REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

Balancing Innovation and Privacy: The Role of AI Governance in Shaping Data Protection Jurisprudence under the Digital Personal Data Protection Act, 2023

Apurva Mishra[1*], Dr Shubham Sharma[2]

[1*]Research Scholar, Chandigarh University, Chandigarh, India.
[2]Assistant Professor, Manipal University, Jaipur, Rajasthan, India.

***Corresponding Author:** Apurva Mishra
*Email: apurvamishra2141@gmail.com

Abstract
The rapid integration of Artificial Intelligence (AI) in various sectors has transformed the digital economy, promising unprecedented innovation while simultaneously challenging fundamental rights—most notably, the right to privacy. In response to the growing concerns over data protection and algorithmic accountability, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act). This paper critically examines the tension between AI-driven innovation and the right to privacy, evaluating how the DPDP Act attempts to balance economic growth and civil liberties. It further explores how Indian courts and regulatory authorities may interpret and implement AI governance principles in light of constitutional privacy jurisprudence. Through a doctrinal analysis, this paper contributes to ongoing debates on AI regulation and proposes a nuanced policy framework for responsible AI governance in India.

1.Introduction

Artificial Intelligence (AI) has emerged as one of the most transformative forces in the 21st century, redefining how societies operate, economies function, and individuals interact with digital systems. From enhancing diagnostic accuracy in healthcare to enabling algorithmic trading in finance, from personalizing learning experiences in education to streamlining administrative functions in governance, AI technologies are becoming deeply embedded in every aspect of modern life. The pervasive application of machine learning algorithms, natural language processing, and data-driven decision-making systems has significantly improved efficiency and productivity across sectors.However, this technological revolution has not come without significant ethical and legal concerns, especially in relation to individual rights and freedoms. One of the most critical areas of concern surrounding AI is its reliance on vast quantities of personal data. AI systems, particularly those designed for predictive analytics, automated decision-making, and profiling, depend on massive datasets to train algorithms and refine outputs. These datasets often include sensitive personal information such as health records, financial transactions, behavioral patterns, and biometric identifiers. While this data-centric approach fuels innovation and commercial competitiveness, it simultaneously raises profound questions about data ownership, informational self-determination, and the erosion of personal privacy[1] .

The fundamental principles of autonomy and informed consent are increasingly being challenged in an AI-driven digital economy. As Reuben Binns observes, algorithmic systems often operate in opaque ways, making it difficult for individuals to understand how their data is used or to exercise meaningful control over it[1]. The concept of "algorithmic accountability" is still evolving, and current frameworks frequently lack mechanisms for transparency, explainability, and redressal. Moreover, AI systems can reinforce existing biases, engage in discriminatory practices, and contribute to surveillance capitalism—a phenomenon where data is commodified for profit at the expense of user rights[2].
In the Indian context, these challenges are exacerbated by the absence of a robust legal framework historically equipped to deal with digital rights. Until recently, data protection in India was governed by piecemeal provisions under the Information Technology Act, 2000 and related rules, which offered limited safeguards against modern forms of digital exploitation[3]. The landmark Supreme Court judgment in *Justice K.S. Puttaswamy v. Union of India*[4] recognized the right to privacy as a fundamental right under Article 21 of the Indian Constitution. This judgment laid the groundwork for the development of comprehensive data protection legislation by emphasizing the principles of legality, necessity, and proportionality in state interference with privacy.

In response to the growing need for data governance and regulatory clarity, the Government of India introduced the Digital Personal Data Protection Act, 2023 (DPDP Act). This Act represents the country's first comprehensive attempt

[1] Reuben Binns, "Algorithmic Accountability and Public Reason" (2018) 31(4) *Philosophy & Technology*.
[2] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs, 2019).
[3] Information Technology Act, 2000, Government of India.
[4] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

to create a legal architecture that balances individual data rights with the demands of digital innovation[5]. It aims to establish a framework for lawful processing of personal data, empower individuals as "Data Principals" with enforceable rights, and impose responsibilities on "Data Fiduciaries" who determine the purpose and means of data processing. The DPDP Act also sets out procedural safeguards, enforcement mechanisms, and conditions for cross-border data transfer—marking a significant step toward harmonizing India's digital economy with global data protection standards.

