LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:420-440, July 2025

BALANCING DATA PRIVACY AND INNOVATION: LEGAL CHALLENGES IN REGULATING ARTIFICIAL INTELLIGENCE UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

By- Harsh Singh[1]

ABSTRACT

India stands at a crucial moment. On one hand, it has made a powerful commitment to protecting personal privacy through the Digital Personal Data Protection Act (DPDP), 2023, which builds upon the Supreme Court's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India declaring privacy a fundamental right. On the other hand, the country is racing ahead as a digital and AI powerhouse, with smart technologies being used in everything from healthcare and banking to education and governance. This rapid growth brings new opportunities but also serious questions. The DPDP Act tries to safeguard our personal data in this fast-changing digital world. It introduces clear rules around consent, gives individuals greater control over their data, and sets responsibilities for companies handling large volumes of personal information. But as promising as this sounds, the law also creates real challenges, especially for India's growing artificial intelligence (AI) sector. AI needs large amounts of data to work well and improve over time, yet the DPDP's strict consent rules, data retention limits, and localization mandates can slow down innovation, especially for small startups working with limited resources. This paper explores one key question: Can India protect personal privacy while still allowing AI to grow and thrive? It looks closely at the DPDP Act and how it affects real-world AI applications in areas like micro-lending, voice-based tutoring, and medical diagnosis. It also highlights how the Act's exemptions for government use of data without strong oversight, raise serious concerns about surveillance and

[1]**Intern, Lex Lumen Research Journal.**

misuse, particularly for already vulnerable communities. By comparing India's approach with global examples like the EU's GDPR and AI Act, this research identifies what's working and where changes are needed. It suggests practical steps forward: smarter consent mechanisms, more flexible rules for low-risk technologies, independent checks on government surveillance, and special support for small innovators. At its core, this paper argues that privacy and innovation don't have to be at odds. With the right safeguards and a thoughtful, people-first approach, India can build a digital future that respects both our rights and our potential. The DPDP Act is a big step but to truly succeed, it must evolve to meet the realities of how technology shapes our lives today.

KEYWORDS: DPDP Act, European Union's General Data Protection Regulation, small and medium enterprises, **Risk-Based Regulation for AI Systems Risk-Based Regulation for AI Systems**

INTRODUCTION: NAVIGATING THE CROSSROADS OF PRIVACY AND INNOVATION

In 2017, the Supreme Court of India made a significant ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India. The court clearly stated that the right to privacy is a fundamental right under Article 21 of the Constitution. This important decision set the stage for a dedicated data protection system in India. It stressed the immediate need for laws that protect individual rights in an increasingly digital world. Following this ruling, and after years of public discussions, reports from expert committees, and debates in Parliament, the Government of India passed the Digital Personal Data Protection Act (DPDP Act) in August 2023. This law comes at a crucial time for India. With over 800 million active internet users, the country is one of the largest digital markets globally. As digital usage has grown dramatically, India's artificial intelligence (AI) field has also expanded rapidly. From facial recognition at airports to AI-based financial assessments and chatbots for

public services, India is quickly adopting smart technologies. Analysts predict that India's AI sector will draw over USD 7 billion in investments by 2025, strengthening its aim to become a global tech hub. However, the combination of privacy laws and AI growth brings complicated issues. The DPDP Act takes cues from the European Union's General Data Protection Regulation (GDPR) by stressing informed consent, user rights, and responsibilities.[2]Yet, it also faces India's unique social and economic challenges. Unlike many Western countries, India has hundreds of millions of first-time digital users, many of whom have limited digital skills and depend on affordable, AI-driven services in essential fields like health, education, and finance. The main question is whether India's privacy-focused legal framework is flexible enough to support the country's AI development goals. Can the DPDP Act handle the data-heavy, evolving nature of AI models, or do its strict consent and data localization rules create hurdles for developers and startups? How does it maintain a balance between individual rights and the need for innovation, especially when AI is used in areas such as national security or predictive governance?

