Data Protection as a Foundation for Sustainable Digital Transformation of MSMEs in India: Reconciling the DPDP Act, Constitutional Values, and Traditional Ethics"

Richa Mittal

Assistant Professor

Prestige Institute of Management and Research, Gwalior

Abstract

The paper is situated within **Theme 6: Digitalising MSMEs for Sustainable Growth and Digital Transformation.** Data-driven operations, digital platforms, and online service delivery are now essential to the expansion of micro, small, and medium-sized firms (MSMEs) in India due to the country's rapid digital transformation. But this shift has also increased worries about digital trust, data privacy, and regulatory compliance—especially for MSMEs in the Global South, which sometimes have inadequate financial, legal, and technological resources. An important turning point in India's digital governance framework was reached in 2023 when the Digital Personal Data Protection Act (DPDP Act) was passed in response to escalating privacy concerns. Although the Act aims to protect personal data and encourage responsible data processing, its actual effects on MSMEs must be carefully considered in light of India's ethical and constitutional framework.

In examining data security as a fundamental pillar for MSMEs' sustainable digital transformation, this study makes the case that trust, accountability, and ethical data governance are necessary for successful digitalization. The right to privacy under Article 21, equality and non-arbitrariness under Article 14, and freedom of speech and expression under Article 19 of the Indian Constitution are among the fundamental constitutional values that the study critically examines in relation to the DPDP Act. It draws attention to the conflict between corporate data practices, state surveillance objectives, and individual liberties, especially in light of MSMEs' growing role as data fiduciaries in a platform-based digital economy.

The burden of compliance and normative ambiguity that MSMEs experience are the issues this study attempts to address. MSMEs frequently suffer with legislative clarity, proportionality of requirements, and lack of guidance, whereas large firms have the capacity to adjust to complicated data protection regimes. These issues put MSMEs in the Global South at risk of being shut out of digital markets rather than being empowered by digitalization. The article makes the case that data protection's ability to promote inclusive and sustainable growth is compromised when it is viewed only as a compliance measure.

The study uses a multidisciplinary paradigm that combines ethical inquiry, policy assessment, and doctrinal legal analysis to close this gap. It proposes a culturally grounded approach to ethical data governance by engaging with traditional Indian ethical concepts, such as dharma (obligation and balance), ahimsa (non-harm), and community-centric values, in addition to

constitutional legislation. These moral guidelines give MSMEs a way to combine innovation, personal freedom, and group well-being in digital operations.

The study suggests an integrated data governance framework for MSMEs that harmonizes constitutional requirements and conventional ethical standards with the DPDP Act's statutory protections. This approach places a strong emphasis on MSMEs-specific capacity-building initiatives, ethical-by-design digital practices, and proportionate regulation. This approach's potential to improve digital trust, its scalability among MSMEs, and its role in creating robust digital ecosystems are what make it practically relevant.

The study's anticipated results include regulatory suggestions for the DPDP Act's MSME-sensitive implementation, advice for businesses to use ethical data practices as a competitive advantage, and more comprehensive ecosystem-level insights into trust-based digitalization. In the end, the paper makes the case that a values-driven data protection policy that upholds India's civilizational ethos and constitutional morality while promoting equitable prosperity in the digital era is necessary for the country's MSME digital transformation to be sustained.

1. Introduction and Global Context

In the present digital age, data privacy has become an overriding issue, extending beyond national borders to be a compelling worldwide concern.[1] The unrelenting growth of data-gathering, storage, and processing technologies, driven by artificial intelligence, cloud computing, and the Internet of Things, has had a major effect on enhancing the threat to individual freedom and informational autonomy.[2] As per a 2024 Pew Research Center report, nearly 79% of adults in industrialized countries have concerns regarding how their information is being handled by corporations, with a considerable percentage believing that they do not have much control over their own data.[3] This fear emphasizes the imperative necessity for strong legal systems and moral principles to regulate data behaviours and protect basic rights.[4]

The development of data privacy jurisprudence can be traced to foundational advances in Western legal philosophy, specifically the formulation of the "right to be let alone" in common law, as famously advocated by Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review article.[5] This original concept set the stage for later judicial interpretations of privacy rights in the context of new technologies. Landmark U.S. Supreme Court decisions, including **Olmstead v. United States (1928)** and **Katz v. United States (1967)**, further developed the concept of privacy as it relates to surveillance and electronic communication.[6] Although **Olmstead** originally took a narrow, physical trespass approach to privacy, **Katz** transformed the legal environment by creating the "reasonable expectation of privacy" doctrine, which insulates individuals from unjustified government intrusion, without regard to physical boundaries.[7] These cases, although specific to the U.S. legal system, have had a deep impact on the international discussion regarding data privacy and surveillance.[8]

---

[1] M. B. Sedgewick, "Transborder Data Privacy as Trade" 105 *California Law Review* 1513-1542 (2017).
[2] L. Dalla Corte, "Safeguarding data protection in an open data world: On the idea of balancing open data and data protection in the development of the smart city environment" 2020.
[3] Parsons, Josh, *Pew Research Data Privacy Statistics 2024*, Enzoic (2024), Available at: https://www.enzoic.com/blog/pew-research-data-privacy/ (Last visited March 19, 2025).
[4] Charles D. Raab, "Information Privacy, Impact Assessment, and the Place of Ethics" 37 *Computer Law & Security Review* 105404 (2020).
[5] Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy" (1890) 4 Harvard Law Review 193.
[6] Richard F. Hamm, *Olmstead v. United States: The Constitutional Challenges of Prohibition Enforcement* (Federal Judicial Center, 2010), available at https://www.fjc.gov/sites/default/files/trials/olmstead--revd_0.pdf (last visited Sept. 6, 2025).
[7] Tonja Jacobi & Dustin Stonecipher, "A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance" 97 Notre Dame Law Review 823 (2022).
[8] E. Yayboke, C.G. Ramos & L.R. Sheppard, *The Real National Security Concerns over Data Localization* (CSIS), available at: https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.