One of the distinguishing features of the DPDP Act is its dual focus: on the one hand, it aims to protect the privacy interests of individuals; on the other, it seeks to create an enabling environment for technological innovation and economic growth[6]. The Act attempts to strike a balance by ensuring regulatory compliance without stifling the dynamism of the digital economy. It reflects a pragmatic approach by acknowledging that over-regulation could hinder entrepreneurship, foreign investment, and the development of indigenous AI solutions. However, this balance remains fragile and contested, especially given the Act's broad exemptions for government agencies and the limited scope for algorithmic audits and impact assessments[7].

The central challenge, therefore, lies in the implementation of the DPDP Act in a manner that genuinely safeguards the right to privacy while not obstructing the legitimate use of AI technologies. The Act, though a necessary and timely intervention, is only a starting point. Its effectiveness will depend on the interpretative role of the judiciary, the independence and capacity of the Data Protection Board of India, and the development of complementary legal standards on AI governance, algorithmic transparency, and ethical data use[8].

In essence, the relationship between AI and privacy is not inherently antagonistic; rather, it is a matter of thoughtful regulation and institutional design. India's efforts to navigate this complex terrain through the DPDP Act offer an opportunity to develop a rights-based, innovation-friendly digital ecosystem. However, whether this legislation succeeds in achieving its dual objectives will depend on continuous legal evolution, stakeholder engagement, and judicial oversight grounded in constitutional values.

2.AI-Driven Innovation and the Digital Economy[1]

Artificial Intelligence (AI) technologies have significantly reshaped how organizations operate and how decisions are made, offering enhanced productivity, efficiency, and precision across sectors. The transformative potential of AI lies in its ability to process large volumes of data using advanced computational methods such as large-scale data analytics, machine learning (ML), and predictive modeling. These technologies allow businesses and governments to derive actionable insights, predict trends, automate processes, and personalize services. AI-enabled systems are particularly adept at identifying patterns, classifying behaviors, and making data-driven decisions in real-time, often surpassing human capabilities in speed and accuracy[9].

However, the functioning and efficacy of such systems rely heavily on the availability and analysis of enormous datasets, which frequently include sensitive personal information. These datasets may contain a wide spectrum of personally identifiable information (PII), including biometric data, health records, financial transactions, browsing history, geo-location details, and behavioral patterns. The aggregation and algorithmic processing of such data—often without the explicit awareness or meaningful consent of individuals—pose substantial risks to the right to privacy[10]. This challenge is exacerbated in digital economies where personal data has become a critical economic resource and a central asset for companies operating on data-driven business models[11].

One of the core features of AI-driven innovation that directly impacts privacy is automated decision-making**,** where machines make or influence decisions that affect individuals—such as credit scoring, job recruitment, insurance underwriting, or predictive policing. These decisions are frequently opaque and lack transparency regarding the logic or rationale behind outcomes, making it difficult for individuals to contest or understand the basis of the decision[12]. Another key concern is data profiling**,** where individuals are categorized based on data attributes to infer behaviors,

[5] Digital Personal Data Protection Act, 2023, Government of India.
[6] NITI Aayog, "Responsible AI for All: Discussion Paper" (2021).
[7] Ujwal Singh, "Balancing AI Regulation and Innovation in India: A Legal Analysis" (2023) 45 *Journal of Indian Law and Technology* 112.
[8] Nandan Nilekani and others, "Data Empowerment and Protection Architecture (DEPA)" (NITI Aayog, 2020).
[9] Russell Stuart and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd edn (Pearson Education, 2010).
[10] Solove Daniel J, "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477.
[11] Zuboff Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[12] Binns Reuben, "Algorithmic Accountability and Public Reason" (2018) 31(4) *Philosophy & Technology*.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

preferences, or risks. While such profiling can enhance service efficiency, it may also reinforce stereotypes, enable discrimination, and erode individual agency[13].

Moreover, AI technologies increasingly contribute to **surveillance practices**, both by state and corporate entities. From facial recognition software deployed in public spaces to data-tracking applications embedded in consumer devices, AI is facilitating a new era of pervasive surveillance. The Organization for Economic Co-operation and Development (OECD), in its AI Principles**,** has emphasized the importance of transparency, accountability, and the protection of human rights in the deployment of AI technologies[14]. Without adequate legal safeguards, the boundaries between legitimate data processing and intrusive surveillance become dangerously blurred, thereby undermining the right to informational self-determination.

In the context of India's emerging digital economy, the stakes are particularly high. While data-driven innovation promises economic growth, job creation, and improved service delivery, the absence of robust privacy frameworks risks creating a landscape of digital exploitation and regulatory opacity. Therefore, there is an urgent need to harmonize AI innovation with comprehensive data protection legislation that upholds individual rights. The Digital Personal Data Protection Act, 2023, represents a significant step in this direction, but its success depends on how effectively it enforces principles of consent, purpose limitation, and data minimization in AI systems Digital Personal Data Protection Act, 2023, Government of India.[15].