This paper will explore these challenges in detail. It will review the key elements of the DPDP Act, including its consent rules, data responsibilities, restrictions on data transfer, and government exemptions, while considering their impact on AI development in India. The paper will also compare India's approach with global examples, such as the EU AI Act and similar frameworks in the United States and Singapore, to identify gaps in regulation and potential areas for change. At this key moment, India needs to develop a balanced and forward-looking data governance model that protects individual privacy while allowing for responsible AI innovation that benefits its large and diverse population.[3]

LEGISLATIVE OVERVIEW

[2] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
[3] European Union, Artificial Intelligence Act, COM/2021/206 final (as amended and adopted in 2024

The Digital Personal Data Protection (DPDP) Act, 2023 is India's first complete framework for managing personal data. It focuses solely on digital personal data, which makes its scope narrower than the EU's GDPR that also includes offline data. However, its wide definitions of terms like automated processing and data fiduciaries explicitly cover AI systems, making it significant for the tech industry. Importantly, the Act introduces the idea of an artificial juristic person, which could allow AI entities to be recognized as data fiduciaries under certain conditions. The Act is based on key privacy principles. It requires clear opt-in consent for all data processing, excluding implied or legitimate interest-based processing. Individuals, referred to as data principals, have rights to access, correction, erasure, data portability, and withdrawal of consent. Entities managing large amounts or sensitive types of data are classified as Significant Data Fiduciaries. They must appoint Data Protection Officers and carry out regular audits.[4]The Data Protection Board of India oversees enforcement. This independent authority has the power to investigate violations, impose fines up to ₹250 crore, and require corrective actions. Proposed rules for 2025 suggest a three-year limit on data retention and compliance requirements that vary based on the size and risk profile of the data processor.

RESEARCH QUESTION

Primary Research Question:

Does the Digital Personal Data Protection Act, 2023, strike an effective balance between protecting individual privacy and enabling artificial intelligence innovation in India?

Sub-questions

- What are the key regulatory provisions of the DPDP Act that directly affect AI development?

[4] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), s. 2(i).

- How do consent and data localization requirements impact startups, developers, and users of AI-based technologies?
- How does India's regulatory approach compare with international data governance models (e.g., GDPR, EU AI Act, U.S. sectoral laws)?
- Can a risk-based or tiered framework offer a more flexible legal approach for AI innovation in India?

RESEARCHSTUDY

Doctrinal and Analytical Legal Research (Qualitative)

- Doctrinal: Reviewing statutory provisions of the DPDP Act and case law (e.g., *Puttaswamy* judgment).
- Analytical: Evaluating the practical impact of the Act on AI innovation through illustrative case studies in fintech, health-tech, and education sectors.
- Comparative: Analysing international frameworks (e.g., GDPR, EU AI Act) to understand best practices and identify gaps.

HYPOTHESIS

Primary Hypothesis (H1): The current framework of the Digital Personal Data Protection Act, 2023, imposes rigid compliance requirements that may unintentionally hinder the growth and innovation of artificial intelligence technologies in India, particularly in critical sectors like healthcare, finance, and education.

TENSIONS BETWEEN PRIVACY & AI NEEDS

The Digital Personal Data Protection (DPDP) Act, 2023, marks an important step in affirming user rights. However, it brings several challenges in the context of rapidly changing artificial intelligence. AI relies heavily on large, diverse datasets and complex algorithms, which often clash with the Act's focus on privacy.

Explainability and Transparency Gaps: A key challenge is the Act's focus on transparency. It requires that users are clearly informed about how their data will be used. However, many AI models, especially deep learning systems, act as black boxes. Their internal decision-making processes are hard to interpret even for developers. For instance, a rural farmer using an AI-powered microfinance chatbot may get tailored loan terms but may not understand why her application was accepted or rejected. The logic of the algorithm might be hidden in layers of training data, making it hard to explain despite legal requirements.

Consent as a Roadblock: The Act also requires purpose-specific consent, meaning data can only be used for clearly defined goals. This presents a challenge for AI development, where models often change and adapt. Developers usually need to test new features, tweak algorithms, or repurpose datasets. Under the DPDP, every change would require new user consent, which slows down innovation. Indian AI developers have expressed frustration, saying that "you would have to re-consent every time the model tries a new feature," which is impractical for dynamic systems.

