International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
ISSN Online: 2349-4182 ISSN Print: 2349-5979
Received: 19-05-2025, Accepted: 18-06-2025, Published: 04-07-2025
Volume 12, Issue 7, 2025, Page No. 28-32

Ethical and AI concerns in data privacy- A charismatic dilemma

Dr. Neha Garg[1], Dr. Bhavana Sharma[2]
[1] Assistant Professor, Department of Law, Institute of Management and Research, Bharati Vidyapeeth Deemed to be University, Odisha, India
[2] Associate Professor, Birla Global University, Bhubaneswar, Odisha, India

Abstract
The role of privacy-first design principles, multi-stakeholder collaboration, and international harmonization of laws is emphasized as critical strategies to address these challenges. By synthesizing insights from legal, technological, and ethical perspectives, this study underscores the importance of robust and adaptive data privacy legislation in building trust in AI systems. It concludes by providing actionable recommendations for policymakers, industry leaders, and researchers to promote accountable AI practices that align with societal values and ethical standards. Ultimately, the paper advocates for a balanced approach that enables technological advancements while safeguarding individual rights and societal well-being

Keywords: Artificial intelligence (AI), accountability, transparency, explainability, privacy-first design, AI regulation, ethical innovation

Introduction

When AI and data privacy rules come together, they show the bigger problems that can happen when data is misused and unfair treatment happens. AI systems are only as good as the data they are taught on. If they are given biased data, they may make biased choices, which can make society's problems worse. Because of this, privacy laws are very important for making sure that the ways we gather and handle data don't accidentally lead to unfair results. For example, rules that say certain personal information has to be made anonymous can help stop AI programs from being biased and treating people unfairly because of their race, gender, or culture. But putting these rules into action comes with its own set of problems [1]. AI is constantly changing and adapting, which is faster than the speed at which standard governmental processes work. This difference makes it take longer for the legal system to keep up with and control new technology advances. Also, because the internet and digital technologies are used all over the world, AI systems often work in more than one state, which makes it harder to police local data privacy laws. For this global operation to work, the current scattered and uneven foreign approach to data privacy needs to be brought together. However, these problems aside, it is very important to have strong data privacy laws. What makes the responsible use of AI technologies very important is how well we can control them and make sure they follow the law and social norms [2]. Without these rules, AI's risks could outweigh its benefits, making people less likely to believe it and less likely to use technologies that could change the world. These rules are very important for both protecting people's rights and making sure that AI works in a decent way. Artificial intelligence (AI) is always getting better, so our laws need to change quickly and smartly to keep an eye on these technologies and make sure they grow in a way that is fair, just, and clear. As this paper will show, using data privacy rules to hold AI ethically responsible is not just a task for regulators; it is also a social necessity.

Examination of situations where privacy laws failed and the lessons learned

Even with the best intentions, data protection rules have not always been able to fully protect people or make sure that AI is used in a responsible way. For instance, the use of AI in social media ads has sometimes gotten around user consent systems, resulting in major data breaches. It was found that AI used in predictive police made racial attitudes worse in another case, even though there were privacy and anti-discrimination rules in place. Most of the time, these mistakes are caused by holes in the law, bad regulation, or technical problems like not enough anonymization. These cases show how important it is to keep making laws better, making enforcement stronger, and using new tools to better deal with the complicated problems AI brings up. They also show how important it is to think about ethics when developing AI from the start, instead of adding them in as an addition.

Table 1: Analysis of failure

Situation	Failure Rate (%)	Privacy Breach Rate (%)	Bias Incidence Rate (%)	Compliance Failure Rate (%)
Social Media Advertising	80	80	20	25
Predictive Policing	70	30	70	30
Facial Recognition at Events	65	65	45	20
AI Loan Approvals	75	35	75	35
AI in Employee Monitoring	60	60	22	40

The table 1 shows a worrisome 80% failure and privacy breach rate for social media advertising. This shows the serious effects of advertising algorithms that don't handle data and consent properly. Since bias doesn't happen very often, it seems like the biggest problem in this area is not having enough information available and people using data without permission, not unfair practices. But the fact that 25% of compliance attempts fail shows that it's still hard to get business practices to match law requirements. Another sensitive application, predictive police, has a significant bias incidence rate of 70%. This shows, in figure 1, the serious ethics problems of racial profiling and other forms of discrimination that can happen when AI systems are not properly trained or managed. Even though the rate of privacy breaches is lower, the high rate of bias shows that we need stricter control by regulators and better ways to handle data to stop discrimination. When facial recognition is used at events, there are a lot of cases of both data breaches and unfair treatment based on AI that doesn't understand something right. These problems are made worse by the fact that the technology is being used by everyone, which raises serious worries about privacy and consent.