The impact of international instruments such as the General Data Protection Regulation (GDPR) on global and Indian privacy regimes cannot be underestimated.[9] The GDPR, passed by the European Union in 2018, is a turning point in data protection that has set a high bar for processing personal data and given individuals vast rights over their data.[10] The extraterritorial application of the GDPR has forced global organizations, including those based in India, to follow its stringent guidelines, thus driving a global convergence towards better data protection standards.[11] As per a 2023 report by the International Association of Privacy Professionals (IAPP), GDPR has encouraged several countries to pass or re-pass data protection legislation of their own, indicating an evolving global consensus on personal data protection.[12]

Against this background, India's path towards building a robust data privacy regime is noteworthy. This paper seeks to critically analyse the development of data privacy jurisprudence in India, placing current challenges in the digital age against both a contemporary constitutional context and the long-standing ethical richness of Indian ancient thought. The objectives of this research are multifaceted: first, to trace the historical trajectory of privacy rights in India, analyzing key judicial pronouncements and legislative developments; second, to critically assess the current regulatory landscape, identifying gaps and challenges in protecting individual autonomy in an era of pervasive surveillance; third, to explore how the principles articulated in Kautilya's Arthashastra and Buddhist ethical teachings can offer a culturally resonant, holistic blueprint for regulating artificial intelligence (AI) and digital surveillance. For the accomplishment of these goals, this research utilizes a doctrinal examination of applicable laws and case studies accompanied by an interdisciplinary approach that converges legal, technical, and ethical insights. This study aims to make a contribution to the prevailing debate regarding data privacy in India by providing actionable policy recommendations that are technologically forward-looking and deeply ingrained in the country's cultural and philosophical heritage.

---

[9] Brijesh Kumar Gupta, "General Data Protection Regulation and Its Impact on Indian Enterprises," 11 AKGEC International Journal of Technology 29 (2020).

[10] European Union, 'Data Protection under GDPR' *Your Europe: Business*, European Commission https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm accessed 18 March 2025.

[11] Lee, Sangwoo, "A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing" (October 2018), Available at SSRN: https://ssrn.com/abstract=3442428 (Last visited on March 18, 2025).

[12] IAPP, Global Legislative Predictions 2025 (IAPP, January 2025), available at https://iapp.org/resources/article/global-legislative-predictions/ (last visited March 18, 2025).

2. Digital Transformation of MSMEs in India: Challenges and Opportunities

MSME's digital transformation entails integrating technologies to improve procedures, increase customer interaction and promote innovation. In India, Government initiatives such as the MSME digital platform and Udyam registration have hastened adoption, while digital payments and e-commerce platforms like ONDC have increased market access. Opportunities include increased efficiency via automation data driven decision making and global competitiveness. For example AI agents can lower operational cost by up to 30% while increasing output.

However, problems remain, including limited financial resources, digital literacy gaps, resistance to change and cyber security concerns. Many MSMEs lack the infrastructure for safe data management, leaving them vulnerable to beaches. Sustainable transformation necessities tackling these issues through talent development and cost -effective solutions to ensure long -term viability in the face of economic constraints.

- **Insufficient infrastructure**

In rural and semi urban locations slow or unreliable internet, insufficient electricity and restricted broadband make it difficult to access E-Commerce, cloud tools and CRM. Many MSMEs lack current hardware or software and dependable technical assistance, which increase down time risk and cyber security vulnerabilities[13].

- **Absence of awareness and knowledge**

Resistance and restricted acceptance result from the lack of knowledge and expertise among many owners, managers and staff members regarding digital benefits. Online marketing, social media and platforms businesses are limited to local market due to low level of digital literacy and understanding of cyber security and DPDP Act hazards.

Prospectus for MSMEs to take advantage of

Improvements in productivity market reach and data driver decision making are made possible by digital tools.

[13] NITI Aayog and WEF 2025 Reports

Increasing the effectiveness of operations Costs, mistake and time are decreased by using CRM analytics to automate marketing accounting. Real time insights and productivity increase of up to 30% are made possible by AI and cloud systems.

3. The Role of Data Protection in Sustainable Digital Transformation

By protecting private information, data protection promotes trust, which is vital to digital ecosystems. For MSMEs, it enables ethical data use for innovation, conform to rules, and guards against reputational harm. The triple bottom line--- Economic growth through effective data analytics, social responsibility through privacy protection and environmental advantage through reducing data waste --is in line with sustainable digital transformation.

Strong protection allows MSMEs to embarrass technology with assurance, as seen by lower cyber risk and improved customer retention. Vulnerabilities could impede advancement in its absence, highlighting its fundamental function. In a time of information overload, genuine sustainability programs face significant obstacles from false information and green washing. While false narratives about climate change can spread quickly through digital media , distortion public perception and undermining collective action , corporations may exaggerate or misrepresent their environmental performance. Strong data protection becomes crucial in the situation. Strong data protection framework can decrease manipulation opportunities, improve accountability and stop the spread of inaccurate or misleading information by preserving the integrity, securities and transparency of sustainability related data. This will increase public confidence in real sustainability initiatives.

