

A Study on the Ethical Implications and Data Privacy Challenges in the Age of Artificial Intelligence

Shardul Santosh Kolte^{1*}, Saurabh Sanjay Kumar², Shirshendu Maitra³

Abstract

The fast adoption of Artificial Intelligence (AI) in areas like education, business, and everyday life comes with both tectonic and important ethical and data privacy issues. This paper examines the principle-practice divide between the ideals of the ethics as they are set and applied in the realities of AI implementation. The study is based on a mixed-methodology design, comprising of a quantitative survey of 52 participants and a qualitative study of four famous case studies, to survey the perceptions of the stakeholders and the sufficiency of existing regulatory frameworks, such as GDPR and the DPDP Act of India. Findings show that the respondents are in unison that AI is an issue of concern ethically, with data privacy being the most notable. A significant difference was determined to exist where the understanding of data protection laws does not generate trust in their effective application ($p < 0.01$). Although not all the survey data provided testimony to the point, case studies conducted qualitatively allowed establishing that absence of organizational and platform governance is a direct cause of privacy breaches. In addition, the study found that the transparency is an effective predictor of user trust ($p < 0.001$). The paper concludes that to solve this ethical dilemma, a multi-dimensional solution is necessary in implementing adaptive legal frameworks, strong governance, and clear AI design to make AI deployment responsible and trustworthy.

Keywords: Artificial intelligence (AI), AI ethics, data privacy, algorithmic bias, AI governance, transparency

INTRODUCTION

Artificial Intelligence (AI) is becoming one of the most transformative technological bases of the 21st century, changing industries, economies, and human relations on a scale never observed before. Examining user experience personalization and advancing healthcare diagnostics to define the edges of automation and decision-making, AI technologies have become the answer to the definition of

*Author for Correspondence

Shardul Santosh Kolte
E-mail: shardulkolte8@gmail.com

¹Research Scholar, Department MCA, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR) Mumbai, Maharashtra, India

²Research Scholar, Department MCA, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR) Mumbai, Maharashtra, India

³Assistant Professor, Department MCA, Thakur Institute of Management Studies, Career Development & Research (TIMSCDR) Mumbai, Maharashtra, India

Received Date: March 10, 2026

Accepted Date: June 09, 2026

Published Date: June 26, 2026

Citation: Shardul Santosh Kolte, Saurabh Sanjay Kumar, Shirshendu Maitra. A Study on the Ethical Implications and Data Privacy Challenges in the Age of Artificial Intelligence. *Current Trends in Information Technology*. 2026; 16(2): 1–13p.

boundaries of automation and decision-making. This rapid change is facilitated by the fact that AI systems can process and learn huge amounts of data and thus can perform tasks previously done by using human cognitive skills. Consequently, AI has already become one of the foundations of the global digital economy, with unprecedented opportunities for innovation and development. Nevertheless, the same basis on which AI builds its work on data has brought about a new set of ethical and privacy issues. The information that drives AI systems is usually sensitive in terms of personal information, such as patterns of behavior, biometrics, and location details. With the ever-increasing use of AI systems in our daily lives by introducing facial recognition, recommendation algorithms, and conversational agents, among others, the question of ethics in the collection, use, and decision-making

of data has received a lot of attention. Issues of fairness, transparency, accountability, and protection of personal data are no longer discussed at the theoretical level but are debated and are an urgent issue for society and policymakers. Although the entire world is aware of these issues, there is an acute lack of correspondence between the moral standards of AI development and the reality of AI implementation.

The pace of AI technology development is often greater than the mechanisms used to regulate it for accountability. Some regulatory regimes, such as the European Union General Data Protection Regulation (GDPR) [1] and the Digital Personal Data Protection (DPDP) Act of India, have attempted to institute legal protection for individual privacy. However, when these structures come into operation, there are many loopholes in terms of enforcing these frameworks, technological flexibility, and cross-border use. Therefore, personal data security in AI-based settings is not uniform and is subject to abuse. Algorithm bias, black box systems, and erosion of public trust are ethical dilemmas that exacerbate this situation.

Trained AIs can reinforce systematic discrimination in hiring, lending, policing, and social media moderation. In addition, many AI systems cannot be explained, compromising accountability; thus, it is difficult to hold individuals responsible in the case of mistakes. All these issues have developed what researchers term the principle-to-practice gap, a disjuncture between the principles of ethical AI and their application in the industry and in social systems.

In this study, the gap was found to be the core issue contributing to the ethical and privacy threats of AI in the current context. Although many organizations purport to exercise ethical systems, they are merely performing compliance at shallow levels, as they are merely concerned with corporate optics and not actual governance. Likewise, despite governments passing data protection legislation, they find it hard to control new AI applications that cross jurisdictional and ethical boundaries. Thus, it is important to bridge the gap between the principles and practice of the gap so that there can be a balance between technological advancement and societal welfare.

