A CRITIQUE OF INDIAN APPROACH TO DATA PROTECTION AND AI IN THE GLOBAL DIGITAL ORDER

Rethiga Ramesh, Tamil Nadu Dr. Ambedkar Law University, SOEL, Chennai

ABSTRACT

The fast pace of digital technology, artificial intelligence, and cross-border data flows has reshaped the global digital economy, strengthening the demand for strong legal frameworks to protect privacy, enhance cyber security, and develop trust. However, the Act's adequacy and enforceability are challenged by the complex landscape of AI-related risks, cyber security threats, and the inherently transnational nature of data exchange. This paper places the DPDPA in the overall international regulatory context, drawing comparative lessons from the EU's General Data Protection Regulation (GDPR), the U.S. sectoral model, and nascent AI regulations. It analyzes how India's model aims to balance innovation with responsibility, and assesses its implications for cyber security resilience, AI regulation, and India's ambitions to become a trusted digital economy hub. This analysis identifies opportunities as well as loopholes in India's regulatory strategy, eventually positing that the success of the DPDPA will decide not only national privacy protection but also India's strategic place in setting norms for the international digital economy. The paper argues that for India to safeguard individual rights and assume a substantive leadership role in global digital governance, its liability regime must transcend procedural compliance to encompass algorithmic transparency, robust deterrence measures, and proactive participation in international treaty frameworks.

Keywords: Data privacy, cross border data, cyber security and AI regulation.

1. INTRODUCTION

Artificial intelligence is transforming the digital data ecosystem by enabling predictive analytics, large-scale profiling, and automated decision-making[1]. These systems thrive on the continuous collection, transmission, and processing of data, much of which crosses national boundaries. However, the globalization of data introduces new risks: data breaches, identity theft, algorithmic profiling, and surveillance that are no longer confined to territorial jurisdictions. Several high-profile breaches highlight this problem. The 2017 Equifax breach compromised the data of 147 million individuals across jurisdictions, triggering multi-billion-dollar settlements in the U.S. Similarly, European regulators have repeatedly fined Meta Platforms Inc. for privacy violations relating to inadequately protected global transfers. These episodes underscore that accountability in the digital economy cannot be resolved merely by national law it requires global harmonization.

Rise in cybercrime – As per NCRB, in May 2024, the Indian Cyber Crime Coordination Centre (I4C) recorded an average of 7,000 cybercrime complaints per day. This is a 60.9% increase from 2022 to 2023 and a 113.7% increase from 2021 to 2023.

India's Digital Personal Data Protection Act, 2023 (DPDPA) marks a watershed moment[2]. For the first time, India has enacted a comprehensive statute regulating personal data governance. Yet, critical questions persist:

1.2 RESEARCH QUESTION:

1. Are the current liability framework under the Indian law adequate to address AI-driven data breaches?

2. Is the liability framework under Indian and comparative international law adequate to address AI-driven breaches affecting global users?

This paper adopts a doctrinal methodology, analyzing statutes, case law, and comparative scholarship across India, the EU, and the U.S. It offers both descriptive analysis of frameworks

[1] Scassa, T. (2021, February 1). *AI and Data Protection Law*. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732969

[2] Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2019*, 494. https://heinonline.org/HOL/LandingPage?handle=hein.journals/colb2019&div=15&id=&page=

and normative recommendations for enhancing India's global role.

1.3 SCOPE OF THE STUDY

The scope of this study lies in a **comparative legal evaluation** of India's *Digital Personal Data Protection Act, 2023 (DPDPA)* within the **broader global digital governance landscape**, focusing on how India's approach interacts with **AI regulation**, **cross-border data flows**, and **cybersecurity**. It examines the extent to which Indian data protection frameworks align with or diverge from international benchmarks such as the **EU GDPR**, the **U.S. sectoral data protection model**, and emerging global AI governance standards. The study encompasses both **doctrinal legal analysis** and **policy implications**, covering issues like liability for AI-driven data breaches, accountability mechanisms, and transnational data oversight.

