to increased scrutiny and tracking of individuals without their explicit consent, impacting their privacy and autonomy. Moreover, the extensive monitoring enabled by AI technologies can contribute to a surveillance culture, where individuals feel constantly observed, potentially stifling free expression and altering behavior. Addressing these concerns requires a careful balance between leveraging AI for beneficial purposes and implementing strict privacy protections and transparency measures to safeguard individuals' rights and prevent misuse.

The long-term retention of data in AI systems carries significant implications for privacy and security. As data is accumulated over time, it becomes a valuable asset for analysis but also increases the risk of misuse and exposure[7]. Extended data retention can lead to the creation of highly detailed and potentially intrusive profiles of individuals, which may be used for purposes beyond the original intent, including targeted advertising, predictive policing, or employment decisions. Additionally, long-term data storage raises concerns about the potential for data breaches and unauthorized access, as the more data is kept, the greater the risk of its compromise.

Over time, outdated or irrelevant data can also contribute to inaccuracies and biases in AI models, affecting decision-making processes and reinforcing systemic biases[8]. The ethical and legal implications of retaining data indefinitely necessitate robust data governance practices, including clear data retention policies, regular audits, and mechanisms for data deletion or anonymization to protect individuals' privacy and ensure that data handling remains aligned with current needs and regulations.

5. Regulatory and Ethical Frameworks

Regulatory and ethical frameworks play a crucial role in guiding the development and deployment of AI technologies while addressing privacy concerns. Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) establish legal standards for data protection, requiring organizations to obtain explicit consent for data collection, ensure transparency in data usage, and provide individuals with rights to access, correct, and delete their personal information. These frameworks aim to safeguard privacy and hold organizations accountable for their data practices. In addition to legal requirements, ethical principles guide the responsible use of AI, emphasizing fairness, transparency, and accountability.

Ethical guidelines advocate for the implementation of privacy-by-design principles, where data protection is integrated into the development process from the outset. Together, regulatory and ethical frameworks help mitigate risks associated with data collection and usage, ensuring that AI technologies are developed and deployed in ways that respect individuals' privacy and uphold public trust.

Ethical principles in AI development are essential for ensuring that technology is used in ways that respect human rights and promote societal well-being. Fairness is a fundamental principle that aims to prevent discriminatory outcomes by ensuring that AI systems do not reinforce existing biases or create new inequalities. This involves designing algorithms that are inclusive and equitable, and regularly auditing them to identify and mitigate any biases that may arise. Transparency is another critical principle, requiring that the processes and decisions made by AI systems are understandable and accessible to users[9]. This includes providing clear explanations of how data is used, how decisions are made, and the underlying logic of algorithms. Transparency helps build trust and allows individuals to challenge or seek recourse if they believe they have been unfairly treated. Additionally, accountability ensures that developers and organizations are responsible for the impacts of their AI systems, including any unintended consequences. By adhering to these ethical principles, AI development can better align with societal values and contribute positively to the broader community while addressing privacy and fairness concerns.

Existing privacy regulations play a pivotal role in safeguarding personal data and ensuring that organizations handle information responsibly. The General Data Protection Regulation (GDPR), enacted by the European Union in 2018, is one of the most comprehensive privacy laws globally. It mandates that organizations obtain explicit consent from individuals before collecting their data, provides individuals with rights to access, correct, and delete their information, and enforces stringent data protection and breach notification requirements. GDPR also introduces the concept of data protection by design and by default, requiring organizations to integrate privacy considerations into their operations from the outset.

The California Consumer Privacy Act (CCPA), which came into effect in 2020, provides similar protections for residents of California. It grants consumers the right to know what personal data is being collected, to opt out of its sale, and to request deletion of their information. CCPA also imposes requirements on businesses to implement robust data protection practices and provides for enforcement by the California Attorney General. Both regulations emphasize transparency, user consent, and data security, setting a high standard for privacy protection and influencing privacy practices and policies worldwide.

6. Strategies for Enhancing Privacy in AI

Enhancing privacy in AI systems requires a multifaceted approach that integrates both technological solutions and organizational practices. One effective strategy is data anonymization, which involves removing personally identifiable information from datasets to prevent the identification of individuals. Techniques such as data masking and aggregation can help achieve this while preserving the utility of the data for analysis. Privacy-preserving technologies such as differential privacy and federated learning also play a critical role. Differential privacy adds controlled noise to data to ensure that individual records cannot be discerned, while federated learning enables model training across decentralized datasets without transferring raw data, thus reducing the risk of data breaches. Implementing privacy-by-design principles, where privacy considerations are integrated into the development process from the beginning, is another key strategy[10]. This includes conducting regular privacy impact assessments to evaluate potential risks and implementing strong data governance policies that outline data collection, storage, and sharing practices.

