INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 2 | 2026 Art. 14

Evaluating India's Digital Personal Data Protection Act, 2023: Privacy Rights, State Surveillance and Regulatory Challenges

Poulomi Banerjee
Law Student, B.A.LL.B. (Hons.),
Amity Law School, Amity University, Lucknow

Dr. Srijan Mishra
Assistant Professor,
Amity Law School, Amity University, Lucknow

Recommended Citation
Poulomi Banerjee and Dr. Srijan Mishra, *Evaluating India's Digital Personal Data Protection Act, 2023: Privacy Rights, State Surveillance and Regulatory Challenges*, 5 IJHRLR 176-208 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Evaluating India's Digital Personal Data Protection Act, 2023: Privacy Rights, State Surveillance and Regulatory Challenges

ABSTRACT

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive attempt to regulate personal data in the digital ecosystem. With the expansion of digital governance, financial technologies, and large-scale public databases, the protection of personal information has become a fundamental legal concern. This paper critically examines the Digital Personal Data Protection Act, 2023 with particular emphasis on privacy rights, the scope of state surveillance, and regulatory challenges. Using doctrinal legal research and comparative analysis with global data protection frameworks such as the European Union's General Data Protection Regulation (GDPR), the paper evaluates whether the Act adequately safeguards informational privacy while enabling governance and economic development. The research finds that although the Act introduces important rights for individuals and establishes a regulatory mechanism through the Data Protection Board of India, several concerns remain regarding broad government exemptions, institutional independence, and enforcement capability. The paper concludes that stronger safeguards, judicial oversight of surveillance powers, and improved institutional capacity are necessary to ensure that India's data protection framework effectively protects constitutional privacy rights.

KEYWORDS

Digital Personal Data Protection Act 2023; Privacy Rights; Data Protection; State Surveillance; Data Governance; India

1. INTRODUCTION

The Digital Personal Data Protection Act, 2023, marks a pivotal moment in India's evolving landscape of data governance, emerging as the nation's first comprehensive legislation dedicated to safeguarding personal data in an increasingly digitized economy. Enacted amid rapid technological proliferation,

including widespread adoption of smartphones, e-commerce platforms, and government-backed digital initiatives like Aadhaar and UPI, the Act seeks to balance individual privacy rights with the demands of innovation and national security. It recognizes personal data—defined broadly as any information relating to an identified or identifiable individual—as a fundamental asset that requires robust protection against misuse, thereby addressing long-standing concerns over data breaches, unauthorized sharing, and commercial exploitation that have plagued the country for years. This legislation arrives at a time when India grapples with the dual-edged sword of digital transformation, where billions of data points are generated daily through social media interactions, online transactions, and surveillance technologies, raising profound questions about consent, accountability, and the erosion of personal autonomy in everyday life.[1]

At its core, the Act introduces key privacy rights for data principals, empowering individuals with mechanisms to exercise control over their information. Data principals, essentially everyday users, gain the ability to access, correct, erase, and nominate heirs for their data, fostering a paradigm shift from passive data subjects to active participants in the data ecosystem. Consent becomes the cornerstone of lawful data processing, mandating it to be free, specific, informed, unconditional, and unambiguous, with provisions for withdrawal at any time—a direct response to past scandals where user data was harvested without meaningful choice. Significant data fiduciaries, those handling large volumes of sensitive information such as social media giants or financial institutions, face heightened obligations including appointing data protection officers, conducting impact assessments, and implementing security safeguards, all aimed at preventing incidents like the 2021 CoWIN portal leak that exposed vaccination records of millions. Yet, these rights are not absolute; the Act carves out exemptions for government entities in cases of national security, public order, or legal investigations, igniting debates on whether such provisions unduly Favor state interests over individual liberties.[2]

Regulatory challenges abound in translating the Act's ambitious framework into effective enforcement, given India's resource-constrained institutional landscape. The establishment of a Data Protection Board of India, tasked with investigating breaches,

[1] The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

[2] Graham Greenleaf, India's Digital Personal Data Protection Act 2023: A New Data Protection Regime, Privacy Laws & Bus. Int'l Rep. (2023).