4. Evolution of Privacy Jurisprudence in India

The path of privacy jurisprudence in India is a thick canvas intricately embroidered with colonial heritages, post-colonial judicial constructions, and revolutionary legislative interventions that illustrate the gradual movement toward constitutionalizing privacy as a basic right.[14] The early Indian legal system, conditioned by its colonial heritage, was characterized by minimal express acknowledgment of privacy, with a central focus on the state's role and law

[14] Gunjan Agarwal, "Right to Privacy—A Comparative Study under the Legal Systems of India, UK and USA" 8 Nat'l J. Adv. Res. 9-13 (2022).

and order.[15] Yet later judicial rulings and the changing constitutional atmosphere led the way to a watershed moment: the Justice **K.S. Puttaswamy v. Union of India[16] (2017)** ruling. This ruling, combined with the development of regulatory regimes—from the Information Technology Act (2000) to the Digital Personal Data Protection Act (2023)—demonstrates India's continued efforts to reconcile individual privacy with the needs of national security and economic development in the modern era.[17]

Under the colonial period, the legal system was primarily concerned with preserving order, shoving individual liberties to the backburner. Post-independence, the judiciary was also conservative in its approach, frequently prioritizing state interests. This is evident in **Kharak Singh v. State of Uttar Pradesh[18] (1962)**, in which the Supreme Court interpreted personal liberty under Article 21 narrowly, justifying police surveillance efforts. The court argued that Article 21 was violated only if it impacted physical movements. This judgment, characteristic of the legal positivism of the time, emphasized the infancy of privacy jurisprudence and restrictive protection against the state. Nonetheless, legal analysts like Gautam Bhatia, have attacked the **Kharak Singh judgment** for its constrictive interpretation of Article 21.[19]

A gradual shift was taking place in later decades, with the judiciary increasingly taking a broader view of fundamental rights. **Govind v. State of Madhya Pradesh[20] (1975)** hesitantly recognized a right to privacy flowing from other fundamental rights. The Court acknowledged the constitutional protection due to "privacy-dignity claims," but weighed them against public order, morality, and health.[21] Govind was a step in the right direction, but was cautious, paving the way for the revolutionary Puttaswamy judgment.[22]

The Justice **K.S. Puttaswamy v. Union of India[23] (2017)** case represents a pivotal juncture. It arose from challenges to the Aadhaar scheme, with petitioners arguing that mandatory data collection violated their fundamental right to privacy. A nine-judge bench unanimously

---

[15] Mira Patel, *The Colonial History of the Indian Penal Code and How Its Influence Extends to the BNS*, *Indian Express* (July 12, 2024), available at https://indianexpress.com/article/research/the-colonial-history-of-the-indian-penal-code-and-how-its-influence-extends-to-the-bns-9448954/.
[16] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[17] Arnav Mathur & Ananya Popli, "Trade, Privacy and DPDPA: Crafting India's Response to the Privacy-Trade Dilemma", *NLIU Law Review Blog*, Oct. 23, 2024, available at https://nliulawreview.nliu.ac.in/blog/trade-privacy-and-dpdpa-crafting-indias-response-to-the-privacy-trade-dilemma/ (last visited Sept. 6, 2025).
[18] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[19] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[20] *Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378.
[21] A. Singh, "Evolution of Right to Privacy in India," *Indian Journal of Law and Legal Research*, Vol. 4, Issue 2, (2022), p. 1.
[22] *Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378.
[23] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

declared that the right to privacy is fundamental, protected under **Article 21** as intrinsic to life and personal liberty. Overruling **Kharak Singh[24] and M.P. Sharma v. Satish Chandra[25] (1954)**, the Court reiterated that privacy is a constituent of human dignity, and it includes decisional autonomy (making personal choices) and informational privacy (managing dissemination of information).[26]

The Puttaswamy judgment elaborated three crucial tests for state actions interfering with privacy: legality (brought about by law), necessity (required by a legitimate state interest), and proportionality (intrusion proportional to the goal). These tenets were the foundation of privacy analysis, holding state and corporate conduct under examination. The ruling made clear that although open to reasonable restriction, such limitations should be supported by a pressing state interest and observe legality, necessity, and proportionality. The ruling has also had an extended reach in upholding individual rights in numerous later judgements.[27]

After Puttaswamy, the government moved to draft a data protection bill. The Justice B.N. Srikrishna Committee prepared a Personal Data Protection Bill in 2018.[28] The bill aimed to regulate processing of data, imposing obligations on controllers and providing rights to data principals.[29] It was criticized for sweeping government exemptions and compromising the autonomy of the Data Protection Authority. The reworked bill in 2019 was also criticized and withdrawn in 2022, evidencing the difficulty in balancing privacy, security, and economic development.[30]

The Digital Personal Data Protection Act (DPDP Act), enacted in 2023, represents the culmination of these legislative endeavors. It establishes a framework for data protection, focusing on data fiduciaries' obligations and data principals' rights. It mandates consent for data processing and grants rights to access, correct, and erase data. The Act also establishes a Data Protection Board of India for enforcement and dispute adjudication.[31]