1.4 OBJECTIVES OF THE STUDY

- To **critically assess** the adequacy of India's current data protection regime, particularly the DPDPA, in confronting **AI-related risks**, **automated decision-making**, and **algorithmic accountability**.
- To **compare** India's legal framework with the **EU GDPR**, **U.S. frameworks**, and **nascent AI laws** (such as the EU AI Act), identifying lessons for India's evolving regulatory model.
- To **analyze** whether India's liability framework provides **effective remedies and enforcement mechanisms** for data breaches arising from AI technologies.
- To **evaluate** India's preparedness to participate in **international data governance and treaty frameworks**, enhancing its credibility as a **trusted digital economy**.
- To **recommend** policy and legal reforms for strengthening India's **liability regime**, **algorithmic transparency**, and **international cooperation** in AI and data protection governance.

1.5 RESEARCH QUESTIONS

1. **Are the current liability frameworks under Indian law adequate to address AI-driven data breaches?**

This question tests the DPDPA's enforcement strength, deterrence capacity, and procedural safeguards in the context of AI-induced privacy violations.

2. **Is the liability framework under Indian and comparative international law adequate to address AI-driven breaches affecting global users?** *This question explores the degree of harmonization between India's approach and international frameworks like the GDPR, assessing gaps in cross-border enforcement, jurisdiction, and international accountability.*

1.6 RESEARCH METHODOLOGY

The methodology employed in this study is primarily doctrinal in nature. In critically evaluating the issue, the researcher relies on previously accessible facts and information, subjecting them to analysis. Numerous studies used in the research are based on secondary data. The secondary data has been collected after doing a comprehensive study which is derived from the writings of eminent scholars in books, articles, research papers, statutes, judgments of the courts, and various other data available on the internet.

1.7 REVIEW OF LITERATURE

1. Thakur, V., & Agrawal, R, Efficacy, Inhibition, Facilitation: Comparative Perspectives on Digital Personal Data Protection Act, 2023 (2025)

The paper is surrounding India's Digital Personal Data Protection Act, 2023 (DPDPA) views it as a long-awaited reform aligning India's privacy framework with global norms while fostering a digital economy. Studies emphasize its balance between individual rights, such as consent and data erasure and innovation needs. The framework introduces obligations for data fiduciaries, data principal rights, and a regulatory board, though scholars highlight concerns regarding government exemptions and enforcement. Compared with your topic, which critiques India's AI governance and data protection in the global digital order, this abstract is narrower and institutional, centering on the DPDPA's legislative and operational features. Your topic, in contrast, assesses India's preparedness for AI-driven data dynamics and international adequacy alignment.

2. Musch, S., Borrelli, M. C., Balancing AI innovation with data protection: A closer look at the EU AI Act (2023).

The literature on the EU AI Act views it as a pioneering regulatory framework addressing AI risks through a risk-based approach, including extraterritorial applicability, AI system classification, and transparency obligations. The Act supplements the GDPR by reinforcing data protection safeguards specifically for AI, such as limiting sensitive data use, mandating human oversight of high-risk AI, and requiring consent and breach notification mechanisms. Compared to your topic, which critiques India's data protection and AI framework in the global digital order, the EU AI Act represents a mature, integrated legislative model combining AI innovation and privacy protections. India, while advancing through the DPDPA, has yet to establish similarly comprehensive AI-specific rules, underscoring a regulatory maturity gap in protecting fundamental rights alongside fostering innovation.

3. Scassa, T, *AI and Data Protection Law* (2021)

This paper highlights Canada's urgent need to reform its outdated data protection regime to reconcile AI-driven innovation with privacy and ethical imperatives. Literature in this space often emphasizes the interplay between AI's data dependency and evolving privacy norms, referencing the GDPR as a benchmark for accountability and adequacy in cross-border data governance. The current topic focuses on India's fragmented and evolving data protection landscape under the DPDPA, its limited AI oversight mechanisms, and global alignment challenges. While Canada's debate centers on modernization and GDPR adequacy, India's critique stresses enforcement depth, institutional readiness, and international interoperability gaps.