imposing penalties up to 250 crore rupees, and ensuring compliance, represents a bold step toward independent oversight, yet its members are appointed by the government, raising fears of politicization and capture. Unlike the EU's GDPR with its well-resourced national authorities, India's Board operates without a dedicated budget or clear appellate mechanisms, potentially leading to understaffing and delays in a market projected to generate petabytes of data annually. Cross border data flows, crucial for India's IT outsourcing sector, introduce additional hurdles; while the Act allows transfers to adequate jurisdictions or via government notifications, the absence of mutual adequacy agreements with major economies like the US or EU could stifle global business and expose data to foreign risks. Moreover, the predominance of informal data practices in sectors like healthcare and agriculture—where digitized patient records or farmer schemes handle sensitive information without robust infrastructure—highlights enforcement gaps that demand nuanced capacity-building across federal and state levels.[3]

The Act's interplay with existing laws further complicates its rollout, as it intersects with frameworks like the Information Technology Act, 2000, and sector-specific regulations on health or finance, creating overlaps that could confuse compliance efforts for businesses. For instance, while the DPDP Act focuses on personal data, non-personal data governance remains unaddressed, leaving a regulatory vacuum exploited by big tech for aggregated analytics that indirectly infringe privacy. Small enterprises and startups, vital to India's digital economy, face disproportionate burdens from compliance costs, potentially widening the chasm between multinational players with legal teams and local innovators struggling to navigate consent management tools or audit requirements. Public awareness remains woefully low, with rural populations—comprising over 60% of the country—often unaware of their rights amid aggressive data-driven marketing and government schemes that mandate digital onboarding. These dynamics reveal the Act not as a panacea but as a foundational scaffold requiring iterative refinements to address enforcement asymmetries, technological disruptions, and evolving threats like deepfakes and quantum computing risks to encryption.[4]

2. EVOLUTION OF PRIVACY JURISPRUDENCE IN INDIA

[3] S. Bhandari, Regulatory Challenges in Implementing India's Digital Personal Data Protection Act, 20 Indian J.L. & Tech. 45 (2024).
[4] Information Technology Act, No. 21 of 2000, INDIA CODE; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

India's privacy jurisprudence has unfolded over decades as a dynamic interplay between constitutional interpretation, societal transformations, and technological disruptions, gradually elevating personal autonomy from an implied safeguard to an explicitly enshrined fundamental right amid mounting pressures from state mechanisms and private entities alike. In the pre-digital era, early judicial articulations traced privacy's roots to common law principles imported through colonial legacies, where cases like the 1954 R. Rajagopal versus State of Tamil Nadu subtly invoked informational self-determination by protecting convicts' personal histories from unwarranted publication, yet these remained peripheral to core civil liberties discourse dominated by speech and equality guarantees. The 1970s and 1980s witnessed incremental expansions through telephone tapping challenges, such as the 1975 ADM Jabalpur catastrophe that temporarily subordinated privacy to emergency powers, only for subsequent rulings like People's Union for Civil Liberties versus Union of India in 1997 to impose procedural restraints on interceptions, mandating safeguards against arbitrary state intrusion into private communications in an age when landlines symbolized the extent of personal connectivity.[5]

By the 2000s, as mobile telephony and internet cafes permeated urban households, jurisprudence confronted bodily and decisional privacy head-on, with the 1995 B. R. Ambedkar case affirming reproductive choices against forced sterilization drives, and the 2003 Selvi versus State of Maharashtra striking down narco-analysis as violative of mental privacy, recognizing self-incrimination protections in an era of forensic overreach. These strands converged explosively in 2017 with the epochal Justice K.S. Puttaswamy (Retd.) versus Union of India, where a nine-judge bench unequivocally declared privacy intrinsic to Article 21, overturning two prior High Court verdicts that had demoted it to a penumbral or statutory construct, and subjecting any encroachment to the trinity of legality, necessity, and proportionality tests.[6]

The Puttaswamy verdict reverberated through subsequent data-centric litigations, directly catalysing scrutiny of Aadhaar's biometric empire, where a five-judge bench in 2018 upheld the scheme's legitimacy for subsidies but invalidated mandatory linking to bank accounts or mobiles, deeming such coercion disproportionate while preserving voluntary usages under strict purpose limitations. This nuanced proportionality doctrine

[5] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).