3.The Right to Privacy in the Indian Legal Framework[1]

The recognition of the right to privacy as a fundamental right in India marked a watershed moment in Indian constitutional jurisprudence. The landmark judgment of the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* [(2017) 10 SCC 1] decisively held that privacy is intrinsic to the right to life and personal liberty under Article 21 of the Constitution**,** as well as to other fundamental freedoms guaranteed by Part III of the Constitution. The Court laid down a robust framework for evaluating any state or private action that impinges upon this right, formulating **a** three-pronged test for lawful limitations on privacy: legality, necessity and proportionality, and legitimate state aim. These principles have since become foundational for any analysis of laws or policies dealing with data collection, surveillance, and personal autonomy.[16]

The principle of legality requires that any invasion of privacy must have a basis in a valid law. The requirement of necessity and proportionality implies that the action taken must be necessary for achieving a legitimate objective, and the means adopted must be proportionate to the aim sought to be achieved. The third limb, legitimate state aim**,** mandates that the objective must be constitutionally valid and justifiable in a democratic society.[17] These principles draw heavily from international human rights jurisprudence and place significant restrictions on the arbitrary use of power in a data-driven governance structure.

The critical issue today is whether the existing legal instruments, especially the Digital Personal Data Protection Act, 2023 (DPDP Act)**,** adhere to the constitutional standards established in the Puttaswamy judgment, particularly in the context of Artificial Intelligence (AI) systems**.** AI-based technologies, by their very nature, operate on massive volumes of personal data, often engaging in automated decision-making, surveillance, and profiling**,** which pose direct challenges to privacy and autonomy.[18] While the DPDP Act attempts to regulate personal data processing and offers individuals certain rights such as the right to consent, correction, and grievance redressal**,** questions remain regarding its sufficiency in ensuring constitutional compliance in the AI era.

One significant gap lies in the lack of explicit provisions regulating AI-specific risks, such as algorithmic opacity, discriminatory outcomes, and automated profiling. The Act does not provide detailed accountability mechanisms for AI developers or processors, nor does it impose transparency obligations for automated decision-making systems—a

[13] Wachter Sandra, Mittelstadt Brent, and Floridi Luciano, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) *International Data Privacy Law* 76.
[14] OECD, "OECD Principles on Artificial Intelligence" (2019), https://www.oecd.org/going-digital/ai/principles/ accessed 18 March 2025.
[15] Digital Personal Data Protection Act, 2023, Government of India.
[16] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[17] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins Publishers India, 2019).
[18] Reuben Binns, "Algorithmic Accountability and Public Reason" (2018) 31(4) *Philosophy & Technology*.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

critical concern in light of the Puttaswamy doctrine.[19] Furthermore, the absence of a robust Data Protection Board with full independence and judicial oversight raises doubts about the enforceability and proportionality of the regulatory regime under the Act.[20]

Therefore, despite the DPDP Act's progressive outlook in creating a data protection framework, it arguably falls short of fully aligning with the constitutional yardsticks of privacy protection laid down by the Supreme Court. As AI systems increasingly mediate human interactions and governance, there is a pressing need for complementary legal instruments and judicial interpretations that uphold the sanctity of individual rights in a technologically evolving ecosystem. The tension between innovation and civil liberties must be mediated through a rights-based regulatory approach grounded in constitutional values. OECD, "Principles on Artificial Intelligence" (2019), https://www.oecd.org/going-digital/ai/principles/ accessed 18 March 2025.

4.Overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant legislative step toward protecting informational privacy in India. It introduces a range of critical provisions intended to regulate the collection, processing, storage, and dissemination of personal data in both public and private domains. The Act is built upon foundational principles such as lawful and fair processing, purpose limitation**,** data minimization**, and** accountability of data fiduciaries**.**[21] One of the core features of the Act is the classification of entities handling personal data into "Data Fiduciaries" **and** "Significant Data Fiduciaries"**,** which mirrors global best practices, including the EU General Data Protection Regulation (GDPR).[22] Data Fiduciaries are required to ensure lawful processing, maintain data security, and fulfill obligations related to transparency, grievance redressal, and accountability mechanisms.