The significance of the present study is that it is an evidence-based analysis that incorporates both empirical evidence and conceptual insights. Although the current literature deals with the technical and regulatory aspects of AI ethics separately, this study uses a mixed-methods approach to merge the two sides. This article is a quantitative survey accompanied by qualitative data in the form of four case studies on Amazon AI Recruitment Tool, Clearview AI, Healthy Chef GPT, and Cax TaskPal. Combined, these approaches will provide a thorough analysis of societal views, regulatory capabilities, and ethical misconduct in AI systems.

This study has the following four objectives:

1. This study discusses the ethical aspects of using AI systems in real-world applications, especially in data-driven environments.
2. The most important issues related to AI-assisted data processing and algorithmic decision-making are privacy.
3. To compare and contrast international data protection laws, such as the GDPR and the Indian DPDP Act, to determine their practicability in the AI era.
4. To suggest a system of best practices and policy suggestions to help bridge the gap between theory and practice in ethics related to technology.

Through these aims, the current research adds to the existing discussion of AI governance, data protection, and trustworthy AI. The results offer practical information to policymakers, developers, and organizations that want to establish AI platforms that are not only effective and innovative but also transparent, equal, and in line with human values.

Finally, the three main hypotheses that led to this study are aimed at testing the main dimensions of the problem.

- *H1*: The current laws on data privacy do not adequately address the reality issues presented by data processing systems that are conducted by AI.
- *H2*: AI systems with no ethical codes of conduct or regulatory actions tend to infringe on user data privacy.
- *H3*: The transparency of AI systems handling personal data is positively and significantly related to public trust in the system.

By empirically confirming these hypotheses, the present study contributes to the development of knowledge regarding the changing intersection of AI ethics, data privacy, and user trust. The final objective is to present a strategic roadmap on how to align AI innovation with the ethics of moral accountability and law.

LITERATURE REVIEW

The overall analysis of the latest academic literature (2021–2025) demonstrates that the ethical, legal, and privacy aspects of Artificial Intelligence (AI) have become a defining research issue in various fields. The literature review shows that 26 studies indicate a growing debate on the issues of data governance, algorithm bias, transparency, and accountability, and point to an expanding divide between the principle and practice of responsible AI system deployment. This section combines the prevailing themes, theoretical approaches, and gaps in the literature that inform this study's research questions.

Data Privacy and Security as a Primary Concern

In the literature, the most important ethical issues in AI adoption are data privacy and security concerns. AI systems, specifically those based on Large Language Models (LLMs) and large-scale deep learning models, require massive amounts of data to be useful, which exposes their inefficiency in data collection, processing, and storage in many cases [2–4].

Research highlights that AI has been used to create massive data monopolies, unethical data mining, and violations of personal data [5, 6] because of the use of user-generated content. Research on the LLM app ecosystem indicates that third-party applications often gather more information than they need to operate, and sometimes sensitive data are collected (e.g., passwords and health data), which is in direct contravention of the rules and regulations of the platform [4, 7].

Domain-specific risks can be especially clear in the case of healthcare, where AI-based diagnostic technologies have accessed patient data [8], and in education, where AI-powered technologies have misused student data [9]. Researchers believe that data protection is not only a legal compliance challenge but also the ethical foundation of responsible AI implementation [2, 10, 11]. The lack of privacy-sensitive architectures and governance frameworks will make AI systems a threat to people's trust and enhance social inequalities.

The “Principle-to-Practice Gap” in Ethical AI

One of the most recurrent themes in several studies is the lack of connection between high-level ethical principles (fairness, transparency, accountability) and their practical application to AI systems [3, 11, 12]. Researchers refer to this as the principle-to-practice gap, or a situation in which AI creators recognize the importance of ethical issues but do not have effective tools, institution-wide incentives, or policies to make them practical [12, 13].

Thalpage et al. [12] concluded that the most challenging ideals to operationalize are human-centered values because developers are usually subjected to time, cost, and performance concerns that prevail over ethical decision-making [14]. It also emphasizes that practitioners' ethical awareness is usually superficial as they are compelled to pass a checklist as opposed to actual participation.

Such systemic disconnection can be explained by three fundamental causes: (1) conceptual vagueness in terms of quantifiable ethical standards; (2) lack of organizational mechanisms of accountability; and (3) conflicting incentives between ethical responsibility and business efficiency [13, 15, 16].

The fact that this gap has not yet been closed underlines the necessity of the current research, which involves quantitative data analysis along with qualitative evidence to uncover the ways these principles can be applied in reality.

The Inadequacy of the Regulatory Landscape

The regulatory frameworks of AI are still disjointed and responsive. Although the General Data Protection Regulation (GDPR) of the European Union remains the international standard in terms of data privacy, it did not intend to target the inductive possibilities of contemporary AI systems [10]. The Mosaic Effect, in which AI models can be used to draw sensitive conclusions based on data that might be considered harmless, is a direct threat to the conventional understanding of consent and anonymization [17].