4. Sartor, G., & Lagioia, F, The impact of the general data protection regulation on artificial intelligence (2020)

The study by Sartor and Lagioia (2020) provides an in-depth analysis of the interplay between the EU General Data Protection Regulation (GDPR) and artificial intelligence (AI). It explains how AI applications, particularly those processing personal data, pose challenges to existing data protection principles such as purpose limitation, data minimisation, and automated decision-making safeguards. The authors highlight tensions between AI's capabilities and GDPR mandates, emphasizing the need for risk-based approaches and data protection by design. While noting GDPR's limitations in providing precise guidance for AI controllers, the study finds it broadly compatible with AI deployment and proposes policy options to bridge gaps, including clearer guidelines and enhanced rights like opt-out from profiling. This

comprehensive evaluation supports understanding GDPR's influence on ensuring ethical AI innovation within legal boundaries.

Compared to the current topic, which critiques the Indian approach to data protection and AI in the global digital order, this study offers a detailed EU-centric perspective. Your work focuses on India's newer legal frameworks and their global adequacy and AI governance challenges, while Sartor and Lagioia analyze a mature, established regime grappling with AI integration complexities, exposing gaps and suggesting forward-looking policies. The difference lies in regulatory maturity: the EU framework is more developed and specific to AI, whereas India's approach is emerging, with ongoing debates on balancing innovation and privacy within global digital norms.

5. Wachter, S., & Mittelstadt, B, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (2019)

The inferential analytics in data protection highlights significant gaps in existing laws, particularly under the GDPR, where inferred data receives weaker protection than raw personal data. Scholars argue that inferences in AI-driven Big Data analytics pose risks such as bias, discrimination, and lack of transparency, calling for novel rights like a "right to reasonable inferences" to ensure accountability and fairness. Compared to your topic, which critiques India’s data protection framework and AI governance globally, this abstract concentrates on the limitations of inference protection within an advanced regulatory regime (GDPR). India’s DPDPA, while addressing personal data protection broadly, lacks specialized provisions for inferential analytics and AI-specific challenges, underscoring a key difference in regulatory maturity and focus.

6. Mitrou, L, Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) “Artificial Intelligence-Proof”? (2018)

The literature on GDPR related to AI reveals that while the GDPR is not AI-specific, it plays a pivotal regulatory role in governing AI-driven data processing through technology-neutral principles such as data minimization, purpose limitation, transparency, fairness, and accountability. Key GDPR provisions impacting AI include requirements for explicit consent, protection of sensitive data, data protection impact assessments (DPIAs), and rights to explanation and data portability. The GDPR demands organizations demonstrate accountability

via transparent processing, security measures, and ongoing monitoring, which supports responsible AI deployment. However, challenges remain due to GDPR's generalist nature, requiring adaptation through complementary legislation like the EU AI Act to address AI-specific risks like bias and high-risk classifications.

Compared to your critique of India's evolving data protection and AI framework, GDPR's mature legal infrastructure offers stronger safeguards and clearer compliance mandates, while India's framework is still developing AI-specific regulations, balancing innovation and data protection with global alignment challenges. This highlights the contrast in regulatory sophistication and implementation scope between the EU and India.

7. Kingston, J, Using artificial intelligence to support compliance with the general data protection regulation. (2017).

The article examines how artificial intelligence (AI) technologies can support compliance with the European Union's General Data Protection Regulation (GDPR) in four key areas: adherence to compliance checklists and codes of conduct, risk assessment support, compliance with automatic profiling regulations, and recognition/reporting of security breaches. It concludes that AI can indeed assist effectively, particularly through rule-based systems which align with GDPR's need for explanation and justification of decision-making processes. While machine learning could offer advantages in certain business contexts, the transparency requirements of GDPR favor rule-based approaches. This highlights the nuanced role AI can play in GDPR compliance, balancing regulatory demands for clarity with operational needs for automation and efficiency.

2. INDIA'S LIABILITY FRAMEWORK FOR DATA BREACHES

(A) Overview of DPDPA

Ministry of Electronics and Information Technology (MeitY) released draft Digital Personal Data Protection Rules, 2025 to facilitate implementation of Digital Personal Data Protection Act, 2023 (DPDP Act). The DPDPA extends its application to domestic and foreign entities that process the personal data of Indian residents.