The Act empowers individuals, identified as "Data Principals"**,** with specific rights including the right to information**,** right to correction and erasure**,** right to grievance redressal**,** and right to nominate another individual to exercise rights in the event of death or incapacity.[23] These rights are aimed at restoring informational autonomy to individuals who often remain vulnerable in a data-driven digital economy. Furthermore, the DPDP Act outlines conditions for cross-border data transfers, permitting such transfers to notified countries subject to safeguards, thereby attempting to strike a balance between data sovereignty and global digital commerce.[24]

However, despite these commendable steps, the Act falls short in addressing Artificial Intelligence (AI)-specific concerns**,** particularly those arising from automated decision-making, algorithmic bias, and lack of transparency in AI systems**.**[25] The law does not explicitly regulate algorithmic profiling, nor does it require Data Fiduciaries to provide individuals with meaningful information about the logic involved in automated decisions**,** which is critical for ensuring fairness and accountability. This omission is particularly concerning in light of the increasing use of AI in areas such as finance, healthcare, law enforcement, and targeted advertising—sectors that directly impact individual rights and freedoms.[26]

Moreover, there is no mandatory requirement for impact assessments or audits of AI-based data processing systems, a key safeguard found in other jurisdictions such as the EU Artificial Intelligence Act and the OECD AI Principles. The absence of such provisions exposes a regulatory vacuum that can be exploited by AI developers and data controllers, ultimately undermining the very goal of protecting personal data. The DPDP Act also lacks clarity on how Significant Data Fiduciaries using AI technologies will be subjected to stricter compliance regimes, thereby creating an uneven and ambiguous legal landscape.

---

[19] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) *International Data Privacy Law* 76.

[20] Anirudh Burman, "India's Data Protection Law: Striking a Balance Between Privacy and Innovation" (2023) Carnegie India, https://carnegieindia.org accessed 18 March 2025.

[21] Government of India, *Digital Personal Data Protection Act, 2023*, Gazette Notification No. 39 of 2023.

[22] Graham Greenleaf, "Global Data Privacy Laws 2023: A Ten-Year Review" (2023) 172 *Privacy Laws & Business International Report* 10.

[23] Rahul Matthan, "The DPDP Bill, 2023: An Analysis of the Rights of Data Principals" (2023) https://takshashila.org.in accessed 18 March 2025.

[24] Pranesh Prakash, "Cross-border Data Flows and India's Data Protection Law" (2023) *Centre for Internet and Society* https://cis-india.org accessed 18 March 2025.

[25] Reuben Binns, "Human Judgment in Algorithmic Decision-Making: The Role of Transparency and Explanation" (2018) 31(2) *Philosophy & Technology* 183.

[26] Sandra Wachter et al., "Transparent, Explainable, and Accountable AI for the Public Sector" (2019) *Oxford Internet Institute Working Paper*.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

In essence, while the DPDP Act is a laudable attempt at codifying data protection norms in India, its technology-neutral approach overlooks the nuanced challenges posed by AI systems. To effectively safeguard the fundamental right to privacy, there is a pressing need to integrate AI governance frameworks, including algorithmic accountability, explainability standards, and human-in-the-loop mechanisms, within the larger data protection architecture.[27] Without such AI-specific statutory interventions, the efficacy of the DPDP Act in regulating the evolving digital ecosystem remains limited.

5.Balancing Innovation and Privacy: A Legal Analysis

One of the significant critiques of the Digital Personal Data Protection Act, 2023 (DPDP Act) is that while it aspires to promote a digitally innovative and business-friendly environment, it does so at the cost of rigorous oversight mechanisms**.** The Act consciously avoids imposing stringent regulatory obligations—such as mandatory Data Protection Impact Assessments (DPIAs)**,** algorithmic audits**,** or ethical evaluations for Artificial Intelligence (AI) systems**.**[28] While this approach may reduce compliance costs and accelerate digital adoption across industries, it also leaves considerable gaps in ensuring accountability and transparency in the deployment of automated systems that process personal data.

Globally, countries like those in the European Union are advancing toward robust AI governance frameworks that include risk assessments and explainability requirements for algorithmic systems.[29] In contrast, India's DPDP Act remains technology-neutral, and does not distinguish between traditional data processing and AI-driven data processing**,** despite the profound privacy implications posed by the latter. Such legislative silence is problematic, especially considering that AI algorithms are often opaque**,** biased**, or** discriminatory**,** and can significantly affect individuals without adequate redress mechanisms.