Comparative analysis reveals significant variance in international regulatory policies. The EU adopts a rights-based precautionary approach characterized by accountability and explainability [18]; the United States is addicted to flexible sectoral models based on market regulation; and the governance approach in China is based on AI innovation and state control [18, 19, 20]. In India, a new law called the Digital Personal Data Protection (DPDP) Act (2023) was hailed as a breakthrough; however, it still does not include provisions for algorithmic transparency, automated profiling, and AI-specific accountability [21]. According to scholars, in the absence of special, AI-focused legal rules, these regulations cannot compensate for the upcoming risks, and the enforcement gap will increase [14, 7].

Moreover, they comment on the dire necessity to harmonize the regulatory environment across borders to ensure the ethical management of AI, and because disjointed legal environments are perilous to accountability and innovation, they advocate this idea [22, 13].

The Role of Transparency in Building Public Trust

Trust and transparency are critical enablers of the ethical use of AI. It is always found that the more people trust AI, the more they can comprehend the working of AI and countercheck it [12, 23]. Nonetheless, based on empirical studies, transparency is a significant failure, where less than 6% of AI-driven applications report transparent data-handling practices in their privacy policy [5].

Transparency is not only a technical value but also a socio-ethical creation that contributes to institutional validity and consumer trust [23]. Organizations that share their data governance practices are more likely to have increased user retention and brand credibility. On the other hand, AI system opacities result in the phenomenon of the black-box environment, where accountability is devolved, and the end-users are not aware of the utilization of their data or its monetization.

The literature reviewed highlights that fairness and accountability are based on transparency. Open auditing and explainable AI (XAI) models are becoming common as some of the most important measures for regaining trust in automated decision systems [24, 16].

This view is directly in line with Hypothesis H3 of the current research: that public trust in AI has a positive correlation with the transparency of data processing.

Proposed Solutions: Technical and Governance Frameworks

To overcome the ethics implementation gap, two key solution domains have been developed: privacy-saving technologies and governance systems.

1. *Technical innovations:* Privacy-preserving AI systems, including Differential Privacy, Federated Learning, Split Learning, and Homomorphic Encryption, allow data analysis without violating the privacy of individuals [5, 4]. These schemes strive to achieve a utility-confidentiality balance; however, there is always a trade-off between accuracy and privacy. According to Chen [5] and Das [4], despite tremendous advancements, these techniques have not been practically applied in the real world owing to the cost of infrastructure and the absence of knowledgeable developers.

2. *Governance frameworks:* These Governance-oriented research suggesting systemic approaches to the operationalization of ethical AI [22]. The Data-Technology-People Process (DTPP) and [13] Technical-Organizational-Human-Regulatory (TOHR) models promote the use of ethics in all phases of AI development, implementation, and management. Additional models, such as Hahnel's Five Ps of Ethical Data Handling (provenance, protection, purpose, preparation, and privacy), can also be used to offer practical guidelines on responsible data management [25, 26].

These architectures emphasize the philosophy of holistic governance, which streamlines human supervision, regulatory adherence, and technical transparency to develop reliable AI ecosystems [25, 22, 13].

Identified Research Gaps

Although certain strides have been made, several gaps have been identified in the literature.

1. Insufficient empirical confirmation of the practical efficiency of the suggested governance frameworks and moral codes is still a weakness [26, 13, 14].
2. The gaps in regulations still restrict the effects of the current legislation on data protection, particularly in the developing world, where legal tools that address AI continue to be developed [15, 17].
3. The human element of ethical implementation, such as bias by the developer, deficient training, and mental overreliance on automation, are under-researched [11, 14].
4. The problem of the dual-use dilemma, in which AI systems intended to serve a useful purpose are now used maliciously (e.g., in misinformation or surveillance), is an increasingly worrying issue that existing frameworks fail to adequately tackle [6, 19].

These research gaps warrant the mixed-method nature of the present study, which combines a quantitative analysis of the population's view on the matter and qualitative case studies to gain empirical insight into the ethical and privacy concerns of AI in the changing legal ecosystem.

RESEARCH METHODOLOGY

The study methodology is a mixed-method design that combines quantitative and qualitative studies to create a unified perspective on the issues of ethics and data privacy brought about by Artificial Intelligence (AI) as a novel technology. This two-sided approach allows for statistical generalization and balancing contextual depth between quantifiable trends and reality. The mixed-method design was chosen because the three hypotheses of the study were to correlate public perceptions with real-life facts about AI-related ethical failures.

Research Design

This research uses a concurrent triangulation design, in which quantitative and qualitative data are gathered and analyzed simultaneously during the research process. The quantitative part consisted of a structured descriptive inferential survey, and the qualitative part comprised a multiple case study analysis.