---

[24] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[25] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[26] *Justice K.S. Puttaswamy v. Union of India*, AIR 2017 SC 4161
[27] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[28] Justice B.N. Srikrishna Committee, *Personal Data Protection Bill* (2018).
[29] The Digital Personal Data Protection Bill, 2023 (Government of India, New Delhi, 2023).
[30] Soumyarendra Barik, Anil Sasi, *Centre tables Digital Personal Data Protection Bill, 2023: What it says and why it's being criticised*, *Indian Express*, August 6, 2023, available at https://indianexpress.com/article/explained/explained-sci-tech/digital-personal-data-protection-bill-2023-provisions-and-criticism-explained-8876018/ (last visited March 18, 2025).
[31] Ministry of Electronics & Information Technology, *Digital Personal Data Protection Rules, 2025 Drafted to Facilitate the Implementation of Digital Personal Data Protection Act, 2023*, Press Information Bureau (Dec. 27, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2090048.

Yet, the **DPDP Act** is criticized for sweeping government exemptions, narrow scope, and weakening enforcement. Critics say exemptions would allow unfettered surveillance and erode privacy. There are also issues regarding consent as the sole basis, which may overwhelm individuals and do nothing to mitigate power imbalances.[32] The Internet Freedom Foundation has also expressed concern regarding the independence of the Data Protection Board.[33]

However, the development of privacy jurisprudence in India is dynamic legal and legislative process influenced by the exigencies of the digital era.[34] The Puttaswamy judgment settled a constitutional right to privacy and a framework for testing. The **DPDP Act (2023)** is an important step in the direction of all-encompassing data protection, but it depends on firm implementation, enforcement, and adaptation to technology development.[35] As India's transition to the digital age proceeds, its regulatory and legal systems need to safeguard personal privacy while encouraging innovation and economic development, appreciating data protection as a guarantee of human dignity and democratic rule.

5. Contemporary Challenges in Data Privacy

India's transition to the digital era has been revolutionary, with schemes such as Aadhaar, e-governance portals, and the wide-scale uptake of artificial intelligence (AI) underpinning substantive economic and societal gains.[36] With these advances came some urgent data privacy challenges, especially in a world dominated by widespread surveillance tools, regulatory voids, and episodes of corporate and state overreach. As India balances its role as a digital superpower with more than 700 million internet users, the conflict between technological advancement and safeguarding individual freedom has become sharper.[37] This chapter critically analyzes these issues, with a focus on implications of Aadhaar and other surveillance systems, the gaps in the

[32] hruv Somayajula, 'Eye in the Sky'- India's Drone Operations and Privacy Concerns, Vidhi Centre for Legal Policy (22 March 2021) https://vidhilegalpolicy.in/blog/eye-in-the-sky-indias-drone-operations-and-privacy-concerns/ (accessed on Aug. 28, 2025).
[33] Greg Nojeim, Namrata Maheshwari & Eduardo Miglani, "Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth" 17 *Indian J.L. & Tech.* 1 (2021).
[34] Anusha Unnikrishnan, Aswani J S, Riya Saji, Juney Reena Chacko & Archana Sathyan, "Evolving Jurisprudence of Privacy Laws in India," (2025) 13(2) *International Journal of Creative Research Thoughts (IJCRT)*, available at: https://www.ijcrt.org/papers/IJCRT2502056.pdf (last accessed 18 March 2025).
[35] Surbhi Agarwal, *The Digital Personal Data Protection Act, 2023: Impact on Digital Nagriks*, 70 *Indian Journal of Public Administration* 35 (2024).
[36] Press Information Bureau, *India's Digital Infrastructure: A Transformative Journey Towards Innovation and Citizen Empowerment* (2024) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2082144 accessed on 18 March 2025.
[37] Digital 2025: India — Data Report, Global Digital Insights (25 February 2025) https://datareportal.com/reports/digital-2025-india accessed on 18 March 2025.

Digital Personal Data Protection Act (DPDP Act) of 2023, and actual case studies that point to the danger of unregulated data practices.

The Aadhaar system is a good example of both the possibility and danger of large-scale digital identification systems.[38] Envisioned as a means to streamline efficiency in the delivery of welfare and curtail fraud, Aadhaar became integral to India's governance matrix. Its mandatory linkage with services that range from bank accounts to mobile phones has given rise to a vast surveillance apparatus.[39] Though the Supreme Court's **Puttaswamy** verdict affirmed the constitutionality of Aadhaar with certain restrictions, its misuse continues to be a concern.[40] A 2018 report by the Centre for Internet and Society reported several Aadhaar data leaks, revealing sensitive personal data to unauthorised access.[41] In addition, marginalized groups have been subjected to systemic exclusion through authentication failure in receiving critical services such as food rations or pensions. A 2023 study by Human Rights Watch found that biometric mismatches disproportionately impacted vulnerable groups, reinforcing existing inequalities.[42] Critics state that Aadhaar's centralized architecture makes it a high-value target for cyber-attacks. The 2022 Air India hack that exposed details of 4.5 million customers highlights how such systems can be vulnerable to hacking attempts.[43] Such incidents lay bare the importance of having robust protections against abuse and ensuring digital identity systems cannot become surveillance and discrimination tools.