Key provisions include obligations for data fiduciaries, expanded duties for significant data fiduciaries (SDFs), individual rights for data principals, and the establishment of the Data

Protection Board of India, which deals successfully with enforcement and penalty powers up to ₹250 crores (DPDPA, 2023). Its extraterritorial scope extends to address transnational breaches, but concrete mechanisms for holding global actors accountable are still nascent.

The Indian approach reflects an effort to harmonize privacy with development in the global digital order, inspired partly by the EU's GDPR but more limited in scope, covering only digital personal data and not distinguishing sensitive data categories. DPDP grants rights for access, correction, erasure, and grievance redressal while imposing strict fiduciary duties on entities processing data, including security safeguards, accuracy obligations, and breach notification requirements.

The Act's establishment of a Data Protection Board promises better enforcement but its efficacy remains to be tested amid India's complex digital ecosystem. Moreover, ongoing delays in fully operationalizing rules and enforcement create implementation uncertainties. From the perspective of AI and emerging technologies, the Act lacks explicit provisions addressing automated decision-making and algorithmic transparency, posing challenges in the burgeoning AI domain within India's global digital integration.

Data Localisation: Certain types of sensitive personal data are required to be stored and processed within India. This provision aims to enhance data security and facilitate easier enforcement of data protection laws.

The Act also, grants **government agencies** broad exemptions for processing personal data without adhering to most compliance obligations when acting in the interest of national security, public order, or sovereignty. This raises significant privacy concerns, as it could lead to excessive surveillance and misuse of data. Such wide latitude allows the state to process and retain vast amounts of data for security purposes beyond the usual privacy safeguards. Additionally, the Act's protection scope is limited to digital personal data, excluding categories like offline data or sensitive data distinctions seen in the EU's GDPR. This narrower scope potentially leaves gaps in privacy protection compared to more comprehensive frameworks. Together, these features illustrate a balancing act between security priorities and data privacy that may impact public trust and rights protections in India.

ONLINE PRIVACY:

There is no regulation of cookies, behavioural advertising, or location data. However, this may

include personal data and it is advisable to obtain user consent, such as by using appropriate disclaimers.

The IT Act contains both civil and a criminal penalties and offences for a variety of computer crimes. Under the IT Act, if any person introduces or causes to be introduced, any computer contaminant (like viruses etc.), into any computer, computer system or computer network, they may be liable to pay damages to the affected person (s). Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed:

1. to modify, destroy, record, or transmit data or programs residing within a computer, computer system or computer network, or

2. by any means to usurp the normal operation of the computer, computer system or computer network.

Further, under the IT Act, any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, may be subject to a prison term of up to three years and a fine up to INR 100,000 or approximately €1,098 (as at January 6, 2025).

(B) Cross-Border Liability and Enforcement

The Digital Personal Data Protection Act (DPDPA) empowers the Indian government to regulate and restrict data transfers; however, it does not require an adequacy assessment process similar to the GDPR[3]. While its extraterritorial application is strongly mentioned in theory, in practice, enforcement against foreign entities or cloud-based service providers largely depends on voluntary compliance, cooperative international treaties, or enforcement actions by foreign jurisdictions which India currently lacks in comprehensive form. This enforcement gap significantly weakens the deterrent effect of imposed penalties and limits the reach of sanctions. Consequently, consumers remain vulnerable when AI-driven data breaches originate or spread beyond Indian borders, highlighting the need for stronger international cooperation and clearer mechanisms to hold cross-border data processors accountable under

[3] Musch, S., Borrelli, M. C., & Kerrigan, C. (2023). Balancing AI innovation with data protection: A closer look at the EU AI Act. *Journal of Data Protection & Privacy*, *6*(2), 135–152. https://www.ingentaconnect.com/content/hsp/jdpp/2023/00000006/00000002/art00004

the DPDPA.