This design improves the validity and reliability by triangulation, where the researcher can cross-verify the results. The points of intersection between the two types of data contribute to the strength of the conclusions constructed there; the points where they differ provide the possibilities of more profound theoretical thought. Such a mixed method enhances the empirical basis of the study because it establishes a link between trends in human perception and real-life data on examples of ethical or privacy infringements in AI systems.

Data Collection and Description

These data were gathered in two different formats: a primary online survey and a case study collection. Multiple sources were used to guarantee the breadth and richness of the context.

The design and distribution of the survey instruments will be completed as follows:

Survey Instrument Design and Distribution

Google Forms were used as the main quantitative tool to develop a structured online questionnaire. The survey consisted of 25 questions divided into five logical parts.

1. Demographics,
2. AI Awareness and Usage,
3. Ethical Implications,
4. Data privacy concerns, and
5. Trust and recommendations.

The questionnaire used multiple-choice and 5-point Likert scale questions to elicit perceptions of the study variables. It was published online and sent to respondents from university and IT-related workplaces. N = 52 valid responses were included in the final dataset.

The sample was largely young (61.5% of the respondents were between 18-24 years old), male (67.3%), and well educated (88.4% of the respondents held undergraduate or postgraduate degrees).

This article indicates that a digitally literate society is in a good place to assess AI ethics and data privacy concerns.

Case Study Selection and Corpus

The qualitative data were in the form of four case studies, which were chosen using a purposive sampling technique. The criteria used for selection were as follows:

- a. Direct impact on the ethical or data privacy lapses in AI systems,
- b. Strong academic or societal influence, and (c) sector diversity to obtain multi-domain insights.

The last case corpus involved:

Algorithms and discrimination in automated hiring: Amazon AI Recruitment Tool.

- *Clearview AI* - massive personal data theft by scraping facial images.
- *Healthy chef GPT* - exploitation of third-party data in generative AI ecosystems.
- *Cax taskpal* - failure in governing platforms and soliciting unethical data.

These cases were chosen to reflect different but related aspects of AI ethics, bias, privacy, transparency, and governance.

Data Analysis Techniques

The quantitative data were analyzed using a combination of statistical analysis and qualitative data using thematic analysis to answer the research questions.

Quantitative Analysis

The GNU PSPP was used to analyze the survey data. The analysis was performed in two phases. First, descriptive statistics (frequencies, percentages, means, and standard deviations) were performed on all variables to provide an overview of the sample characteristics and overall notion of AI ethics and privacy. Second, inferential statistics were applied to test the research hypotheses. The Chi-Square test of Association was used to test whether the relationship between the categorical variables, including awareness of data privacy law and perceived law effectiveness, was statistically significant (H1, H2). The concept of transparency variables was used to construct a predictive model based on the intention to comprehend how transparency variables could predict the overall trust of a user in AI systems to offer a solid test of H3. In all inferential tests, a p-value below 0.05 was considered statistically significant.

Qualitative Analysis

The chosen case studies were thematically analyzed using Braun and Clarke's systematic procedure. Every case was broken down to identify:

The primary ethical issue:

- It's technical or organizational situation,
- The character of the injury or scandal, and
- Its effects on AI governance and user trust. Cross-referentiality with the quantitative results was then performed with emergent themes, which included, but were not limited to, algorithmic bias, lack of transparency, and regulatory insufficiency. This combination of data made the convergence of patterns between empirical evidence and popular perception possible, which increased the explanatory power of the research.

Ethical Considerations and Validity

All data were gathered according to the principles of ethical research. The survey was voluntary and anonymous, guaranteeing informed consent and confidentiality of the data collected. The case studies only used publicly available data, of which the academic and journalistic sources were verified.

Methodological triangulation, peer-reviewed data on cases, and consistency tests between descriptive and inferential results were employed to strengthen validity. These measures, in combination, guarantee the reliability and integrity of the research results.

RESULTS AND ANALYSIS

This section presents the empirical results of the research, including both quantitative surveys and qualitative case studies. GNU PSPP was used to analyze the data, and the statistical methods were descriptive and inferential statistics to test the research hypotheses.

Quantitative Survey Results

The participants who took part in the survey were 52 individuals, which constituted the quantitative basis of this study. The respondents were mostly young (61.5% were between 18 and 24), men (67.3%), and highly educated (88.4% possessed undergraduate or postgraduate degrees). The majority of them were students (51.9%).

Descriptive Findings

The descriptive analysis showed that 80.7% of the interviewees responded as very/moderately familiar with AI, and 94.2% had used AI tools in the past 12 months, mostly chatbots (90.4%).

There was complete agreement with 100 percent concurrence that AI is an ethical issue, and the two areas most discussed included the misuse of AI to cause harm (82.7%) and employment displacement (61.5%).

