International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A REVIEW ON DATA PROTECTION IN THE ERA OF AI – CHALLENGES AND SOLUTIONS

KSHETRA, MERCY, VARSHA, AKSHARA

ABSTRACT

Artificial Intelligence (AI) is changing the way personal data is collected, stored, and used in different fields. Although AI makes many tasks faster and easier, it also creates challenges such as data leaks, privacy violations, unauthorized access, and misuse of personal information. This review examines the importance of data protection in the era of AI and explores how existing laws and security measures help protect individuals' privacy. It also discusses the challenges of ensuring transparency, obtaining user consent, and preventing the misuse of sensitive data by AI systems. Furthermore, the review highlights the role of strong data protection laws, secure technologies, and ethical AI practices in reducing privacy risks. It emphasizes the need to balance technological progress with individual privacy rights to ensure that AI is developed and used safely, responsibly, and fairly.

Keywords: Artificial Intelligence, Data Protection, Privacy, Data Security, Ethical AI

1. INTRODUCTION

Artificial Intelligence is changing how personal information is collected, analysed, and used. From online shopping to banking and education, AI systems use data to provide faster and more personalized services. However, AI can sometimes reveal information that individuals never directly shared. This creates a new challenge for data protection. Therefore, protecting personal information requires more than securing databases; it also requires controlling how AI interprets and uses data.

2. REVIEW OF LITERATURE

Previous studies and reports highlight the importance of privacy, fairness, and accountability in AI systems. • UNESCO (2021) emphasizes protecting human rights and privacy throughout the development and use of AI. • NIST (2023) presents a framework for identifying and managing risks associated with AI systems. • Russell and Norvig (2021) explain the principles and applications of artificial intelligence, providing a foundation for understanding AI-based decision-making. These sources highlight the need to combine technological development with responsible data management.

3. RESEARCH GAP

Existing discussions often focus on protecting stored personal information. However, greater attention is needed on information that AI can infer from ordinary activities, such as browsing habits, purchase patterns, and online behaviour. This paper examines how such hidden data risks can be reduced through responsible AI practices.

4. OBJECTIVES OF THE STUDY

To understand the relationship between AI and data protection. To identify major privacy and security challenges caused by AI. To examine the risks of collecting and analysing personal information. To suggest practical solutions for responsible AI-based data handling.

5. RESEARCH METHODOLOGY

Research design: Descriptive research. Nature of data: Secondary data. Sources of data: Research publications, books, institutional reports, and relevant policy documents. Method of analysis: The collected information is reviewed to identify major data protection challenges and possible solutions in AI applications.

6. CONCEPTUAL BACKGROUND

6.1 Artificial Intelligence:

AI refers to computer systems that perform tasks such as learning, prediction, and decisionmaking.

6.2 Data Protection:

Data protection involves safeguarding personal information against unauthorized access, misuse, and improper disclosure.

6.3 Inferred Personal Data:

This refers to information that AI predicts about a person by analysing existing data, even when the person has not directly provided that information.

6.4 Responsible AI:

Responsible AI involves designing and using AI systems with fairness, transparency, privacy, security, and human accountability.

7. ANALYSIS AND DISCUSSION

7.1 The Hidden Data Problem:

AI can connect small pieces of information to identify personal habits, interests, or preferences. Even ordinary data may reveal sensitive details when combined. Therefore, data protection must consider what AI can discover, not just what an organization collects.

7.2 Privacy Beyond Consent:

People may agree to share information without understanding how it could be analysed later. Organizations should explain data usage clearly and provide meaningful choices wherever possible.

7.3 Data Security and AI Misuse:

AI systems may expose information through weak security controls, excessive data access, or unsafe handling of user inputs. Strong access controls, encryption, and regular security testing can reduce these risks.

7.4 The Problem of Invisible Decisions:

AI can influence decisions about education, employment, loans, and other services without making its reasoning clear. Individuals should have appropriate ways to question important decisions and request human review.

7.5 Data Minimization as a Solution:

A practical solution is to collect only the information necessary for a specific purpose. Less unnecessary data means fewer opportunities for exposure and misuse.

7.6 Privacy by Design:

Privacy should be considered from the beginning of AI development rather than added after a problem occurs. Privacy testing, limited data retention, and secure system design can help prevent risks early.

7.7 Human Responsibility:

AI should not become an excuse for avoiding responsibility. Organizations must identify who is accountable for data misuse, investigate complaints, and correct harmful outcomes.

8. MAJOR FINDINGS

AI creates privacy risks through both direct data collection and inferred information. Consent is less meaningful when people do not understand how their data may be reused. Data minimization can reduce unnecessary privacy risks. Transparent decision-making can improve public trust. Human oversight remains important for sensitive decisions. Effective protection requires cooperation between developers, organizations, users, and regulators.

9. SUGGESTIONS / RECOMMENDATIONS

• Collect less data: Gather only information necessary for a clearly stated purpose. • Protect inferred information: Assess whether AI predictions could reveal sensitive personal details. • Improve transparency: Explain how personal data is collected, analysed, and shared. • Strengthen security: Use encryption, access restrictions, and regular security assessments. • Provide human review: Allow important AI-based decisions to be questioned where appropriate. •

Set clear accountability: Assign responsibility for privacy failures and corrective action. • Train users and employees: Promote awareness of safe and ethical AI practices.

10. CONCLUSION

Artificial Intelligence offers valuable opportunities, but its ability to discover hidden patterns creates new challenges for personal privacy. Data protection must therefore extend beyond securing stored information to controlling how AI interprets, predicts, and uses personal data. Data minimization, privacy-conscious design, transparency, and human accountability can help reduce these risks. The future of AI should not be measured only by how intelligently it processes information, but also by how responsibly it protects the people behind that information.

REFERENCES

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1 Russell, S. J., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137