(C) AI-Specific Gaps

Critically, the DPDPA does not directly address harms arising specifically from AI, such as algorithmic bias, opaque decision-making, or automation risks[4]. In comparison, the EU has enacted the 2024 AI Act, which ties risk-based obligations and fines to specific AI activities, ensuring algorithmic transparency and accountability (AI Act, EU, 2024)[5]. India's lack of similar provisions means systemic risks posed by automated tools, such as AI-powered profiling or discriminations are neither explicitly prevented nor easily remedied under current law.

3. COMPARATIVE ANALYSIS: GLOBAL REGIMES

(A) European Union: GDPR and AI Act

The EU's GDPR represents the benchmark for extraterritorial enforcement. It has stringent penalty regime (up to 4% of global turnover) and the AI Act's algorithmic obligations illustrate a sophisticated, risk-based approach to AI-driven harms ie) EU's GDPR[6], 2016 and AI Act, 2024[7].

Notable enforcement actions such as Amazon's €746 million fine and Meta's €1.2 billion penalty display the EU's capacity to deter and remediate transnational breaches.

Amazon was fined €746 million for violating the EU's General Data Protection Regulation (GDPR) related to its targeted advertising practices. The fine stemmed from a 2018 complaint alleging that Amazon processed customer data without proper user consent to personalize ads, violating transparency and consent requirements. The Luxembourg data protection authority

[4] Bag, S. (2024, December 23). *Digital Personal Data Protection Act: Shaping India's AI-driven fintech sector*. Orfonline.org; OBSERVER RESEARCH FOUNDATION (ORF). https://www.orfonline.org/expert-speak/digital-personal-data-protection-act-shaping-india-s-ai-driven-fintech-sector

[5] Mitrou, L. (2018, December 31). *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?* Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914

[6] Sartor, G., & Lagioia, F. (2020b). The impact of the general data protection regulation on artificial intelligence. In *European Parliament eBooks* (pp. 1–84). European Parliament. https://doi.org/10.2861/293

[7] DLA Piper. (2024). *Data Protection Laws in India - Data Protection Laws of the World*. Dlapiperdataprotection.com. https://www.dlapiperdataprotection.com/?t=law&c=IN

upheld the fine after Amazon contested it.

Meta was fined €1.2 billion primarily for unlawfully transferring the personal data of European users to the United States without adequate data protection safeguards, exposing users to surveillance risks. This systematic, ongoing violation prompted the Irish Data Protection Commission to impose the record penalty to enforce compliance and protect user privacy.

Furthermore, the EU's harmonized legal framework allows data subjects to seek remedies even when violations involve companies operating outside their local jurisdiction[8]. This mechanism ensures that individuals' privacy rights are protected regardless of where the offending organization is based, strengthening consumer protection against transnational data misuse.

(B) United States: Sectoral and Civil Liability

The United States employs a sectoral model for data protection, with laws like HIPAA Act, 1996 protecting healthcare information and the CCPA Act, 2018 covering consumer data. A key enforcement example is the 2017 Equifax data breach, where hackers accessed the personal data of approximately 147 million people. Following investigations, Equifax agreed to pay up to $700 million in settlements. This included a $425 million consumer restitution fund for credit monitoring and reimbursements, $175 million to states, and $100 million in civil penalties. The case highlighted Equifax's failure to patch critical security vulnerabilities, exposing consumers to identity theft risks. This enforcement demonstrated the role of civil liability and regulatory pressure in the U.S., compensating affected individuals and incentivizing stronger corporate data security practices despite the absence of a unified privacy law (Equifax Litigation, 2019).