Additionally, 73.1% of participants thought that AI posed a threat to personal data privacy, and 96.2% of respondents felt that AI companies should be legally obligated to publish what they did with their data.

Nonetheless, 77 percent of them said that they seldom or never read privacy policies, despite the widespread concern (see Table 1 and Figures 1 and 2).

Hypothesis Testing

The three hypotheses (H1-H3) were tested using inferential statistics. Chi-Square and Linear Regression tests were performed, and the results are summarized in Table 2.

The discussion suggests that people are well aware of privacy laws, but they do not trust their implementation (H1 supported). There were no significant relationships between adherence to ethical

guidelines and data breaches (H2 not supported). Nevertheless, user trust had a strong correlation with transparency (H3 supported) and a predictive relationship ($R^2 = 0.56$).

Qualitative Case Study Analysis

Four case studies were thematically analyzed to supplement the survey findings. These are real-life examples of the manifestations of ethical and data privacy issues in actual AI systems.

Amazon's AI Recruitment Tool

Evidence of algorithmic bias, in which AI allows gender discrimination by learning from biased historical data. This is a manifestation of the ethical principle of fairness, and it directly aligns with the concern of the survey on AI decision-making being biased.

Clearview AI–Facial Recognition and Mass Surveillance

An example of an information privacy breach is when public pictures are scraped to train AI. This demonstrates the principle-to-practice gap in the area of data protection that most of the respondents (73.1%) mentioned.

Healthy Chef GPT–Excessive Data Collection

Demonstrated a breach of the principle of data minimization. The application has been gathering sensitive user health information through third-party advertising options, highlighting the necessity for more stringent control and openness of information.

Cax TaskPal–Platform Governance Failure

An AI application that asked users to provide passwords against the policy. This shows a lack of accountability and responsibility of the platforms and proves that ethical guidelines cannot be effective without enforcement.

Summary of Findings

Table 3 presents a consolidated overview of the key quantitative and qualitative findings of this study. The results indicate a strong awareness of the ethical concerns associated with AI technologies, with all respondents acknowledging the importance of ethical considerations in AI deployment. Privacy-related issues also emerged as a significant concern, as the majority of participants perceived AI systems as potential threats to personal data security. Furthermore, the statistical analysis revealed a significant relationship between transparency and user trust, highlighting the importance of explainable and accountable XAI systems.

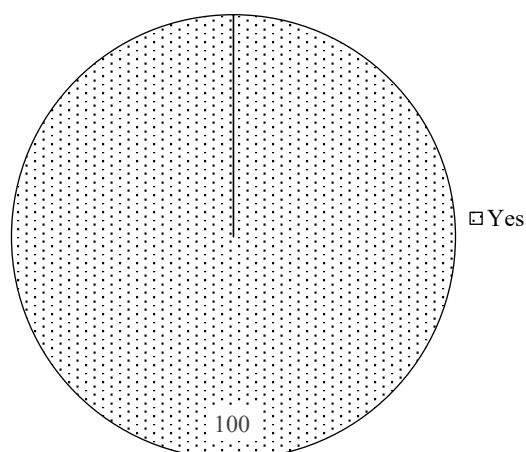


Figure 1. Pie chart showing ethical concerns raised by AI.

The case studies included in the analysis further demonstrate that ethical challenges often arise when governance mechanisms are weak or are poorly enforced. Together, these findings emphasize the need for transparent practices, robust privacy protection, and effective regulatory frameworks to ensure the responsible development and use of artificial intelligence. As summarized in Table 3, both empirical evidence and real-world examples point to the critical role of ethics and governance in fostering public trust in AI systems.

DISCUSSION

The results of this study highlight the presence of a large principle-to-practice gap in the ethical use of Artificial Intelligence (AI) systems. Although the responsiveness toward AI ethics and data privacy seems to be remarkably high among the interviewees, this awareness has not been effectively transferred into confidence in organizational or legal regulations. The following discussion combines the quantitative results with the qualitative case study results to provide an overall picture of the observed phenomena.

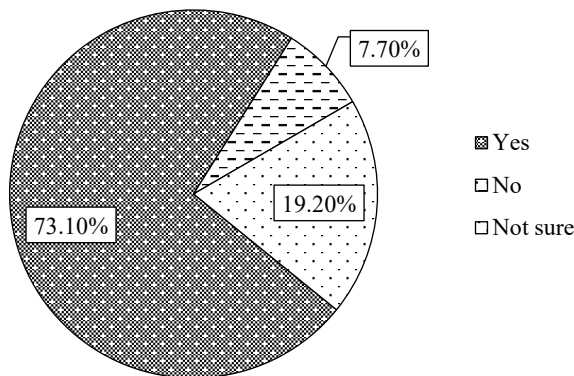


Figure 2. Pie chart showing ethical concerns raised by AI.

Table 1. Summary of respondent demographics and awareness.