Additionally, organizations should prioritize user consent and transparency, ensuring that individuals are informed about how their data will be used and can exercise control over it. By adopting these strategies, organizations can better protect user privacy while harnessing the benefits of AI technology.

Data anonymization and minimization are crucial techniques for enhancing privacy and mitigating risks associated with data collection in AI systems. Data anonymization involves transforming personal data in a way that removes or obfuscates identifying information, making it impossible to trace the data back to individuals. Techniques such as data masking, pseudonymization, and generalization help ensure that even if data is exposed or accessed without authorization, it cannot be used to identify specific individuals. The fig.3 represents Privacy Enhancing Technologies (PET).

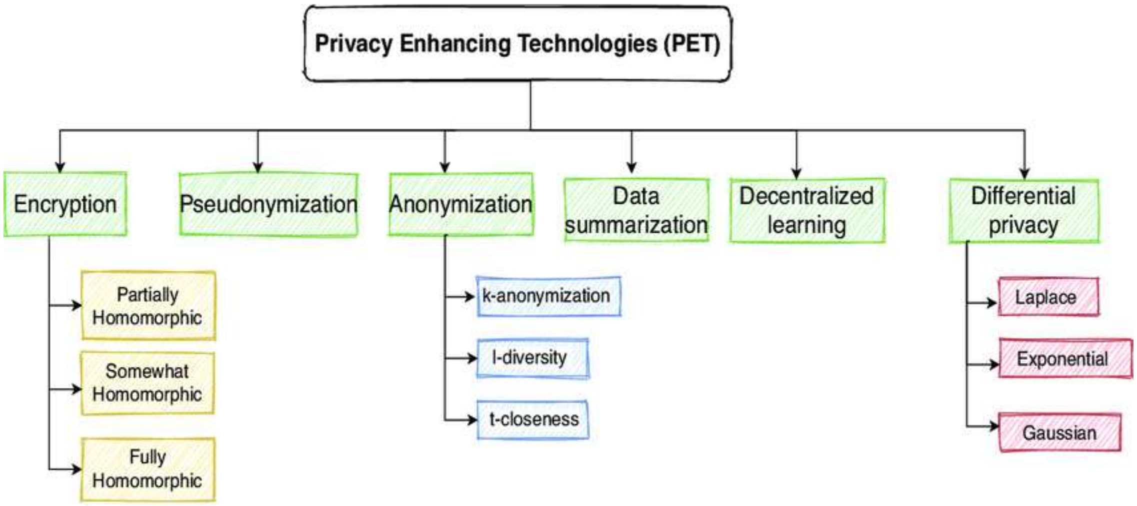

Fig.3: Taxonomy of Privacy Enhancing Technologies

Data minimization complements anonymization by ensuring that only the data necessary for a particular purpose is collected and retained. This principle advocates for the collection of minimal data required to achieve specific objectives, reducing the overall volume of data at risk. Methods such as data aggregatio, where individual data points are combined into summary statistics, and feature selection, which involves choosing only the most relevant data attributes, help implement data minimization. By applying these techniques, organizations can enhance privacy protection, reduce the likelihood of data breaches, and maintain compliance with privacy regulations while still leveraging data for valuable insights and AI advancements.

Privacy-preserving AI technologies are designed to protect individuals' personal data while enabling the effective use of AI systems. Differential privacy is one such technology that adds carefully calibrated noise to datasets, ensuring that the inclusion or exclusion of any individual’s data does not significantly affect the overall outcome of the analysis. This technique provides strong privacy guarantees by making it difficult for adversaries to infer information about any single individual from the results. Federated learning is another advanced approach that enhances privacy by training machine learning models across decentralized data sources without centralizing the data.

For AI developers and organizations, adopting best practices is essential to ensure the responsible use of technology and protect user privacy. One fundamental practice is data protection by design, which involves integrating privacy measures into the development process from the outset. This includes conducting privacy impact assessment to identify potential risks and implementing robust security protocol to safeguard data against breaches. Developers should also employ privacy-enhancing technologies such as differential privacy and federated learning to minimize the risks associated with data handling.

Additionally, organizations should establish clear data governance policies that define data collection, storage, and sharing practices, and ensure compliance with relevant regulations. Transparent data practices are also crucial; this involves providing users with clear information about how their data will be used, obtaining informed consent, and allowing them to exercise control over their information. Regular training and awareness programs for staff on privacy and data protection principles can further support these practices. By adhering to these guidelines, AI developers and organizations can build trust with users, enhance data security, and foster ethical AI development.