Data Minimization vs. AI's Dataset Needs: The principle of data minimization and the suggested three-year data retention limit further conflict with AI's need for data. High-performance models, particularly in language processing and computer vision, often need millions of historical data points. If data gets deleted after three years, developers risk losing the depth needed for training and maintaining model accuracy, especially for applications that rely on long-term trends.

[5]**Individual Rights vs. Technical Feasibility:** Finally, the right to erasure, which lets users request deletion of their data, conflicts with technical realities. In AI systems, personal data may be spread across training weights, making it nearly impossible to remove without completely retraining the model. This adds costs and complexity that are especially challenging for startups.

CROSS-BORDER DATA AND LOCALIZATION

Stringent Localization Mandates

The Draft Rules require local data storage and prior government permission for any transfers, effectively ending free-flowing cloud integration with global partners.

- For Indian startups, this means building or leasing local data centers adding 15–25% to upfront costs.
- Companies scaling rapidly may face infrastructures hurdles, operational latency, and compliance delays.

International Collaboration Challenges

India's AI ecosystem thrives on collaboration with global researchers and services fine-tuning multilingual models, accessing worldwide datasets. Localization fragments these flows, inhibiting knowledge exchange.
A health-tech startup says it has had to halt plans to use an international lung-diagnosis ML tool due to tight data export restrictions.

[5] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), s. 5(1)(c) (data minimization) and s. 8(7) (data retention).

GOVERNMENT EXEMPTIONS & SURVEILLANCE RISK

Broad State Powers: DPDP allows exemptions for sovereignty, public order, and prevention, investigation, detection of crime. These broad terms may enable unchecked data collection. Without mandatory judicial oversight, mass-surveillance programs like facial recognition and behavioral profiling can happen without meaningful recourse.

Public Trust & Social Impact: Marginalized communities, already facing over-policing, may suffer the most from non-consensual AI surveillance. This undermines democratic norms and erodes faith in technology. Stories have surfaced about local activists whose voices were captured by public surveillance without their knowledge. This human cost remains hidden behind government immunity clauses. One of the most debated aspects of the Digital Personal Data Protection (DPDP) Act, 2023, is its provision for broad exemptions for the Indian government and its agencies. Under Section 17(2), the Central Government can exempt any instrumentality of the State from the Act's provisions in the interest of sovereignty, integrity, national security, public order, or friendly relations with foreign states.[6] This is particularly important regarding artificial intelligence (AI) since the state acts as both a regulator and an operator of AI-driven surveillance technologies. The conflict between individual privacy and state surveillance isn't new. However, the scale and opacity of AI technologies, combined with these legislative exemptions, create a dangerous mix with significant consequences for democratic rights, minority protections, and ethical governance.

LEGAL CONTEXT: THE PROPORTIONALITY DOCTRINE

[6] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), s. 17(1).

In its 2017 K.S. Puttaswamy judgment, the Supreme Court established a four-part proportionality test to evaluate privacy restrictions:

- Legality: The requirement for a law.
- Legitimate aim: The law must have a valid objective.
- Proportionality: There must be a rational connection between means and ends.
- Procedural safeguards: These are needed to prevent abuse.

While Section 17 of the DPDP Act meets the existence of law requirement, its lack of judicial or independent oversight raises constitutional concerns under the procedural safeguards test. Unlike the European Union's General Data Protection Regulation (GDPR), which requires data protection impact assessments and public interest balancing tests even for national security exceptions, India's law allows broad exemptions at the government's discretion.[7]This legal gap threatens to make mass surveillance not just allowed but largely unaccountable.

The AI Factor: Invisible Surveillance at Scale

AI greatly increases the state's surveillance capacity. With machine learning models powering facial recognition systems, predictive policing tools, social media monitoring, and citizen scoring algorithms, the government can process vast amounts of personal data in real-time. When this data is collected without consent and stored without time limits, the consequences are serious.

Real-World Examples: Delhi Police's Facial Recognition System reportedly has an 80% success rate, but internal reports showed that nearly 90% of those flagged were false positives, impacting marginalized groups like Muslims and Dalits disproportionately.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 35–36.