Parameter	Percentage (%)
Age 18–24	61.5
Male respondents	67.3
Undergraduate/postgraduate	88.4
Students	51.9
Familiar with AI	80.7
Used AI tools in last 12 months	94.2
Agree ai raises ethical concerns	100.0

Table 2. Summary of hypothesis test results.

Hypothesis	Variables tested	Test used	P value	Result
H1	GDPR/DPDP Awareness versus. law effectiveness	Chi-square	< 0.01	Supported
H2	Org. Guidelines vs. experienced breach	Chi-square	0.885	Not supported
H3	Transparency vs. User Trust	Linear regression	< 0.001	Supported

Table 3. consolidated summary of quantitative and qualitative insights.

Research focus	Quantitative finding	Supporting case study
Ethical awareness	100% agree AI raises ethical issues	Amazon ai recruitment tool
Data privacy concern	73.1% perceive AI as a privacy threat	Clearview AI
Transparency and trust	$P < 0.001$ (supported)	Healthy chef GPT
Governance failures	Ethics ineffective without enforcement	CAX TaskPal

The Space between Recognition and Implementation

According to the quantitative findings, it can be concluded that the majority of the respondents are familiar with the current data protection laws (like General Data Protection Regulation (GDPR) and the Digital Personal Data Protection (DPDP) Act in India). However, the results of the chi-square test proves that the disconnection between awareness and trust in the effectiveness of these laws is statistically significant ($p < 0.01$). This means that being aware of regulations does not guarantee perceived protection. An example of this enforcement lapse is the facial recognition information scraping conducted by Clearview AI despite privacy laws. These gaps indicate that legal provisions with weak implementation mechanisms cannot establish user trust in AI systems.

Ethical Oversight and accountability in the organization

The second hypothesis (H2) addressed whether ethical standards of adherence are associated with avoiding data breaches. The insignificance of the statistical significance ($p = 0.885$) indicates that ethical policies do not always eliminate unethical outcomes. This is in line with the qualitative data of the Cax TaskPal, which revealed that although there were general ethics in place, there was no form of governance and no monitoring of the policies of the company, which resulted in a direct breach of ethics. This implies that there should be clear organizational responsibility not only by documents but also by action, frequent audits, and open communication.

Transparency as a Foundation for Trust

Transparency was found to be an important predictor of user trust and was statistically proven ($p < 0.001$) through the Amazon AI Recruitment Tool and Healthy Chef GPT cases. The regression model showed that users who were aware of how AI decisions were made, had higher levels of trust. These outcomes confirm that transparency is not only a recommendation for ensuring sustainable AI adoption but also an operational requirement. Systems developed using explainability-by-design are better positioned to gain user confidence and achieve regulatory approvals.

Ethics, Governance and Technology Cross-Linking

The case study/survey data triangulation demonstrates that it is impossible to have ethics, governance, and technology operating in isolation. For example, technical approaches such as distributed machine learning or differential privacy provide valid opportunities to reduce risks; however, they need to be strengthened with human control and legal responsibility. This is consistent with modern ethical AI paradigms of responsible innovation- a trade-off between technological and social change.

Implications for Policy and Practice

The implications of the findings for policymaking are that national and international regulators ought to shift to technology-adaptive frameworks that change with AI capabilities. For practitioners, this study supports the message that ethical assessment points should be implemented at every stage of the AI development cycle, from data gathering to implementation. To operationalize the principles of fairness, accountability, and privacy protection, organizations should invest in ethics review boards, transparency audits, and public reporting.

Synthesis with Previous Research

The results of this study are consistent with those of previous studies, which have also found the lack of a way to translate ethical intent into practice to be a problem. However, this study provides the widest scope of discussion, as it integrates empirical data on users and provides real-life case studies, presenting a dual perspective that bridges societal perception and organizational conduct. This dual-lens approach helps gain better insight into how trust deficits are created and maintained in the AI ecosystem.

Implications for Policy and Practice

To conclude, the paper confirms that:

- There is a high level of awareness regarding AI ethics and data protection legislation, but their implementation is low.

- Ethics systems should transform into concepts on paper to executable methods of governance.
- The only important determinant of user trust is transparency.
- The development of ethical AI necessitates the joint efforts of technology developers, policymakers, and regulators.

Finally, this study supports the idea that responsible AI cannot only be related to harm reduction but also to the introduction of ethical reasoning, transparency, and accountability in all steps of AI innovation.

CONCLUSION AND FUTURE WORK

This study examined the ethical implications and issues of data privacy related to the rapid implementation of Artificial Intelligence (AI). This study, based on a mixed methods design that combined a quantitative survey and qualitative case analysis, offered both empirical and conceptual insights into the so-called principle-to-practice gap in the context of ethical theory and real-world AI implementation.