7. Case Studies and Solutions:

Examining case studies of AI applications provides valuable insights into effective solutions for addressing privacy concerns. One notable example is Apple’s approach to privacy with its differential privacy techniques, used to gather user data for improving services while minimizing the risk of identifying individuals. By adding noise to data sets, Apple ensures that user data remains anonymous, thereby protecting privacy while still allowing for meaningful data analysis. Another significant case is the use of federated learning by Google in its G Board keyboard app[11]. This approach enables the model to be trained on users' devices without sending personal text data to the cloud, thereby preserving user privacy and reducing data security risks. In the healthcare sector, IBM’s use of secure multi-party computation (MPC) in its Watson Health platform demonstrates how encrypted data can be used for collaborative research while safeguarding patient confidentiality. These case studies highlight that implementing privacy-preserving technologies and strategies can address privacy concerns effectively while still leveraging the power of AI. By adopting similar solutions, organizations can enhance privacy protection and build trust with their users.

Examining real-world examples where privacy concerns have been effectively addressed reveals the practical application of privacy-preserving AI initiatives. For instance, Microsoft's use of differential privacy in its data analytics services demonstrates a successful approach to mitigating privacy risks. By integrating differential privacy algorithms, Microsoft enables the aggregation of user data for insights while ensuring individual data points remain untraceable, thereby balancing data utility with privacy protection. Another notable example is the Project Soli by Google, which uses radar-based sensing technology to collect non-intrusive, anonymized gesture data for improving user interaction with devices. This approach reduces the risk of sensitive data exposure by focusing on aggregated, anonymized data rather than individual records.

In the financial sector, Zerocash technology, developed by a research team including members from MIT, showcases a successful application of cryptographic techniques to ensure transaction privacy while maintaining blockchain integrity. These initiatives highlight how innovative privacy-preserving technologies can be integrated into AI systems, providing effective solutions that protect user privacy and maintain trust. By analyzing these examples, it becomes evident that implementing advanced privacy measures can address concerns while still enabling the benefits of AI-driven advancements.

Google's federated learning approach is a prime example, where machine learning models are trained across decentralized data sources on users' devices. This method ensures that sensitive information remains local, only sending aggregated model updates to central servers, thereby reducing the risk of data breaches and enhancing privacy. Another notable initiative is Apple's implementation of differential privacy in its data collection processes.

Apple employs differential privacy techniques to analyze usage patterns and improve services while ensuring that individual user data cannot be extracted or traced back to specific users. Similarly, IBM's use of homomorphic encryption in its research collaborations allows computations to be performed on encrypted data without exposing the underlying information, protecting sensitive data throughout the process[12]. These successful initiatives demonstrate that integrating privacy-preserving technologies—such as federated learning, differential privacy, and homomorphic encryption—into AI systems can effectively address privacy concerns while still delivering valuable insights and maintaining user trust. By learning from these examples, other organizations can develop and implement strategies that balance innovation with robust privacy protection.

8. Future Directions:

As AI technologies continue to evolve, the future of privacy protection will likely involve a blend of emerging innovations and enhanced regulatory measures. One promising direction is the development of advanced privacy-preserving techniques, such as quantum cryptography and secure multi-party computation (MPC), which offer new ways to protect data while enabling complex computations.

Additionally, AI-driven privacy tools that automatically detect and mitigate privacy risks in real-time could become more prevalent, leveraging machine learning to enhance data protection dynamically. Regulatory frameworks are also expected to evolve, with greater emphasis on international cooperation and harmonization of privacy laws to address the global nature of data flows. The integration of ethical AI practice will be crucial, with a focus on ensuring fairness, accountability, and transparency in AI systems. Moreover, public awareness and engagement regarding privacy will likely increase, driving demand for more robust privacy measures and influencing policy development. By exploring these future directions, the AI community can advance both technology and privacy protection, ensuring that innovations are aligned with ethical standards and societal values.

Emerging trends in AI and privacy are shaping the landscape of data protection and technology use. One notable trend is the rise of privacy-enhancing technologies like federated learning and differential privacy, which are gaining traction as methods to secure data while still enabling meaningful analysis. These techniques help mitigate privacy risks by ensuring that sensitive information remains decentralized and anonymized. Another trend is the increasing adoption of privacy-by-design principles, where privacy considerations are embedded into the development process from the outset, rather than being addressed as an afterthought. This approach is supported by evolving regulatory standards that emphasize data protection and user rights, such as the updated regulations under the European Union’s Digital Services Act (DSA) and the California Privacy Rights Act (CPRA).