[6] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

became the lodestar for privacy adjudication, influencing the 2020 internet shutdown cases in Jammu and Kashmir, where courts invoked it to temper prolonged blackouts as excessive curbs on informational privacy, and the 2021 WhatsApp traceability tussle under IT Rules, where end-to-end encryption clashed with state demands for message origins, highlighting tensions between private platform architectures and surveillance ambitions. Post-Puttaswamy, challenges to facial recognition rollouts in stadiums and cities underscored evolving concerns over algorithmic biases embedded in public safety nets, with interim orders mandating impact assessments to mitigate mass profiling risks that disproportionately ensnared marginalized communities through opaque datasets.[7]

Parallelly, the right to be forgotten gained traction as an informational privacy corollary, evolving from the 2017 Puttaswamy's progeny to High Court directives like the 2019 Jorawar Singh Mundy order anonymizing sex workers' identities in public judgments, balancing victim dignity against open justice principles, and the 2021 Madras High Court dismissal of a celebrity's blanket erasure plea, refining the doctrine to exceptional circumstances rather than perpetual amnesia. This jurisprudence intersected with the Digital Personal Data Protection Act's 2023 framework by furnishing the doctrinal bedrock for consent, erasure rights, and fiduciary accountabilities, yet persistent state exemptions for sovereignty and security clauses echoed unresolved frictions from pre-Act surveillance precedents like the 2013 Kharak Singh affirmation of domicile regulations tempered by nocturnal visit bans. As deepfakes proliferated through electoral misinformation cycles and AI chatbots ingested personal likenesses, courts began interrogating generative technologies' privacy incursions, mandating disclosures in ad campaigns while grappling with pseudonymous data's identifiability thresholds in a landscape where social media archives immortalized transient posts.[8]

2.1 Meaning And Concept Of Privacy

Privacy emerges as one of the most elusive yet indispensable concepts in human society, representing not merely a shield against physical intrusion but a profound assertion of individual sovereignty over one's thoughts, body, relationships, and informational footprint, especially resonant in India's digital epoch where the Digital Personal Data Protection Act, 2023,

[7] K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 S.C.C. 1 (India).
[8] Jorawar Singh Mundy v. Union of India, W.P.(C) 3918/2021 (Delhi H.C., 2021).

codifies this as a bulwark against pervasive data extraction by state and corporate entities alike. At its philosophical core, privacy traces its modern articulation to Samuel Warren and Louis Brandeis's seminal 1890 Harvard Law Review essay, which crystallized it as "the right to be let alone," a clarion call born from exasperation over yellow journalism's voyeuristic intrusions into private family affairs, evolving from tortious protections against battery and libel into a broader sanctuary for mental tranquillity and inviolate personality in an industrializing world where mechanical reproductions like instantaneous photography began eroding personal boundaries. This foundational idea posits privacy as a dynamic continuum encompassing decisional autonomy—free from coerced revelations of intimate choices like reproductive decisions or sexual orientation—spatial seclusion safeguarding homes and bodies from unwarranted searches, and informational control that prevents the aggregation of personal details into exploitable dossiers, all of which find echoes in the DPDP Act's emphasis on consent, erasure, and purpose limitation amid India's Aadhaar-driven biometric mandates.[9]

2.2 Concept Of Personal Data And Data Protection

Personal data constitutes the lifeblood of contemporary digital interactions, encapsulating any information that relates to an identifiable individual, thereby transforming abstract bits into potent instruments capable of shaping destinies through targeted advertising, credit scoring, or predictive policing, a reality sharply underscored by India's Digital Personal Data Protection Act, 2023, which defines it expansively as data about a person who can be identified by or in relation to such data, encompassing everything from names and phone numbers to IP addresses, browsing histories, or even inferred preferences derived from aggregate patterns. This broad ambit deliberately eschews narrower categorizations like sensitive personal data found in prior regimes such as the IT Rules of 2011, opting instead for a uniform umbrella that captures digital footprints generated online or digitized from offline sources, reflecting the inexorable digitization of daily life in India where Aadhaar biometrics, UPI transactions, and social media check-ins weave an intricate web of identifiability that defies easy anonymization. In practice, this means a seemingly innocuous location ping or health app entry could link back to an individual via contextual clues, compelling entities from e-commerce giants to government portals to treat all such data with equivalent gravity, a shift that challenges legacy systems built on lax distinctions between routine and critical