In Telangana, automated surveillance drones have monitored public protests, with footage often stored indefinitely. Aadhaar-linked AI systems are being tested to verify government scheme beneficiaries, but activists assert these systems frequently exclude deserving recipients due to technical errors or outdated data. These instances reveal a contradiction: AI is promoted as increasing efficiency, but when used without strong privacy protections, it can become a means of systemic exclusion and excessive surveillance.[8]

Human Cost: The Story of Seema and the Silent Camera

Seema Devi, a 39-year-old domestic worker from East Delhi, walks her daughter to school every morning. Unbeknownst to her, a recently installed AI-enabled CCTV camera on the street captures their daily movements. The footage is part of a city initiative to improve women's safety, yet Seema does not know how the data is stored, who has access to it, or if it could be used against her family. A few months later, her husband, falsely accused of a minor theft, finds himself listed in a predictive policing database due to AI-driven suspicion scoring. The family faces regular police visits, harming their reputation and mental well-being. There was no way to respond: no grievance mechanism, no data deletion, no apology. For individuals like Seema, surveillance isn't just an abstract concept; it's a painful reality.

Comparing Global Approaches: While national security is a common reason for privacy exceptions, most democracies include checks and balances. Here's how India compares:

India remains one of the few large democracies where broad data access and state use of AI occur with minimal legal or democratic limitations.

Policy Recommendations: To prevent India from becoming a surveillance-heavy state under the guise of AI modernization, several reforms are necessary:

[8] Internet Freedom Foundation, Surveillance in India: Case Study – Telangana's Use of Drones, available at: https://internetfreedom.in

1. Narrow and Precise Exemptions: Revise Section 17 to limit exemptions to clearly defined threats, such as terrorism and espionage, instead of vague terms like public order.

2. Mandatory Oversight: Establish an Independent Oversight Board, possibly under the DPB, to assess each state exemption request for proportionality and necessity.

3. Sunset Clauses: Each data collection or AI surveillance order should have a time limit of six months and require renewal based on demonstrated need.

4. Audit Trails and Public Registers: Any government use of AI for surveillance must create auditable logs and maintain a public disclosure register with redactions for national security.

5. Privacy Impact Assessments: Mandate Privacy Impact Assessments (PIAs) before any AI system is deployed by the government that processes personal data.

6. Consent or Notification Mechanisms: Citizens should be informed when they are under AI-based surveillance, even retroactively, and must be able to challenge incorrect data.

Ethical AI Governance in a Democratic India

The potential of AI in India is clear: smarter cities, better healthcare, faster justice delivery. But without democratic safeguards, AI can widen social divides and make privacy a luxury. In such a diverse country as India, technology must be inclusive, clear, and accountable. A well-regulated AI environment doesn't mean being against surveillance; rather, it requires justified, audited, and consensual use of surveillance technologies. The DPDP Act, in its current state, does not insist on this from the government. The real question is not whether the government should use AI but how it should use it. That approach must be governed by law, not discretion; by rights, not secrecy.

REGTECH: SANDBOXING & INNOVATION PATHWAYS

What Are Sandboxes?

Pilot environments where AI solutions can operate under regulatory oversight, with temporary exceptions to data norms, are emerging globally and DPDP contemplates a similar concept.

Pros and Cons

- Pros: Allows controlled experimentation, fosters rapid iteration, and helps calibrate rules.
- Cons: No clear criteria yet in India for who qualifies; without data minimization safeguards, sandboxes risk turning into loopholes for Big Tech experiments, with little benefit for smaller players.

How It Should Work

- Tiered access: Early-stage R&D gets more flexibility, but production uses should remain under full compliance.
- Transparent reporting: Mandatory logs, public reporting, and data exit rules should accompany sandbox use.

SME Compliance & Economic Strain

For India's small and medium enterprises (SMEs), especially AI startups, the compliance requirements under the DPDP Act, such as audits, documentation, Data Protection Impact Assessments (DPIAs), and hiring Data Protection Officers, can lead to annual costs ranging from ₹500,000 to ₹5 lakh, according to industry estimates. These financial and operational pressures might push innovation to less regulated areas or slow growth in important sectors like regional language AI, agritech, or health-tech. Without tailored compliance support, the Act could unintentionally hinder grassroots innovation. This would particularly impact those addressing India-specific challenges with limited resources and early-stage funding.