The results demonstrate conclusively that although awareness of AI ethics and privacy is high among the population, it is not reflected in the confidence in the implementation of existing legal and organizational provisions. The statistically significant correlation ($p < 0.01$) between awareness of laws such as the GDPR and the DPDP Act and the perceived inefficiency of their application proves the urgency of the need to build a stronger system of governance. Furthermore, the fact that the relationship between ethical policies and actual protection against data breaches does not have a significant level of correlation ($p = 0.885$) indicates that the intentions are not reflected in real operations.

This finding was supported by qualitative evidence based on case studies such as Clearview AI and Cax TaskPal, where regulatory failures, misuse of data, and lack of accountability frameworks were identified. In contrast, the AI Recruitment Tool and Healthy Chef GPT of Amazon focused on the fact that transparency and explainability are the foundation of user trust, which underlines the quantitative finding that transparency is a statistically significant predictor of trust ($p < 0.001$). This study concludes that responsible AI will only be realized when ethics, governance, and technical innovation are synchronized. Ensuring that there is an improvement in data privacy legislation, transparency tools, and ethical auditing of AI use is necessary to close the gap between awareness and assurance. Moreover, to trust AI based on real accountability and not on claims, organizations need to incorporate ethical compliance in all phases of the AI lifecycle, including data collection and model-making, deployment, and monitoring.

Practical Implications

From a managerial and policy perspective, the research underscores the need for:

- *Transparent AI practices*: Developers should disclose data sources, decision-making processes, and algorithmic limitations to ensure public trust.
- *Adaptive regulatory frameworks*: Governments must implement dynamic, technology-agnostic privacy laws that evolve with AI advancement.
- *Ethical governance integration*: Organizations should establish internal AI ethics committees to evaluate risks, fairness, and compliance prior to deployment.
- *Public digital literacy initiatives*: Increasing user awareness of data rights and privacy control can enhance collective ethical accountability.

Limitations

Although this study offers insightful ideas, it has some limitations need to be mentioned. The number of respondents (52) was small and not diverse enough to be statistically generalized. In addition, the fact that self-reported survey responses are prone to bias. Qualitative case studies, as descriptive as they

are, are restricted to publicly available documentation and might be inadequate in reflecting internal organizational processes.

Future Scope of Research

Further studies should focus on increasing the sample size to encompass a variety of professionals in diverse industries, including healthcare, finance, and education, to gain a wider perspective on the ethical issues that are specific to the industry. Longitudinal research may also examine changes in AI ethics perceptions as the regulatory context develops. State-of-the-art modeling strategies, such as structural equation modeling (SEM), may be applied to determine the causal interrelations between awareness, trust, and ethical compliance.

My other good suggestion for a future effort would be to interview AI developers, policymakers, and data protection officers to obtain firsthand experience on the difficulty of ensuring an ethical AI implementation project is operational. This would fill the empirical gap between user perception and institutional practice, which would increase the basis of international AI governance standards.

Concluding Remarks

Finally, the research concludes that the ethical and privacy dilemmas of AI are not issues that can be resolved through pure technology but rather socio-legal and governance problems and thus require a multi-stakeholder strategy. To fill the current gap in ethics, it is necessary to resort to open communication, strict management, and human-oriented innovation. Responsible AI is not an ambition to become a policy but a shared duty, that is, a marker of the reliability and viability of future technological ecosystems.

Acknowledgment

We convey our deep appreciation to Prof. Shirshendu Maitra, our research guide at Thakur Institute of Management Studies, Career Development and Research (TIMSCDR) and the priceless assistance, wise feedback and unending support that he has offered us during this course of research.

Our subject teacher, Prof. Ashwini Renavikar, also deserves our hearty thanks and appreciation, and we will not forget her highly valuable academic support, motivation, and constructive suggestions that contributed to the perfection of our work.

The TIMSCDR has helped us with the required academic infrastructure and resources, and all survey participants and reviewers have contributed to our research with their inputs.

Finally, we owe our families and peers undying faith and support throughout this research process.

REFERENCES

1. Malalla B, Al Mubarak M. Ethical challenges in artificial intelligence technology: business applications. In: Al Mubarak M, editor. Sustainable Digital Technology and Ethics in an Ever-Changing Environment. Vol. 1. Springer Nature; 2025. p. 27-46. doi:10.1007/978-3-031-86712-5_2.
2. Timan T, Mann Z. Data protection in the era of artificial intelligence: trends, existing solutions and recommendations for privacy-preserving technologies. In: The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem. Springer International Publishing; 2021. p. 153-75.
3. Kordzadeh N, Ghasemaghaei M. Algorithmic bias: review, synthesis, and future research directions. Eur J Inf Syst. 2022;31:388-409. doi:10.1080/0960085X.2021.1927212.
4. Das BC, Amini MH, Wu Y. Security and privacy challenges of large language models: a survey. ACM Comput Surv. 2025;57:1-39. doi:10.1145/3712001.
5. Chen J, Yan H, Liu Z, Zhang M, Xiong H, Yu S. When federated learning meets privacy-preserving computation. ACM Comput Surv. 2024;56:1-36. doi:10.1145/3679013.