Additionally, there is growing interest in AI ethics frameworks that guide responsible AI development, focusing on transparency, fairness, and accountability. The integration of blockchain technology for secure and transparent data transactions is also emerging as a potential solution to enhance privacy[13]. As these trends develop, they promise to advance the balance between leveraging AI's capabilities and safeguarding individual privacy.

The evolving role of regulation and public awareness is crucial in shaping the future of AI and privacy. As AI technologies advance, regulatory frameworks are becoming more comprehensive and globally coordinated, aiming to address the complex challenges posed by data collection and usage. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are setting precedents for data protection, but there is a growing need for updates and harmonization to keep pace with technological innovations. Emerging regulations, such as the EU’s Digital Services Act (DSA) and the proposed

As a result, organizations are facing pressure to adopt more stringent privacy practices and to communicate their data handling policies clearly. The interplay between evolving regulations and increasing public awareness is shaping a landscape where privacy is better safeguarded, and responsible AI practices are more widely adopted.

9. Conclusion

In conclusion, the intersection of AI and privacy presents both significant opportunities and challenges. As AI technologies continue to advance and integrate into various aspects of daily life, the need for robust privacy protections becomes increasingly critical. Privacy concerns, including data breaches, unauthorized access, and intrusive profiling, highlight the importance of implementing effective measures to safeguard personal information. Successful privacy-preserving initiatives, such as differential privacy, federated learning, and privacy-by-design principles, demonstrate that it is possible to balance technological innovation with strong privacy protections. Regulatory frameworks are evolving to address these concerns, but continued adaptation and international cooperation are necessary to keep pace with rapid technological changes. Public awareness is also rising, driving demand for greater transparency and accountability in AI practices. By embracing emerging technologies, adhering to ethical standards, and fostering a culture of privacy, stakeholders can ensure that AI advancements contribute positively to society while protecting fundamental rights.

References:

[1] N. Kamuni, S. Dodda, V. S. M. Vuppalapati, J. S. Arlagadda, and P. Vemasani, "Advancements in Reinforcement Learning Techniques for Robotics," *Journal of Basic Science and Engineering,* vol. 19, pp. 101-111.

[2] S. Thiebes, S. Lins, and A. Sunyaev, "Trustworthy artificial intelligence," *Electronic Markets,* vol. 31, pp. 447-464, 2021.

[3] F. Boniolo, E. Dorigatti, A. J. Ohnmacht, D. Saur, B. Schubert, and M. P. Menden, "Artificial intelligence in early drug discovery enabling precision medicine," *Expert Opinion on Drug Discovery,* vol. 16, no. 9, pp. 991-1007, 2021.

[4] S. Dodda, N. Kamuni, V. S. M. Vuppalapati, J. S. A. Narasimharaju, and P. Vemasani, "AI-driven Personalized Recommendations: Algorithms and Evaluation," *Propulsion Tech Journal,* vol. 44.

[5] K. B. Johnson *et al.*, "Precision medicine, AI, and the future of personalized health care," *Clinical and translational science,* vol. 14, no. 1, pp. 86-93, 2021.

[6] A. Blasiak, J. Khong, and T. Kee, "CURATE. AI: optimizing personalized medicine with artificial intelligence," *SLAS TECHNOLOGY: Translating Life Sciences Innovation,* vol. 25, no. 2, pp. 95-105, 2020.

[7] S. Dodda, N. Kamuni, J. S. Arlagadda, V. S. M. Vuppalapati, and P. Vemasani, "A Survey of Deep Learning Approaches for Natural Language Processing Tasks," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 9, pp. 27-36.

[8] V. Shah, "Next-generation artificial intelligence for personalized medicine: challenges and innovations," *International Journal of Computer Science and Technology,* vol. 2, no. 2, pp. 1-15, 2018.

[9] B. Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era," *BMC Medical Ethics,* vol. 22, pp. 1-5, 2021.

[10] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When machine learning meets privacy: A survey and outlook," *ACM Computing Surveys (CSUR),* vol. 54, no. 2, pp. 1-36, 2021.

[11] W. Naudé, "Artificial intelligence vs COVID-19: limitations, constraints and pitfalls," *AI & society,* vol. 35, pp. 761-765, 2020.

[12] S. K. Katyal, "Private accountability in the age of artificial intelligence," *UCLA L. Rev.,* vol. 66, p. 54, 2019.

[13] A. Konar, *Artificial intelligence and soft computing: behavioral and cognitive modeling of the human brain*. CRC press, 2018.