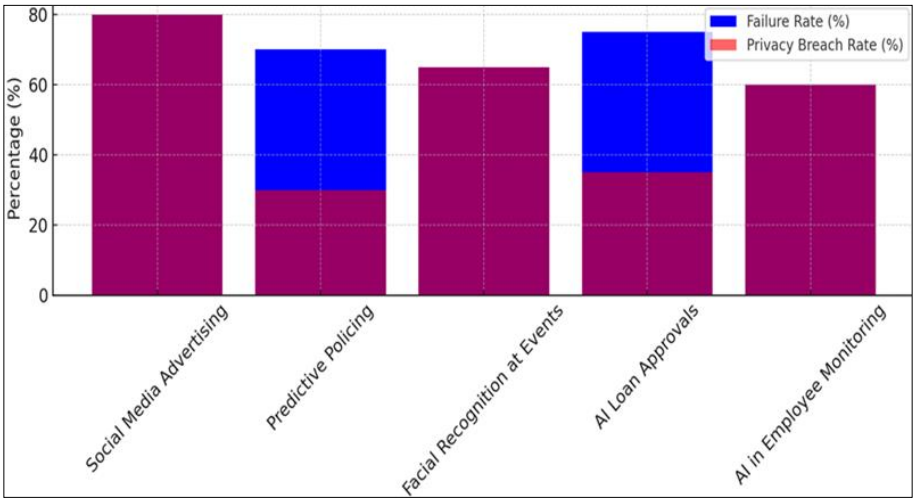

Fig 1: Failure Rate and Privacy Breach Rate

When AI is used to approve loans, it fails or is biased 75% of the time, which is a worrying statistic that shows there are problems with how financial institutions use AI as a whole. This means that stronger rules are needed to make sure that AI systems used in finance don't make things more unequal or create new biases, representation in figure 2.

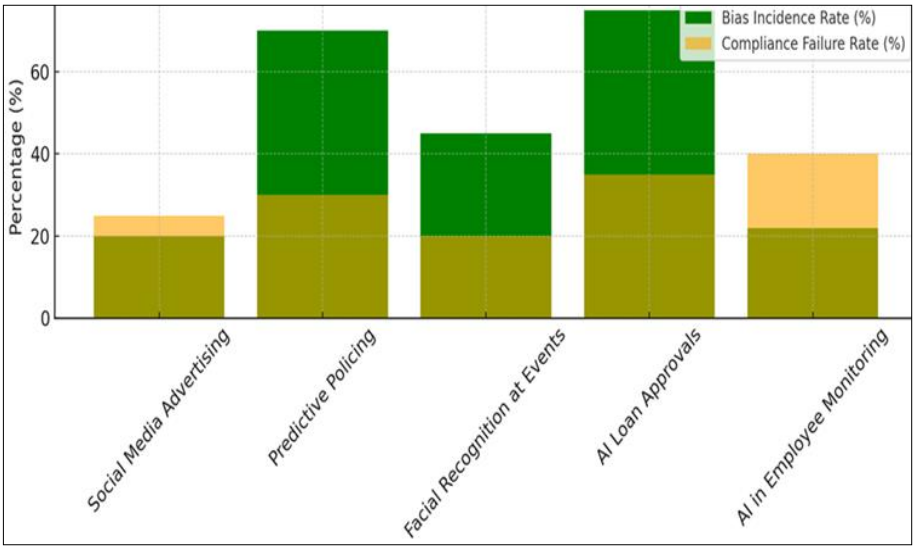

Fig 2: Representation of Incidence and Compliance Failure Rates

Ethical Concerns Addressed by Data Privacy Legislation

1. Bias and Discrimination in AI Algorithms

Some of the most important social problems that data privacy laws are meant to fix are bias and discrimination in AI systems. If AI systems are taught on biased data sets or if their design and operation don't take diversity into account enough, they may unintentionally keep or even make social problems worse. Data protection rules help solve these problems by implementing ideas like fairness, purpose limits, and data minimisation [3]. These rules make sure that only the data that is needed for a certain task is gathered. This lowers the chance that AI systems will be biased by data that isn't relevant to the task at hand. Also, rules like the GDPR say that processing data must be fair and not favour one group over another. Especially in areas like hiring, credit score, and law enforcement, where unfair AI

decisions can have very bad results for people, this is very important. One example is that an AI hire tool shouldn't use gender or race to make choices unless that information is officially required for the job. Even in these situations, the use of this information must be clearly explained and strictly controlled to stop unfair practices. Privacy rules make it easier to make AI systems that are fairer and just by encouraging fair data processing.