6. Ganesh P, Tran C, Shokri R, Fioretto F. The data minimization principle in machine learning. In: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency; 2025. p. 3075-93. doi:10.1145/3715275.3732195.
7. Kaushik K, Khan A, Kumari A, Sharma I, Dubey R. Ethical considerations in AI-based cybersecurity. In: Kaushik K, Sharma I, editors. Next-Generation Cybersecurity: AI, ML, and Blockchain. Springer Nature; 2024. p. 437-70. doi:10.1007/978-981-97-1249-6_19.
8. Lastrucci A, Pirrera A, Lepri G, Giansanti D. Algorethics in healthcare: balancing innovation and integrity in AI development. Algorithms. 2024;17:432. doi:10.3390/a17100432.
9. Huang L. Ethics of artificial intelligence in education: student privacy and data protection. Sci Insights Educ Front. 2023;16:2577-87. doi:10.15354/sief.23.re202.
10. Kashefi P, Kashefi Y, Ghafouri Mirsarai A. Shaping the future of AI: balancing innovation and ethics in global regulation. Uniform Law Rev. 2024;29:524-48. doi:10.1093/ulr/unae040.
11. Tahaei M, Constantinides M, Quercia D, Muller M. A systematic literature review of human-centered, ethical, and responsible AI. arXiv [Preprint]. 2023 Feb 10. arXiv:2302.05284.
12. Thalpage N. Unlocking the black box: explainable artificial intelligence (XAI) for trust and transparency in AI systems. J Digit Art Humanit. 2023;4:31-6. doi:10.33847/2712-8148.4.1_4.
13. Spehar GD, Mittal A. Responsible AI horizons: a multi-dimensional framework for verifiable AI behavioral assessment with cryptographic verification. In: International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISSET); 2026. Institute of Electrical and Electronics Engineers; p. 1-8. doi:10.1109/ICAISSET66439.2026.11541913.
14. Sayyed H. Artificial intelligence and criminal liability in India: exploring legal implications and challenges. Cogent Soc Sci. 2024;10:2343195. doi:10.1080/23311886.2024.2343195.
15. Koplin JJ. Dual-use implications of AI text generation. Ethics Inf Technol. 2023;25:32. doi:10.1007/s10676-023-09703-z.
16. Hagerty A, Rubinov I. Global AI ethics: a review of the social impacts and ethical implications of artificial intelligence. arXiv [Preprint]. 2019 Jul 18. arXiv:1907.07892.
17. Wei Y, Carney J, Stamper J, Belmont N. From defense to advocacy: empowering users to leverage the blind spot of AI inference. arXiv [Preprint]. 2026 Jan 16. arXiv:2601.11817.
18. Pang CK. A comparative analysis of artificial intelligence regulation: implications for Singapore. Sing Acad Law J. 2025;37:189-232.
19. Kumar D, Sahu CK. Artificial intelligence governance and social policy divergence: a comparative political economy perspective on global AI regulation. Int J Sociol Soc Policy. 2026:1-25. doi:10.1108/IJSSP-02-2026-0129.
20. Burton S, Habli I, Lawton T, McDermid J, Morgan P, Porter Z. Mind the gaps: assuring the safety of autonomous systems from an engineering, ethical, and legal perspective. Artif Intell. 2020;279:103201. doi:10.1016/j.artint.2019.103201.
21. Ebenibo L, Enyejo JO, Addo G, Olola TM. Evaluating the sufficiency of the Data Protection Act 2023 in the age of artificial intelligence (AI): a comparative case study of Nigeria and the USA. Int J Sch Res Rev. 2024;5:88-107. doi:10.56781/ijssr.2024.5.1.0044.
22. Swarnali SH. AI-enhanced ERP financial intelligence systems for real-time business analytics and risk decision support. ASRC Procedia Glob Perspect Sci Scholarsh. 2025;1:2703-41. doi:10.63125/t1zw3w09.
23. Schmidt P, Biessmann F, Teubner T. Transparency and trust in artificial intelligence systems. J Decis Syst. 2020;29:260-78. doi:10.1080/12460125.2020.1819094.
24. Tiwari R. Explainable AI (XAI) and its applications in building trust and understanding in AI decision making. Int J Sci Res Eng Manag. 2023;7:1-3. doi:10.55041/IJSREM17592.
25. Narayanan DB. Data engineering for responsible AI: architecting ethical and transparent analytical pipelines. Int J Emerg Res Eng Technol. 2024;5:97-105.
26. Chang X. Gender bias in hiring: an analysis of the impact of Amazon's recruiting algorithm. Adv Econ Manag Polit Sci. 2023;23:134-40. doi:10.54254/2754-1169/23/20230367.