Furthermore, the Act grants broad exemptions to government agencies on grounds such as national security, public order, and law enforcement.[30] These blanket exemptions**,** devoid of any meaningful judicial or parliamentary oversight, risk institutionalizing surveillance regimes and diluting the fundamental right to privacy recognized under Article 21 of the Indian Constitution. As pointed out by scholars like Martin Tisné, unchecked state access to personal data under the guise of public interest can severely weaken democratic norms and individual freedoms.[31] Therefore, while the DPDP Act aims to catalyze India's digital economy, its lack of enforceable accountability provisions for AI systems and wide government exemptions raise substantial concerns about the balance between innovation and civil liberties**.**

6.Judicial Interpretation and the Role of Regulators

The role of the Indian judiciary in interpreting the Digital Personal Data Protection Act, 2023 (DPDP Act) will be pivotal in shaping India's data protection jurisprudence in harmony with the constitutional right to privacy. The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017)[32] recognized privacy as a fundamental right under Article 21 and laid down the three-fold test **of** legality, necessity and proportionality, and legitimate state aim for any state action infringing this right. These principles are expected to serve as a constitutional lens through which the provisions of the DPDP Act will be judicially examined.

With the growing deployment of AI technologies, future litigation is likely to revolve around critical issues such as the legality of AI-driven profiling**,** the validity and scope of consent mechanisms in automated decision-making processes, and the extent of government exemptions under Section 17 of the Act.[33] Questions may arise about whether consent obtained through automated interfaces truly satisfies the standards of free, informed, and specific consent, as required under data protection principles.[34] Additionally, the courts will be called upon to determine whether algorithmic opacity and lack of explainability violate individuals' rights to autonomy and due process.

---

[27] Anirudh Burman, "AI Regulation and India's Data Protection Framework: A Missed Opportunity?" (2023) Carnegie India https://carnegieindia.org accessed 18 March 2025.
[28] Government of India, *Digital Personal Data Protection Act, 2023*, Gazette Notification No. 39 of 2023.
[29] European Commission, *Proposal for a Regulation on Artificial Intelligence (AI Act)* COM/2021/206 final.
[30] Government of India, *DPDP Act 2023*, Section 17.
[31] Martin Tisné, "The Data Delusion: Protecting Individual Rights and Collective Freedom in the Age of Surveillance" (2020) *Carnegie Endowment for International Peace* https://carnegieendowment.org/2020/11/17/data-delusion accessed 18 March 2025.
[32] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[33] Government of India, *Digital Personal Data Protection Act, 2023*, Gazette Notification No. 39 of 2023, s 17.
[34] Graham Greenleaf, "Global Data Privacy Laws 2023: DPAs, Consent, and Enforcement" (2023) 182 *Privacy Laws & Business International Report* 2.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

Moreover, the Data Protection Board of India (DPBI)**,** as the regulatory authority under the Act, must be sufficiently empowered and independent to ensure effective enforcement.[35] Its role in adjudicating disputes, imposing penalties, and monitoring AI-based data processing activities will be essential for upholding data protection norms. However, without strong institutional autonomy and judicial oversight, the DPBI risks becoming a toothless watchdog.[36] Thus, the judiciary's interpretive and supervisory functions, along with an empowered DPBI, will be crucial to ensure that AI governance aligns with constitutional values and safeguards individual privacy in the digital age.

7.Global Comparisons and Lessons for India

India's regulatory approach to artificial intelligence and data protection can benefit significantly by drawing lessons from established international frameworks such as the European Union's General Data Protection Regulation (GDPR) and Canada's Artificial Intelligence and Data Act (AIDA**)**. These frameworks offer progressive models that integrate algorithmic accountability with individual rights protection in the context of emerging technologies.

The GDPR**,** implemented in 2018, mandates Data Protection Impact Assessments (DPIAs) for high-risk processing activities, including automated decision-making and profiling**.**[37] Article 35 of the GDPR requires organizations to evaluate risks to data subjects and adopt mitigation strategies prior to deploying such systems. Additionally, Article 22 of the GDPR provides individuals the right not to be subject to decisions based solely on automated processing, thereby introducing a layer of algorithmic transparency and human oversight.[38] These provisions strike a critical balance between technological innovation **and** privacy protection.

Similarly, Canada's AIDA, introduced in 2022, proposes a forward-looking legal framework specifically for high-impact AI systems**,** emphasizing risk classification, impact assessments, transparency measures, and third-party audits.[39] The Act places accountability obligations on AI system deployers and requires public disclosure of how AI technologies impact individuals and society. Such legislation not only enhances trust in AI technologies but also ensures proactive regulatory intervention in cases of algorithmic harm or bias.