2. Accountability Measures for AI Developers and Operators

Accountability is a key part of responsible AI, and data privacy laws make sure that AI makers and users follow the law by putting many requirements on them. As a result of these steps, companies that plan, build, install, and run AI systems are held accountable for following privacy and data protection rules and will be held responsible for any violations or failure to do so [4]. The General Data Protection Regulation (GDPR) for example requires businesses to take the right technical and organisational steps to make sure and show that they handle data in a way that follows the rules. This includes keeping thorough records of all the activities that process data, doing effect studies for processing that is high-risk, and protecting data "by design and by default." Because of these rules, AI makers have to think about privacy at every stage of designing and running an AI system, building safety features into the system's structure. Additionally, these laws require people to be responsible by sharing any data breaches, even ones that happen because of problems with AI systems. This openness not only lets people who are affected know, but it also lets governing bodies know what they can do next. This keeps AI systems under constant review and improvement. Measures of accountability encourage a culture of responsibility among AI partners, which forces them to follow ethical standards and practices [5].

Conflicts Between Corporate Interests and Regulatory Compliance

Legislation that protects personal data and business interests often go against each other, which makes following the rules very hard. Businesses may see compliance as something that stops them from coming up with new ideas or making the most money. For instance, privacy rules like consent standards or data minimisation principles might be hard for AI-driven business models that depend on analysing large amounts of data and personalisation services. Because of these disagreements, businesses may try to find legal holes or less strict ways to follow the rules that only follow the letter of the law [6]. There is also a chance that big businesses will push for less strict rules, which would hurt efforts to protect data. Strong enforcement methods and punishments that discourage noncompliance are needed to make sure that companies not only follow the laws that are already in place but also help make AI systems that are fair and useful.

1. Technical Challenges in Compliance (e.g., Anonymization, Data Tracking)

There are big technical problems with following data privacy rules, especially when it comes to the needs for tracking and anonymising data. Anonymization is the process of removing personally identifiable information from data sets that are used in AI systems. This makes sure that the people whose data was taken can't be found. This process needs to be strong enough to stop re-identification, which can be hard to do technologically, especially with big, complicated data sets where many pieces of non-personal information can be put together to make a person's identity [7]. Legal requirements like the GDPR require organisations to keep track of the flow of data inside and outside the organisation. However, this is not always easy to do technically. It is hard and expensive to keep accurate records of all the activities that handle data, make sure that all data exchanges are safe, and set up systems that can effectively manage and protect data security while meeting audit standards [8]. To get around these technical problems, you need to put a lot of money into new protection and data handling tools. To make sure that technology measures are properly put in place and kept up to date, AI writers and workers must also receive ongoing training in the best ways to protect data and follow the law [9].

Discussion

1. Analysis of specific instances where data privacy laws have been successfully implemented to manage AI ethics

A number of important cases show that data privacy rules have been very helpful in keeping AI ethical in many different areas. One example is the healthcare enterprise, where following GDPR guidelines has greatly advanced the privacy and safety of patient information. One instance is a health facility in Europe that used AI to expect when a patient could worsen. The clinic made sure that each one AI strategies met GDPR's strict policies for defensive facts by means of design and through default [10]. These regulations consist of strong access controls and encrypting all records. This implementation not best stored private health records safe, however it additionally helped sufferers and healthcare people agree with AI technology. It shows how privacy rules can make it less difficult to use AI in touchy regions in an amazing way [11]. In an exclusive case, the financial industry became affected by the CCPA whilst an American bank used AI to score credit score. The bank instructed clients sincerely approximately the AI's role in making decisions and the kind of records it looked at below CCPA. Customers could recognize and agree to the processing in their data because it became clean, and they might pick out now not to participate in the event that they did not trust how the AI treated their records. This case showed how a success records privacy legal guideline are at shielding users' energy over private information and ensuring that AI utilized in monetary decisions is truthful.