(C) Singapore and UK: Hybrid Innovation Models

Singapore's PDPA and the UK's post-Brexit model balance innovation and accountability by encouraging industry compliance while maintaining strong enforcement mechanisms[9]. Both regimes show incremental reform responsive to the global flow of data and emerging risks but

[8] Sharma, A. K., & Sharma, R. (2024). Comparative Analysis of Data Protection Laws and AI Privacy Risks in BRICS Nations: A Comprehensive Examination. Global Journal of Comparative Law, 13(1), 56–85. https://doi.org/10.1163/2211906X-13010003

[9] Sundara, K., & Nikhil Narendran. (2023). *The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection*. *24*(5), 129–141. https://doi.org/10.9785/cri-2023-240502

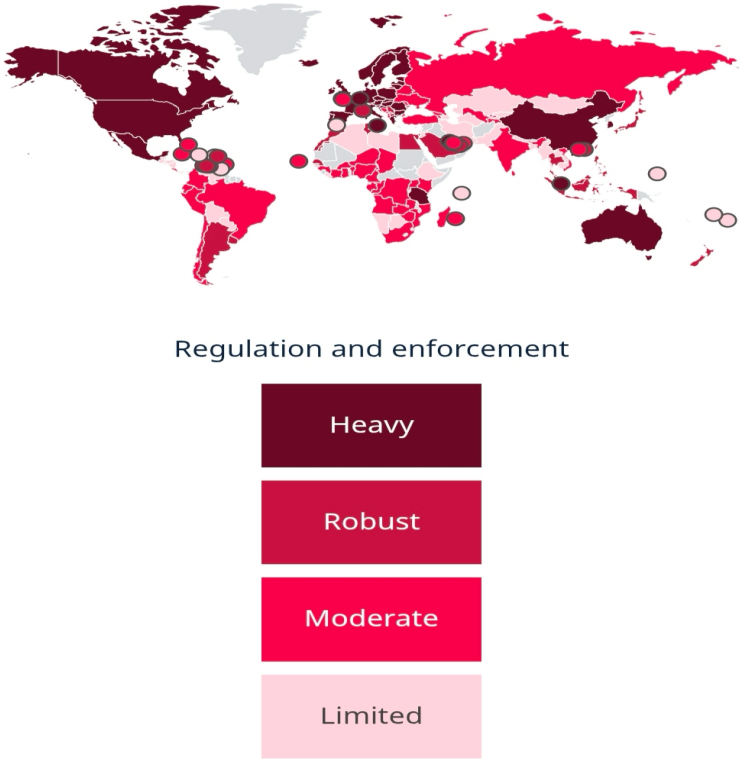
stop short of the comprehensive reach of the EU's GDPR-GAI ensemble (PDPA, Singapore; UK GDPR).

4. ENFORCEMENT AND JURISDICTION CHALLENGES

A central barrier to effective liability in AI-driven breaches is the multiplicity of legal regimes and enforcement asymmetry. The EU, via adequacy frameworks and mutual assistance treaties, actively polices global corporations. India, by contrast, struggles with jurisdiction over foreign entities and lacks access to quick mutual legal assistance mechanisms which are critical when breaches impact global users eg.Schrems II, 2020. Without international agreements, penalties under DPDPA risk becoming symbolic, limiting their deterrent effect[10].

The Schrems II case (2020) was a landmark ruling by the Court of Justice of the European Union (CJEU) that invalidated the EU-US Privacy Shield framework, a key mechanism allowing personal data transfers from the EU to the US. The court found that US surveillance laws were too broad and lacked sufficient safeguards to meet EU data protection standards, putting EU citizens' data at risk. While upholding the use of Standard Contractual Clauses (SCCs) for data transfers, the court required stricter assessments to ensure that data protections are equivalent to EU standards. The ruling emphasized that if an adequate level of protection cannot be guaranteed, data transfers must be suspended. Schrems II has significantly impacted global data transfer practices and reinforced the need for strong international data protection agreements to safeguard privacy rights beyond borders. It highlights challenges countries like India face in enforcing data protection extraterritorially without similar treaty mechanisms.

[10] Kingston, J. (2017). Using artificial intelligence to support compliance with the general data protection regulation. *Artificial Intelligence and Law*, *25*(4), 429–443. https://doi.org/10.1007/s10506-017-9206-9



5. ADEQUACY OF INDIA'S LIABILITY FRAMEWORK

Strengths:-

- **Extraterrestrial reach** under DPDPA aligns with global standards and signals intent to regulate global actors.
- **Structured penalty regime** provides strong theoretical deterrence for negligent or malicious conduct.