COMPARATIVE INSIGHTS & GLOBAL MOMENTUM: LEARNING FROM GLOBAL PRACTICES TO STRENGTHEN INDIA'S DATA AND AI GOVERNANCE

As India embarks on the path of regulating data privacy through the Digital Personal Data Protection (DPDP) Act, 2023, it becomes essential to understand how this framework aligns or diverges from international legal regimes. Globally, countries are developing comprehensive legal systems that strike a balance between safeguarding personal privacy and promoting responsible innovation, especially in artificial intelligence (AI). India, as one of the largest digital economies, cannot afford to operate in isolation. Instead, it must draw from global lessons to design a responsive, context-aware regulatory ecosystem that accommodates its unique needs while meeting international standards.

GDPR Vs. DPDP: Key Differences in Scope And Flexibility

The European Union's General Data Protection Regulation (GDPR) is widely regarded as the gold standard for personal data protection. Enacted in 2018, it not only emphasizes individual rights and data controller obligations but also provides multiple lawful bases for data processing. One such basis is legitimate interest, which allows entities to process personal data without explicit consent, provided they can demonstrate that the interest pursued does not override the rights and freedoms of the data subject. In contrast, the DPDP Act mandates explicit, purpose-specific consent as the primary lawful basis for processing personal data. This rigidity becomes particularly challenging in the context of AI systems, which are inherently dynamic and often require adaptive data use beyond the original stated purpose. For example, AI models are frequently retrained, fine-tuned, or repurposed with evolving data sets. Under DPDP, such repurposing would require repeated re-consent, slowing down iterative innovation especially for startups and resource-constrained developers. The absence of alternative legal bases such as legitimate interest or contractual necessity could thus hinder the development of robust AI tools in India. Another key distinction is that GDPR anticipates AI-related risks through transparency, accountability, and fairness provisions, and its future alignment with the EU AI Act further strengthens these

safeguards. The DPDP Act, however, lacks specific provisions addressing AI accountability.[9] There are no mandated algorithmic audits, risk categorization of AI systems, or transparency standards such as documentation or data sheets. This omission may lead to a regulatory gap as AI becomes increasingly embedded in everyday services and governance.

EMERGING REGULATORY MODELS: RISK-BASED AND SECTOR-SPECIFIC APPROACHES

Around the world, new regulatory models are emerging to address the challenges posed by artificial intelligence. The EU AI Act, in particular, is a pioneering legislative initiative that proposes a risk-based classification of AI systems into high-risk, limited-risk, and low-risk categories. High-risk systems, such as those used in healthcare, law enforcement, or critical infrastructure would be subject to strict requirements including algorithmic transparency, human oversight, accuracy testing, and mandatory impact assessments. Limited-risk systems would face transparency obligations like disclosure of AI use, while low-risk systems would be largely exempt from heavy regulation. This tiered approach acknowledges that not all AI systems pose the same level of risk and offers regulatory flexibility without compromising fundamental rights. India currently lacks this granularity in its legal framework.[10]The DPDP Act treats all digital personal data more or less uniformly, without regard for how it is used or the potential harm it may cause. This one-size-fits-all approach could discourage the development of low-risk AI innovations, such as language learning bots or crop advisory systems for farmers which could otherwise benefit millions without posing serious privacy risks. The New Delhi G20 Declaration (September 2023) also recognized the importance of ethical, human-centric AI. It echoed principles found in both the GDPR and DPDP such as transparency, fairness, and accountability. However, the declaration

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation (GDPR), art. 6(1)(f).
[10] The EU Artificial Intelligence Act: Regulating High-Risk AI Systems, European Commission, 2021.

remains broad in tone and does not address India-specific implementation challenges. For example, how will AI be made ethical and human-centric for a rural farmer using a voice bot, or a small fintech firm trying to provide loans to low-income groups? These questions remain unanswered in both international and domestic discourse.

RECOMMENDATIONS BASED ON GLOBAL BEST PRACTICES

1. Risk-Based Regulation for AI Systems: India should adopt a layered regulatory approach similar to the EU AI Act. AI systems used in sensitive areas such as healthcare, education, and justice should be categorized as high-risk and face stricter compliance obligations, including algorithmic audits, fairness checks, and human-in-the-loop governance. In contrast, low-impact systems, such as recommendation engines for music or translation tools, could benefit from more relaxed requirements. This tiered approach would allow for targeted regulation without overburdening developers.