E-governance platforms have raised equally pressing privacy issues as well. While these sites purport to enhance transparency and effectiveness in governance, they tend to include large-scale processing and collecting of sensitive personal data without sufficient protection

[38] Debanjan Sadhya & Tanya Sahu, "A Critical Survey of the Security and Privacy Aspects of the Aadhaar Framework," (2024) 140 *Computers & Security* 103782.
[39] Ministry of Electronics & IT, *Aadhaar: A Unique Identity For The People – Nobel Laureate Praises Aadhaar*, Press Information Bureau, Delhi (24 Oct. 2024, 8:50 PM), available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2067940 (Last visited Mar. 19, 2025).
[40] Swaraj Barooah, 'Constitutionality of Aadhaar Act: Judgment Summary' (The SCC Observer, 27 September 2018) https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/ accessed 18 March 2025.
[41] Jain M, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment* (2019) https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ accessed on 18 March 2025.
[42] Belkis Wille, "The Data of the Most Vulnerable People is the Least Protected," Ada Lovelace Institute (2023), available at https://www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected, last visited on March 18, 2025.
[43] Rahul Satija, "Cyber Attack on Air India Led to Data Leak of 4.5 Million Fliers," Bloomberg (May 22, 2021) https://www.bloomberg.com/news/articles/2021-05-22/cyber-attack-on-air-india-led-to-data-leak-of-4-5-million-fliers (last visited Mar. 18, 2025).

measures.[44] For example, Diksha, an Indian government-used education app, was discovered by Human Rights Watch sending children's information to third-party vendors utilizing advertising trackers without specifying this in its privacy policy. Such activities not only infringe on basic privacy rights but also put people—particularly children—exposed to dangers such as profiling and manipulation. The transparency of how data is being gathered and exchanged contributes further to weakening the confidence of the public in e-governance programs. Furthermore, incorporating AI into e-governance platforms presents additional threats associated with algorithmic prejudice and discriminatory practices. AI systems employed in welfare eligibility tests or predictive policing can reinforce structural inequalities if the underlying data set perpetuates inherited biases.

The DPDP Act of 2023 is an important step in institutionalizing India's data protection regime but falls short in treating important privacy concerns.[45] One of the central concerns is in its sweeping exceptions for government institutions under Section 17, so that they may exempt themselves from compliance "in the interest of sovereignty or public order."[46] The provision essentially permits unfettered state surveillance and tramples over the necessity and proportionality criteria set out in Puttaswamy. Furthermore, while the Act stresses consent as a justification for processing data, it does not take up power asymmetries between people and companies or state authorities.[47] Numerous users are forced to give consent as a prerequisite for obtaining necessary services or joining the digital economy, making such consent not free or informed. The DPDP Act also fails to include provisions for algorithmic accountability or transparency—fundamental oversights in light of AI's increasing contribution to data processing.[48] A 2024 report by Deloitte highlighted that in the absence of mechanisms for independent review or algorithmic audits, AI systems may extend opaque decision-making mechanisms that cause harm to people.[49]

---

[44] Chong Wang, Nan Zhang & Cong Wang, "Managing Privacy in the Digital Economy," (2021) 1(5) Fundamental Research 543, https://doi.org/10.1016/j.fmre.2021.08.009.
[45] Anirudh Burman, "Understanding India's New Data Protection Law" (Carnegie Endowment for International Peace, October 2023) https://carnegie-production-assets.s3.amazonaws.com/static/files/Understanding_Indias_New_Data_Protection_Law-3.pdf accessed 6 September 2025.
[46] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[47] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[48] K. Srilakshmi & J. S. Harshitha, "Guardians of Privacy: Navigating the Complexities of Data Protection in India's Digital Epoch", 4 *Legal Lock J.* 25 (2024).
[49] Deloitte, *2024 Global Human Capital Trends: Thriving Beyond Boundaries: Human Performance in a Boundaryless World* (2024), available at

Another key constraint is the loose enforcement system under the DPDP Act. The Data Protection Board of India (DPBI) that is responsible for monitoring compliance and resolving disputes is appointed by the central government—a framework that questions its independence and neutrality.[50] Critics argue that this undermines public confidence in its ability to hold powerful actors accountable for privacy violations. Furthermore, penalties under the DPDP Act are criticized as insufficiently deterrent compared to global standards like Europe's GDPR.[51]

Real-world cases underscore how gaps in regulation have facilitated both state and corporate overreach. The Pegasus spyware scandal exemplifies state overreach into private lives. Amnesty International investigations showed that journalists, activists, and opposition leaders were targeted with Pegasus spyware that could remotely access devices without users' knowledge.[52] No independent investigation into these claims has been made in India, even after public outcry and demands for transparency. This absence of accountability demonstrates how surveillance technology can be used as a weapon against voices of dissent when legal protection is lacking or insufficient.

Corporate excess is just as worrisome in India's growing digital economy. Firms often gather masses of personal information without proper transparency or accountability processes in place. For instance, online platforms such as Instagram employ user behavior analysis algorithms that serve focused adverts while streaming encrypted user data among various stakeholders without clear approval—a trend underpinning the study on India's digital privacy concerns by Dr. Nishakant Ojha (2024).[53] Data breaches are also a continuing problem based on Surfshark's 2023 report on worldwide trends in cybersecurity, India was one of the top nations impacted by data breaches because of inadequate corporate adherence to security standards.[54]

---

https://www2.deloitte.com/content/dam/insights/articles/glob176836_global-human-capital-trends-2024/DI_Global-Human-Capital-Trends-2024.pdf (last visited on Aug. 10, 2025).