Table 2: Illustrate successful applications of data privacy laws

Case Study	Industry	Law Applied	Outcome	Ethical Issue Addressed
AI in Healthcare Diagnostics	Healthcare	GDPR	Improved patient data protection and AI transparency	Privacy and Bias
AI Personalized Learning	Education	GDPR	Enhanced data security and user control over	Privacy and

			personal data	Transparency
AI in Job Recruitment	HR	CCPA	Reduction in discriminatory hiring practices	Bias and Discrimination
AI Credit Scoring	Finance	GDPR	Greater transparency in decision-making processes	Transparency and Fairness
AI for Retail Customer Insights	Retail	CCPA	Increased customer control over personal data usage	Privacy and Consent
AI in Public Surveillance	Public Sector	GDPR	Strengthened data anonymization practices	Privacy and Surveillance
AI in Insurance Premiums	Insurance	CCPA	More accurate and fair data processing	Bias and Fairness
AI-Powered Chatbots	Customer Service	GDPR	Improved consent mechanisms and data handling	Consent and Transparency
AI Traffic Management Systems	Transportation	GDPR	Enhanced data security and transparency in data usage	Privacy and Transparency
AI in Real Estate Analytics	Real Estate	CCPA	Greater user control and fairness in data usage	Privacy and Bias

2. Comparative analysis of different regulatory approaches and their outcomes

The strength of each law is judged by how well it is followed, how many violations are recorded, and an AI ethics score that shows how well these rules support moral AI behaviour, as shown in Table 3. The GDPR from the European Union stands out because it has the best compliance rate (85%) and the highest AI ethics score (9.2). This means that strong data security rules and a strong ethical framework for AI are in place [12].

Table 3: Regulatory Comparison

Region	Law	Compliance Rate (%)	Breaches Reported	AI Ethics Score
EU	GDPR	85	120	9.2
USA	CCPA	78	150	8.7
China	PIPL	65	90	7.8
India	PDPB	70	80	8.0
Brazil	LGPD	72	100	8.3

Privacy and data protection are held to a high standard by the GDPR's strict rules on permission, the right to access, and the right to be forgotten. But the relatively high number of breaches (120) reported under GDPR also shows how hard it is for entities to follow these strict rules.

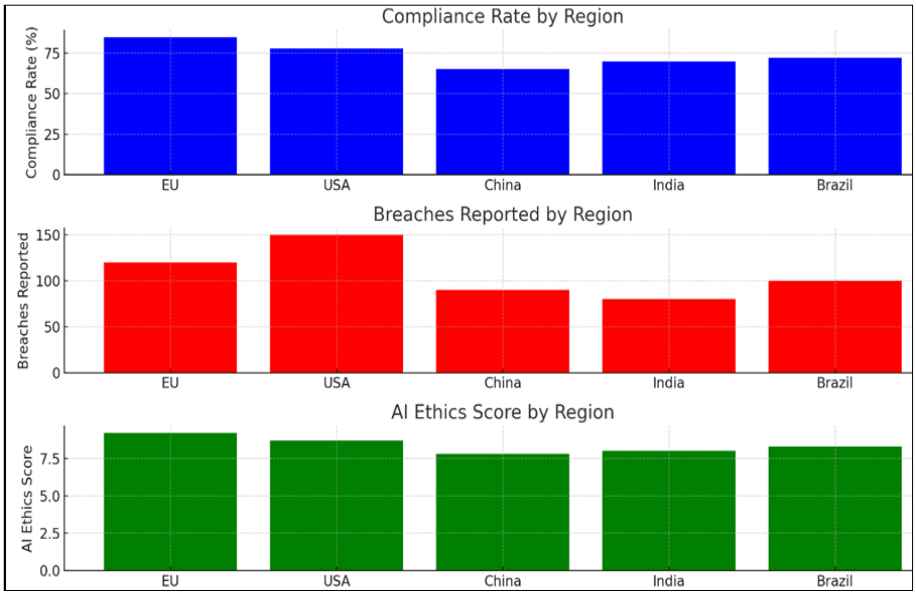

Fig 3: Representation of Compliance Rate by Region

This shows that organisations are still having trouble fully integrating and following GDPR rules. The CCPA has a 78% compliance rate in the US, with 150 recorded breaches. This shows that Californian companies are following the law's rules, but it also shows where changes need to be made. It's possible that the CCPA's lower AI ethics score compared to the GDPR is because it has a smaller focus and was just put into place recently, which means that its governing system needs more time to mature and improve. The low compliance rates of 65% for China's PIPL and 70% for India's PDPB show how new data protection rules are in these areas. Laws like these are important for making sure that countries with large populations and fast-growing digital economies have complete data privacy standards, even if they aren't always followed. The slightly lower AI ethics scores than those of the EU and the USA show that these systems are still in their early stages and could be improved in the future. With 100 recorded breaches and a compliance rate of 72%, Brazil's LGPD is off to a good start in an area that hasn't always had strict data privacy laws,

compilation comparison by region illustrate in figure 3. It got an 8.3 for AI ethics, which means that the system works, but there are still things that need to be done to make sure people follow it and enforce it [13].