2. Expand Legal Grounds for Data Processing: Introducing additional lawful bases such as legitimate interest or contractual necessity would ease the compliance burden for companies, especially in enterprise or business-to-business (B2B) settings. It would enable organizations to process data when it's reasonably expected and necessary for service delivery, without undermining core privacy rights. This would align India’s framework with that of GDPR and enable more practical and scalable AI deployment.

3. Enforce Explainability and Transparency Standards: AI systems that make impactful decisions such as denying a loan, assigning risk scores, or filtering job applications must be explainable. India should require developers to maintain model cards or data sheets outlining the training data used, limitations of the algorithm, accuracy rates, and fairness metrics. This would enhance user trust, promote transparency, and help regulators understand the implications of emerging technologies.

4. Limit Government Exemptions: Section 17 of the DPDP Act gives the Indian government broad discretion to exempt its agencies from data protection norms for reasons such as national security and public order. This is concerning, particularly when AI surveillance tools are involved. Unlike GDPR, which mandates public interest balancing tests and independent oversight, the DPDP Act lacks judicial or parliamentary safeguards.[11] India should reform this provision to ensure that exemptions are narrow, time-bound, and reviewed independently, to prevent abuse and build public trust.

5. Implement Smart Regulatory Sandboxes: India should actively promote AI sandboxes-controlled environments where new technologies can be tested under regulatory supervision. These sandboxes should have clearly defined objectives, transparent evaluation criteria, and exit rules. While they provide flexibility, they must also be monitored to prevent misuse, especially by large tech companies looking to bypass compliance under the guise of experimentation.

6. Introduce Tiered Data Retention Norms: AI models, particularly in healthcare or finance, often require long-term data to detect patterns and improve over time. Instead of a blanket three-year limit, the law could allow longer retention for anonymized data or where explicit consent is provided.[12]This would ensure both privacy and accuracy in data-driven systems.

7. Support for SMEs and Startups: Small and medium enterprises (SMEs) are often the most affected by complex regulations. Compliance costs for audits, Data Protection Officers (DPOs), and documentation can be prohibitive. India should introduce support mechanisms, such as subsidies, shared compliance toolkits, open-source consent managers, and template DPIA (Data

[11] GDPR, art. 6(1)(f); see also Handbook on European Data Protection Law, European Union Agency for Fundamental Rights (FRA), 2018.
[12] Privacy International, Data Retention and AI Development: Balancing Access and Protection, Research Brief, 2022.

Protection Impact Assessment) guides. This would democratize access to innovation and prevent regulatory overreach from stifling grassroots development.

Building India's Inclusive Tech Future: India has taken a bold step forward with the DPDP Act, 2023. Yet, for the law to truly support a digital future that is both innovative and rights-respecting, it must evolve in line with global best practices. By adopting a risk-based, flexible, and transparent approach, India can ensure that its regulatory regime encourages safe AI innovation while protecting citizens 'fundamental rights. Comparisons with GDPR, the EU AI Act, and other global frameworks offer clear lessons: effective regulation is not about being strict, it's about being smart, proportionate, and people-first.

As the digital world becomes more complex, India's success will depend not just on protecting data, but on empowering innovation to solve real-world problems ethically, inclusively, and responsibly.

HUMAN-CENTERED SCENARIOS: THE REAL-WORLD IMPACT OF DATA PRIVACY

Regulations on AI

Real-World Implications of the DPDP Act: The Digital Personal Data Protection (DPDP) Act is more than a theoretical milestone; it carries concrete implications for the real-world use of artificial intelligence (AI). To understand the human dimension of these changes, let's examine a few case studies that highlight the tension between privacy protection and technological innovation in India's evolving tech ecosystem.

Fintech: AI in Micro-Lending and Creditworthiness Assessment

A micro-lending startup in India uses AI to assess creditworthiness and provide loans to underserved populations. However, under the DPDP Act, the company must obtain explicit

consent from every borrower before using historical financial data to train its models. This requirement significantly slows down operations, reduces the accuracy of credit models, and limits the startup's ability to offer competitive loan terms.[13] As a result, some potential borrowers who could benefit from lower interest rates—are excluded altogether, deepening the financial divide.