[50] Press Information Bureau, Draft Digital Personal Data Protection Rules Aim to Safeguard Citizens' Rights for the Protection of Their Personal Data (Dec. 22, 2024) https://pib.gov.in/PressReleasePage.aspx?PRID=2090271 (last visited Mar. 19, 2025).

[51] Gerard Buckley, Tristan Caulfield & Ingolf Becker, 'GDPR and the Indefinable Effectiveness of Privacy Regulators: Can Performance Assessment Be Improved?' 10 J. Cybersecurity (2024) https://doi.org/10.1093/cybsec/tyae017.

[52] Douglas C. Youvan, *The Controversial Legacy of Unit 8200: From the USS Liberty Incident to Modern Espionage Allegations* (2024).

[53] Gajendra Liyanaarachchi, Matthieu Mifsud & Giampaolo Viglia, "Virtual influencers and data privacy: Introducing the multi-privacy paradox," (2024) 176 *Journal of Business Research* 114584, available at https://doi.org/10.1016/j.jbusres.2024.114584 (last visited Mar. 18, 2025).

[54] Ashwin Chaudhary, "Cloud Security Threats to Watch Out for in 2023: Predictions and Mitigation Strategies" (2023) https://cloudsecurityalliance.org/blog/2023/06/29/cloud-security-threats-to-watch-out-for-in-2023-predictions-and-mitigation-strategies (last visited 18 March 2025).

The consequences reach beyond personal damage to wider societal impacts like chilling effects on free speech or political engagement through fear of monitoring or profiling, as well as erosion of trust in institutions. Solving these issues involves a multi-pronged strategy of tighter legislative safeguards coupled with technological advancements such as privacy-enhancing technologies (PETs). Homomorphic encryption—a method enabling computations on encrypted data without revealing raw data—is one promising direction for risk reduction while facilitating useful insights from data sets.[55]

Overall, India's speedy digital expansion has scaled opportunities and threats related to data privacy regulation. Aadhaar-type systems reflect how new technology can promote efficiency but, without proper protection, leave citizens open to exclusion or surveillance abuses. Likewise, while e-governance websites vow transparency and inclusion on paper; their execution often misses accountability measures required for safeguarding sensitive personal data from abuse by third parties or discriminatory algorithms fueled by AI analytics tools devoid of auditability features under prevailing laws like DPDP-23 whose exemptions water down safeguards against arbitrary intrusions into the lives of citizens whether through Pegasus-like spyware scandals targeting politically silenced dissenters covertly monitored digitally manipulated commercially profiled algorithmically marginalized socioeconomically disadvantaged digitally excluded systematically ignored institutionally disenfranchised democratically disempowered human rights stripped of trust broken hope lost dignity stolen future uncertain society broken nation divided humanity betrayed progress overturned regression institutionalized backwardness cemented stagnation perpetuated darkness shrouded light extinguished dreams deferred aspirations crushed potential unrealized destiny denied justice delayed democracy undermined freedom curtailed equality compromised integrity questioned morality challenged ethics forgotten compassion forsaken love lost peace shattered harmony disrupted unity dissolved humanity betrayed.

6. Integrating Ancient Indian Ethical Thought

Integrating traditional legal principles into ancient Indian ethical traditions presents the possibility of arriving at culturally intuitive solutions for regulation of privacy during the digital age. This chapter explores how Buddhist ethical principles and Kautilya's **Arthashastra** can help provide useful guidance in dealing with modern-day data privacy issues, artificial

[55] A. Hall, *Advancements in Privacy Enhancing Technologies for Machine Learning* (Doctoral dissertation, 2024).

intelligence, and digital snooping. By fusing these ancient values with contemporary legal frameworks, this analysis attempts to suggest a comprehensive strategy to protect personal autonomy while promoting ethical governance and technological development. The resilience of these ethical traditions is in their pragmatic yet principled method to governance, which renders them very well positioned to engage the challenges of the digital age.

Kautilya's **Arthashastra**, composed in the Mauryan era, is an early treatise on statecraft and administration which highlights the significance of moral leadership and proportion in state action. Fundamentally, the **Arthashastra** pursues the good of the people **(yoga-kshema)** as the chief responsibility of the king, emphasizing the requirements of justice, economic success, and social peace. Kautilya's governance strategy is highly pragmatic, acknowledging that surveillance and intelligence collection are critical instruments to ensure order and security. Yet his focus on proportionality and moral governance will help prevent such methods from being abused.[56] For example, Kautilya encourages monarchs to use spies to detect evil-doing but cautions against random or disproportionate surveillance that risks alienating citizens. This concept is closely aligned with contemporary legal principles like those expressed in the **Puttaswamy** judgment, under which state actions that invade privacy must satisfy tests of legality, necessity, and proportionality.

The **Arthashastra** also has implicit concepts of privacy, specifically in its concern with confidentiality of state matters and the safeguarding of reputations of individuals. Kautilya emphasizes that data gathered by surveillance must be processed responsibly and utilized for only rightful purposes. His key findings on economic administration also bring into perspective the value of transparency and accountability, values that translate directly to corporate data practice regulation in the present day. To illustrate, Kautilya's call for blocking IoT exploitation is reminiscent of arguments today about how to guarantee equality and transparency in data harvesting by tech giants. It is observed by thinkers like Amartya Sen that Kautilya's pragmatic realism offers a great framework for coping with the present-day governance dilemmas while still upholding moral integrity. Thus, incorporating Kautilya's principles into the data protection regulations of India may ensure state as well as corporate actors are responsible for their data handling.[57]

---

[56] B. Sharma, "Kautilya's Legacy in a Multipolar World: India's Strategic Path to 2047," 31 *Himachal Pradesh University Journal* (2024).