By comparison, the Digital Personal Data Protection Act, 2023 (DPDP Act) in India does not explicitly mandate AI-specific audits, algorithmic transparency, or mandatory impact assessments**,** creating potential regulatory gaps.[40] Hence, Indian policymakers can look toward integrating best practices from GDPR and AIDA to formulate AI governance frameworks that protect individual rights while fostering technological development in the digital economy**.**

8.Policy Recommendations

This paper puts forth a set of critical recommendations aimed at strengthening AI governance and data protection frameworks in India, especially in light of the Digital Personal Data Protection Act, 2023 (DPDP Act**)** and the increasing deployment of AI systems in public and private sectors. The first recommendation is the mandatory introduction of AI impact assessments**.** These assessments would require organizations to evaluate the potential risks, harms, and discriminatory outcomes of AI applications before their deployment, similar to the Data Protection Impact Assessments (DPIAs) under the European Union's General Data Protection Regulation (GDPR).**[41]** Such pre-emptive evaluations are crucial for identifying algorithmic bias, ensuring fairness, and safeguarding fundamental rights.

Secondly, there is a need to incorporate algorithmic transparency mechanisms. This would include mandatory disclosures of AI system architecture, logic, data sources, and decision-making criteria**,** especially in contexts involving automated profiling or decision-making that impacts individuals' rights. Transparency enables both regulatory oversight **and** public accountability, and is increasingly considered a core principle in AI governance worldwide.[42]

[35] DPDP Act 2023, s 19.
[36] Pranesh Prakash, "The Weaknesses in India's Data Protection Bill" (2023) *Centre for Internet and Society* https://cis-india.org/internet-governance/blog/the-weaknesses-in-india-data-protection-bill accessed 18 March 2025.
[37] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art 35.
[38] Ibid, art 22.
[39] Government of Canada, *Artificial Intelligence and Data Act (AIDA)*, Bill C-27 (2022).
[40] Government of India, *Digital Personal Data Protection Act, 2023*, Gazette Notification No. 39 of 2023.
[41] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art 35.
[42] ECD, *Recommendation of the Council on Artificial Intelligence* (OECD Legal Instruments, 2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 accessed 18 March 2025.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 02/08/2024 Revised: 30/08/2024 Accepted: 04/09/2024 Published: 17/09/2024

Third, the establishment of an independent AI ethics body is proposed. This body should consist of experts in law, technology, ethics, and human rights, tasked with formulating ethical guidelines, reviewing high-risk AI deployments, and providing advisory inputs to regulators and policymakers.

Moreover, this paper recommends imposing limitations on government exemptions under Section 17 of the DPDP Act.[43] Excessive state discretion in AI-driven surveillance or data processing risks eroding public trust and violating privacy rights.
Lastly, the development of enhanced grievance redressal mechanisms, including the right to human intervention and appeal against algorithmic decisions, is essential to uphold procedural fairness and individual autonomy in the digital age.

9. Conclusion

The Digital Personal Data Protection Act, 2023 (DPDP Act**)** represents a significant milestone in India's evolving data protection landscape, aiming to provide a structured approach to safeguarding personal data while fostering the growth of the digital economy. It is a commendable legislative effort in response to the growing demand for individual privacy protection in the age of big data and artificial intelligence (AI)**.** However, the true impact of this legislation will depend not merely on its textual provisions, but on how it is interpreted by the judiciary**,** enforced by regulators**,** and adapted to emerging technological challenges. The tension between technological innovation and the fundamental right to privacy**,** recognized in *Justice K.S. Puttaswamy v. Union of India***,** continues to pose a constitutional dilemma. Although the Act introduces foundational concepts such as data fiduciaries**,** data principals**,** and lawful processing**,** it does not yet integrate AI-specific safeguards such as algorithmic transparency**,** impact assessments**, or** fairness audits**,** which are increasingly being seen as essential to ethical AI deployment. For the DPDP Act to realize its full potential, it must evolve in tandem with a comprehensive AI governance framework. This should include rights-based accountability mechanisms**,** independent oversight bodies, and robust grievance redress systems, drawing on global best practices like the EU's GDPR and Canada's AIDA. Moreover**,** judicial oversight will be vital to interpret ambiguous clauses, especially those granting broad state exemptions, to ensure they pass constitutional muster and do not undermine individual liberties.In essence, while the DPDP Act lays a legislative foundation, its effectiveness in balancing innovation and privacy will depend on dynamic policy reforms, technological foresight, and a commitment to constitutional values.

[43] EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art 35.