Health-tech: Diagnostic AI and Cross-Border Data Barriers

In the healthcare sector, an AI-based diagnostic tool designed to detect diseases from patient data faces deployment delays due to the DPDP's data localization requirements. The model requires access to global datasets to ensure accurate and timely diagnoses. However, cross-border data transfers are restricted unless explicitly approved by the government. This bottleneck impedes the tool's implementation in underserved regions, where access to advanced healthcare is already limited. Consequently, the Act, while protective, may inadvertently stall life-saving innovations.

Rural Education: Voice-Based AI Tutors

In rural India, a voice-based tutoring bot supports low-income students by offering personalized lessons. Yet, it struggles to communicate effectively with parents due to limited digital literacy and the complexity of DPDP's consent norms. The bot's natural language processing capabilities are still developing, and without clear, context-aware explanations, it fails to earn the trust of rural families. This mistrust creates a barrier to the adoption of AI in education particularly in regions that could benefit the most.

These examples underscore a key reality: privacy-first regulations, though well-intentioned, can have unintended human consequences. Safeguarding rights is essential, but not at the cost of

[13] Vidushi Marda, Artificial Intelligence and the Right to Privacy in India: A Constitutional Perspective, Indian Journal of Law and Technology, Vol. 14, 2018, pp. 1–33.

equitable access to life-changing technology. The challenge lies in designing laws that protect both individual rights and the broader social good.

Path Ahead: Synergy Between Policy and Technology

The DPDP Act is a significant achievement. IR. Shokri & V. Shmatikov, "Privacy-Preserving Machine Learning: Threat Models and Solutions," *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, 2015, pp. 62–77.[14]This means categorizing AI applications based on their potential impact on privacy. For instance, high-risk applications (e.g., healthcare, predictive policing) could be subject to stricter scrutiny, while low-risk uses (e.g., content recommendation systems) might warrant lighter oversight.

To improve transparency, developers should be required to:

- Maintain audit trails of model development.
- Document their models clearly.
- Conduct ethical impact assessments.

These measures should become standard criteria for AI governance, ensuring accountability, fairness, and non-discrimination in AI systems. Additionally, India should invest in privacy-preserving technologies like homomorphic encryption and federated learning. These tools enable data collaboration without compromising individual privacy, paving the way for responsible AI that respects both innovation and fundamental rights.

[14] R. Shokri & V. Shmatikov, Privacy-Preserving Machine Learning: Threat Models and Solutions, Proceedings of the 2015 IEEE Symposium on Security and Privacy, 2015, pp. 62–77.

CONCLUSION: A HUMAN-CENTERED APPROACH TO AI REGULATION

The **Digital Personal Data Protection Act, 2023**, marks a pivotal moment in India's digital governance journey. It represents the country's first comprehensive legal recognition of data privacy as a statutory right, building on the constitutional principles established in *Justice K.S. Puttaswamy v. Union of India*.

[15]While the Act rightly empowers individuals and holds data fiduciaries accountable, it also presents new challenges for AI development. AI thrives on access to large, diverse datasets, frequent updates, and cross-border collaboration, all of which are hindered by rigid consent norms and localization mandates. The absence of AI-specific provisions like explainability or impact assessments further complicates matters, particularly for small businesses, startups, and research institutions. India now stands at a critical crossroads. A one-size-fits-all approach may protect privacy, but could also undermine AI-led progress in sectors such as education, healthcare, agriculture, and governance.[16]

TO MOVE FORWARD:

- Introduce context-sensitive consent mechanisms.
- Differentiate regulation based on AI risk.
- Establish regulatory sandboxes for safe innovation.
- Ensure strong public oversight especially for state-driven AI use.

Most importantly, India must place the human impact of both privacy violations and tech exclusion at the center of policymaking. If thoughtfully implemented, the DPDP Act has the potential to

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[16] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).

become not just a constraint but a catalyst enabling the development of AI that is ethical, inclusive, and aligned with democratic values.