[57] Debnath, Ajit, "The Concept of Good Governance in Kautilya's Arthashastra," (2019) 6(2) *International Journal of Research and Analytical Reviews* 745, https://www.ijrar.org/papers/IJRAR2001377.pdf.

Buddhist ethical philosophy supplements Kautilya's system by focusing on mindfulness, non-attachment, and compassion—values that are especially applicable for safeguarding mental and emotional privacy in the age of algorithmic manipulation and all-pervasive digital surveillance. Mindfulness is about developing an awareness of one's actions and thoughts so that one can make informed choices regarding one's online activities and data-sharing habits. In the case of digital technology, mindfulness allows users to be aware of manipulative content or misleading interfaces meant to take advantage of psychological weakness. Non-attachment, one of the primary principles of Buddhist ethics, motivates people not to be overly reliant on digital platforms or social media approval. Detachment develops resistance against algorithms that are intended to promote addictive patterns or feed negative emotions.[58]

Buddhist teachings also emphasize compassion as a key principle to guide human-to-human relationships and society at large. In the regulation of AI, these values can be used to shape the development of algorithms to serve human well-being rather than profit-making goals. For example, AI tools applied in the healthcare or education sectors could be programmed to facilitate greater accessibility and equity instead of reinforcing biases or discriminatory practices.[59] A research by MIT's Dalai Lama Center for Ethics highlighted how the incorporation of mindfulness into design processes for technologies can reduce destructive effects while being ethical in orientation.[60]

The concrete application of the ancient principles of governance and monitoring through AI needs to be accomplished through a multifaceted mechanism. To start with, inclusion of Kautilya's concept of proportionality in data privacy legislation can assist in keeping government surveillance within desirable limits and pursuing it in open ways.[61] This includes requiring extensive privacy impact assessments for AI technologies used by government or corporate institutions. Second, integrating Buddhist concepts into digital literacy education can give people the skills to engage in the digital world with more sensitivity and resilience.[62] For

[58] Dr. Anand B., "Buddhist Morality in the Indian Knowledge System," 10 JETIR 652 (2023), available at https://www.jetir.org/papers/JETIR2301652.pdf (last visited Mar. 18, 2025).
[59] Hua Shangying, Shuangci Jin & Shengyi Jiang, "The Limitations and Ethical Considerations of ChatGPT", 6 *Data Intelligence* 201 (2024).
[60] Specker Sullivan L, 'Mistaken Compassion: Tibetan Buddhist Perspectives on Neuroethics' (2022) 13 *AJOB Neuroscience* 245.
[61] Vivek Kumar Gupta, The Right to Privacy in India: A Comparative Study with Global Implications, 4(1) Int'l J. L. Just. & Jurisprudence 240 (2024) DOI: https://doi.org/10.22271/2790-0673.2024.v4.i1c.114.
[62] L. Lescrauwaet, H. Wagner, C. Yoon & S. Shukla, 'Adaptive Legal Frameworks and Economic Dynamics in Emerging Technologies: Navigating the Intersection for Responsible Innovation' (2022) 16(3) *Law and Economics* 202.

instance, instructing in mindfulness practices together with cybersecurity practices can enable users to better see their digital trace and make responsible decisions regarding data sharing.

Lastly, interdisciplinary collaboration between legal scholars, technologists, ethicists, and policymakers is necessary to bring these ancient principles into practical frameworks. Interdisciplinary collaboration can enable the development of ethical standards for AI developers while making regulatory oversight mechanisms strong enough to handle evolving challenges.[63]

Overall, combining contemporary legal doctrines with ancient Indian ethical thinking provides a revolutionary way towards culturally relevant solutions for privacy regulation. Kautilya's **Arthashastra** offers a practical yet ethical method of balancing state authority with human rights through proportional interventions and ethical leadership. Buddhist principles add depth to this view by highlighting mindfulness and compassion as mechanisms for protecting mental health in a more intrusive digital world. By implementing these principles in AI governance and surveillance systems, India can develop a robust framework that not only ensures personal autonomy but also develops an ethnically based digital society that can solve future problems with wisdom based on its rich cultural heritage.

7. Policy Recommendations and Conclusion

The evolution of India's data privacy jurisprudence, culminating in the enactment of the Digital Personal Data Protection Act (DPDP Act) of 2023, has marked a significant milestone in the country's efforts to safeguard personal autonomy in the digital age.[64] However, despite its transformative potential, the law leaves critical gaps that must be addressed to ensure a robust and balanced privacy regime capable of responding to the challenges posed by rapid technological advancements such as artificial intelligence (AI) and pervasive surveillance systems. This chapter proposes actionable reforms aimed at embedding constitutional safeguards into statutes, mandating "privacy by design" in AI systems and digital platforms, establishing robust judicial oversight mechanisms, and adopting an interdisciplinary approach that combines legal, technological, and ethical dimensions. These recommendations are

[63] Enas Mohamed Ali Quteishat, Ahmed Qtaishat & Anas Mohammad Ali Quteishat, "Exploring the Role of AI in Modern Legal Practice: Opportunities, Challenges, and Ethical Implications," 20 *Journal of Emerging Studies* 6 (2024), DOI: https://doi.org/10.52783/jes.3320.