Weaknesses:-

- **Lack of algorithmic accountability**: No explicit rules for AI bias, profiling, or explainability risks central to global AI-driven breaches.
- **Enforcement capacity**: Collection of fines and remedial action against foreign firms remains problematic.
- **Harmonization gaps**: Absence of adequacy frameworks and lack of harmonized procedures for cross-border enforcement leave India isolated.

- **Judicial underdevelopment**: Few precedents exist under DPDPA; actual case law is evolving but not mature enough to offer predictability or systemic remedies.

6. RECOMMENDATIONS

(A) AI-Specific Liability Reform

India should amend or supplement the DPDPA to mandate:

- Transparency and explainability standards for AI systems.
- Algorithmic impact assessments to preempt harms from automated decision making.
- Specific liability provisions for discriminatory or high-risk AI conduct, modeled after the EU AI Act[11].

This is necessary to address unique AI risks, ensure accountability in automated decision-making, and align with global best practices like the EU AI Act to protect individual rights and foster trustworthy AI innovation[12].

(B) Cross-Border Harmonization

India must actively pursue adequacy negotiations and treaty arrangements with the EU, U.S., and other data-receiving jurisdictions to facilitate enforcement and predictable redress, overcoming the current limitations of voluntary compliance and jurisdictional uncertainty.

(C) Deterrence and Leadership

- Strengthen penalties to include criminal sanctions for willful misconduct.
- Impose executive accountability for systemic failures.
- Join or lead coalitions such as the G20 or OECD to develop global norms for AI and privacy

[11] Peck Pinheiro, P., & Batista Battaglini, H. (2022). Artificial Intelligence and Data Protection: A Comparative Analysis of AI Regulation through the Lens of Data Protection in the EU and Brazil. *GRUR International*. https://doi.org/10.1093/grurint/ikac049

[12] [12] Meurisch, C., & Mühlhäuser, M. (2021). Data Protection in AI Services. ACM Computing Surveys, 54(2), 1–38. https://doi.org/10.1145/3440754

rather than simply adopting foreign frameworks.

The liability framework under Indian and comparative international law is only partially adequate to address AI-driven breaches affecting global users.

- **India (DPDPA, 2023):** Strong extraterritorial scope and penalty regime, but enforcement against foreign actors is weak; no AI-specific accountability for bias, profiling, or opaque decision-making.
- **EU (GDPR & AI Act):** Most comprehensive framework with harmonized enforcement, adequacy mechanisms, risk-based AI obligations, and stringent global fines that deter cross-border misconduct.
- **US (Sectoral model):** Relies on civil liability and sector-specific statutes; enforcement (e.g., Equifax) provides compensation but lacks unified federal AI/data protection law.
- **Other regimes (UK/Singapore):** Balance innovation with accountability but stop short of EU-style harmonization.
- **Key Gaps:** India lacks adequacy agreements, treaty-based enforcement, and AI-specific liability, limiting protection for global users.

Thus, India's liability framework is underdeveloped compared to EU standards and requires AI-focused reforms, cross-border harmonization, and stronger enforcement mechanisms to be globally effective.

6. CONCLUSION

India's DPDPA, 2023, represents an important leap forward, but it remains insufficient for the complex reality of AI-driven, global data breaches[13]. Gaps in AI-specific regulation, cross border enforcement, and harmonization limit the liability regime's adequacy for protecting global users. Immediate reforms mandating algorithmic transparency, pursuing adequacy agreements, and bolstering deterrence are vital. With proactive domestic reform and

[13] Singh, R., & Singh, V. (2025). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. *Journal of Indian Academy of Forensic Medicine*. https://doi.org/10.1177/09710973251328785

international engagement, India can evolve from a passive rule-taker to an influential rule-shaper in global AI and data protection governance.

While the government is taking various initiatives in respect of AI, the concerns regarding the applicability of existing regulatory frameworks in India, or the adoption of a new law to govern the adoption and use of AI by proactively addressing these concerns, we can ensure that India's legal and regulatory landscape keeps pace with the rapid evolution of this transformative technology.