3. The Role of International Cooperation in Standardizing AI Regulations

To make sure that data protection and ethics standards are followed around the world, it is very important for countries to work together to standardise AI laws. AI technologies work across countries, so local rules won't work as well without international standards to back them up. An international regulatory framework could make it easier for ethics rules and privacy rules to be followed consistently. This would cut down on differences that could lead to forum shopping or taking advantage of regulatory holes. International groups like the United Nations, the World Economic Forum, or already-formed international unions could lead these efforts by coming up with a set of core values and laws that all member countries can agree to follow. Not only would this make it easier for regulators to do their jobs, but it would also encourage a world mind-set of ethical AI creation. Better teamwork could also lead to international deals for sharing data that follow privacy rules. These agreements are needed to move AI research and development forward around the world while also protecting data strongly [14].

Conclusion

To keep a balance between encouraging new ideas and protecting people's rights across countries, there needs to be a worldwide system that works well together. This kind of teamwork would help lower the risks of legal arbitrage and make sure that the development of AI is led by a set of ethical standards that are agreed upon by everyone. How AI is governed in the future will depend on how well we can change and improve data privacy rules. To do this, we need to be proactive and make sure that ongoing changes to the law, foreign cooperation, and specific rules for AI all work together to build a strong environment that can keep social responsibility even as AI gets smarter. Making sure AI is used in a decent way is not just a problem for regulators; it's a world issue that needs everyone to work together and share responsibility.

References

1. Zhan WD, Jin B, Xu H, Dong C. Data security management based on transparent encryption policy. IEEE 2nd International Conference on Mobile Networks and Wireless Communications,2022:1(1):1–4.
2. Michel-Villarreal R, Vilalta-Perdomo E, Salinas-Navarro DE, Thierry-Aguilera R, Gerardou FS. Challenges and opportunities of generative AI for higher education as explained by ChatGPT. Education Sciences,2023:13:856.
3. Ong DS, Chan CS, Ng KW, Fan L, Yang Q. Protecting intellectual property of generative adversarial networks from ambiguity attacks. IEEE/CVF Conference on Computer Vision Pattern Recognition, 2021, 3630–3639.
4. Farina M, Yu X, Lavazza A. Ethical considerations and policy interventions concerning the impact of generative AI tools in the economy and in society. AI Ethics, 2024, 1–9.
5. Acion L, Rajngewerc M, Randall G, Etcheverry L. Generative AI poses ethical challenges for open science. Nat. Hum. Behav,2023:7:1800–1801.
6. Sharma Bhavana. Impact of artificial intelligence on the legal industry Advantages, challenges, ethical implications. BioGecko: A Journal for New Zealand Herpetology,2023:12(2):3363–3374.
7. Voss E, Cushing ST, Ockey GJ, Yan X. The use of assistive technologies including generative AI by test takers in language assessment: A debate of theory and practice. Language Assessment Quarterly,2023:20:520–532.
8. Zhong H, Chang J, Yang Z, Wu T, Mahawaga Arachchige PC, Pathmabandu C, *et al*. Copyright protection and accountability of generative AI: Attack, watermarking attribution. ACM Web Conference Companion Proceedings, 2023, 94–98.
9. Zhang P, Kamel Boulos MN, Generative in medicine and healthcare: Promises, opportunities challenges. Future Internet, 2023, 15, 286.
10. Schubert KD, Barrett D. Data governance, privacy, ethics. In Lacity MC, Coon L, *et al* eds Human Privacy in Virtual and Physical Worlds. Technology, Work and Globalization, 2024. https://doi.org/10.1007/978-3-031-51063-2_5
11. Prather J, Denny P, Leinonen J, Becker BA, Albluwi I, Craig M, *et al*. The robots are here: Navigating the generative AI revolution in computing education. Innovation and Technology in Computer Science Education Working Group Reports, 2023, 108–159.
12. Pathak A, Tyagi P, Sharma B, Natarajan R. Adoption of artificial intelligence technology for effective human resource management. Routledge, https://doi.org/10.4324/9781032708294
13. Saeidnia HR, Hashemi Fotami SG, Lund B, Ghiasi N. Ethical considerations in artificial intelligence interventions for mental health well-being Ensuring responsible implementation impact. Social Sciences, 2024, 13, 381. https://doi.org/10.3390/socsci13070381
14. Protection F. General data protection regulation GDPR. Intersoft Consulting,2018:24(1).
15. Auxier B, *et al*. Americans and privacy Concerned, confused and feeling lack of control over their personal information, 2019.