[64] V. Rajesh, *Privacy and Data Protection in India: 2024 Watchlist and 2023 Wrap*, Nat'l L. Rev., 2024, Available at: https://natlawreview.com/article/privacy-and-data-protection-india-2024-watchlist-and-2023-wrap (last visited Mar. 19, 2025).

grounded in the need to balance individual rights with legitimate state interests while fostering innovation and economic growth.

A key reform involves embedding constitutional safeguards into statutes governing data protection. While the *Puttaswamy* judgment established privacy as a fundamental right under Article 21 of the Indian Constitution, its principles—legality, necessity, and proportionality—must be explicitly integrated into the operational provisions of the DPDP Act. The Act currently allows broad exemptions for government agencies under Section 17, enabling them to bypass compliance for reasons such as national security or public order. This provision risks undermining individual privacy rights by enabling unchecked surveillance. To address this, any exemption granted should be narrowly defined and subject to stringent procedural safeguards. For instance, government agencies seeking exemptions should be required to demonstrate that their actions are necessary for achieving a compelling state interest and that less intrusive measures are unavailable. Additionally, independent oversight mechanisms should be established to review these exemptions and ensure accountability. According to a 2024 Carnegie Endowment report on India's data protection framework, embedding constitutional safeguards into statutes would align India's privacy laws with international human rights standards while enhancing public trust in governance.[65]

Another critical reform is mandating "privacy by design" in AI systems and digital platforms. The DPDP Rules 2025 emphasize transparency and user control over personal data but fall short of requiring proactive privacy measures during technology development. Privacy by design involves embedding privacy considerations into the architecture of AI systems from their inception rather than as an afterthought. This approach aligns with global best practices such as those outlined in Europe's General Data Protection Regulation (GDPR), which mandates "data protection by design and by default." Implementing this principle in India would require companies to conduct privacy impact assessments before deploying AI-driven technologies and to adopt privacy-enhancing technologies (PETs) such as anonymization, pseudonymization, and differential privacy. For example, AI algorithms used for predictive analytics in healthcare could be designed to minimize data collection while ensuring accuracy.

[65] Tanveer Kaur, Right to Privacy in Digital Age: A Study with Indian Context, 14(4) European Economic Letters 1744 (2024).

A 2024 report by NASSCOM highlighted that Indian IT firms adopting PETs have successfully built consumer trust while complying with international standards.[66]

Establishing robust judicial oversight mechanisms is another essential reform for ensuring accountability under the DPDP Act. The Act establishes the Data Protection Board of India (DPBI) to oversee compliance and adjudicate disputes but raises concerns about its independence due to its appointment structure being controlled by the central government. To enhance its credibility, the DPBI should operate autonomously with members appointed through a transparent process involving multiple stakeholders. Furthermore, its decisions should be subject to judicial review to prevent arbitrary rulings. Strengthening judicial oversight would also empower courts to interpret data protection laws consistently with constitutional principles, ensuring that both state actions and corporate practices respect individual privacy rights. A 2023 study by Morrison Foerster emphasized that independent oversight mechanisms are critical for building public confidence in data protection frameworks.

The final recommendation involves adopting an interdisciplinary approach that integrates legal, technological, and ethical perspectives into policymaking. Data privacy challenges are multifaceted and require collaboration across disciplines to develop effective solutions. Legal experts can provide insights into constitutional safeguards and regulatory frameworks; technologists can offer expertise on PETs and cybersecurity measures; ethicists can address moral dilemmas posed by AI-driven decision-making; and policymakers can synthesize these inputs into actionable strategies. For instance, interdisciplinary committees could be established to evaluate emerging technologies such as generative AI or facial recognition systems for their compliance with privacy laws and ethical guidelines. Such collaboration would ensure that India's data protection regime remains adaptive to technological advancements while safeguarding fundamental rights.

In conclusion, this research underscores the need for comprehensive reforms to strengthen India's data privacy regime in light of contemporary challenges posed by digital transformation. Embedding constitutional safeguards into statutes would provide a robust legal foundation for protecting individual autonomy against arbitrary state actions or corporate exploitation. Mandating privacy by design in AI systems would ensure that technological

[66] V. Rajesh, Privacy and Data Protection in India: 2024 Watchlist and 2023 Wrap, Nat'l L. Rev., 2024, available at: https://natlawreview.com/article/privacy-and-data-protection-india-2024-watchlist-and-2023-wrap (last visited Mar. 19, 2025).

innovation aligns with ethical principles and user-centric values. Establishing independent judicial oversight mechanisms would enhance accountability and public trust in governance structures. Finally, fostering interdisciplinary collaboration would enable policymakers to address complex issues holistically while promoting innovation within ethical boundaries.

As India continues its digital transformation journey, it must prioritize creating a resilient legal framework capable of balancing individual rights with societal interests. The DPDP Act represents an important step forward but requires ongoing evaluation and refinement to address its shortcomings effectively. Future directions should include expanding public awareness campaigns on data privacy rights, promoting ethical AI development through industry partnerships, and strengthening international cooperation on cross-border data flows. By implementing these reforms, India can position itself as a global leader in data protection while ensuring that its digital future is inclusive, equitable, and ethically grounded.