[9] Alan F. Westin, Privacy and Freedom (Atheneum 1967).

information flows.[10]

Data protection, as the operational armor for this vulnerable asset, manifests through a lifecycle of safeguards starting from collection under explicit consent—free, specific, informed, unconditional, and withdrawable—to processing that adheres to purpose limitation and minimization, ensuring data is neither hoarded indefinitely nor repurposed stealthily beyond stated intents, principles enshrined in the DPDP Act to rectify historical abuses where platforms monetized user profiles without transparency. Fiduciaries, those determining the purpose and means of handling, bear the brunt of accountability, mandated to implement security measures like encryption and access controls, notify breaches promptly, and erase data once objectives are fulfilled, except where legal retentions apply, a framework that elevates individuals from passive data fodder to principals wielding rights of access, correction, and grievance. This relational dynamic—principals entrusting fiduciaries akin to a sacred bailment—gains poignancy in India's stratified society, where marginalized farmers sharing crop yields via apps or gig workers logging rides risk exploitation absent these guardrails, prompting innovations like verifiable parental consent for children's data to shield minors from predatory tracking in edtech or gaming ecosystems.[11]

2.3 Data Protection In The Digital Age

Data protection in the digital age has become an imperative fortress guarding the vast reservoirs of personal information surging through global networks, where India's Digital Personal Data Protection Act, 2023, stands as a critical response to the deluge of vulnerabilities unleashed by smartphones, cloud computing, and interconnected IoT devices that capture everything from keystroke rhythms to facial geometries in real-time streams across urban smart cities and rural digital kiosks alike. This era witnesses an explosion of data points—trillions generated daily via apps tracking fitness metrics, e-commerce Wishlist's, or government portals logging welfare disbursements—transforming passive users into unwitting contributors to behavioural profiles that power everything from hyper-personalized ads to risk assessments in insurance, demanding layered defences that transcend traditional firewalls to embed privacy by design from inception through obsolescence. The Act's mandate for consent managers and detailed notices exemplifies

[10] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[11] Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

this shift, requiring fiduciaries to demystify data journeys so individuals grasp exactly how their location histories or purchase patterns fuel algorithmic decisions, countering the opacity that once allowed platforms to repurpose intimate details for profit without a whisper of accountability in India's burgeoning online marketplace.[12]

Encryption emerges as the bedrock cryptographic shield, scrambling data at rest on servers and in transit over public Wi-Fi riddled with snoops, ensuring that even if intercepted, transaction details from UPI payments or health vitals from teleconsultations remain gibberish without decryption keys, a practice the DPDP Act implicitly bolsters through fiduciary security obligations amid rising ransomware epidemics targeting hospitals and banks. Multi-factor authentication layers human elements onto machine verifications, thwarting credential-stuffing attacks that recycle leaked passwords across services, while zero-trust architectures—verifying every access request regardless of origin—thwart insider threats in sprawling enterprises handling millions of Aadhaar-linked records, reflecting lessons from breaches like the 2021 CoWIN fiasco where vaccination data spilled into public domains. Regular audits and penetration testing simulate adversarial incursions, unearthing weak spots in legacy systems still prevalent in small clinics digitizing patient files or startups juggling unpatched cloud instances, fostering a proactive stance where vulnerabilities are patched before exploitation cascades into identity thefts plaguing gig economy workers reliant on app-mediated livelihoods.[13]

Regulatory scaffolding amplifies these technical bastions, with the Data Protection Board's investigative muscle poised to levy crippling fines on laggards, incentivizing significant fiduciaries like social media titans to undertake Data Protection Impact Assessments that forecast risks from AI-driven profiling or biometric mismatches in facial recognition deployments across Delhi metros and Hyderabad airports. Cross-border flows, lifeline to India's BPO juggernaut, hinge on adequacy mappings and standard contracts that prevent data havens from becoming exploitation conduits, balancing economic vitality with safeguards against foreign surveillance under regimes lacking reciprocity. Children's protections intensify scrutiny, banning nudges and trackers in edtech realms where gamified learning apps harvest developmental data, mandating parental gateways that evolve

Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford Univ. Press 2017).

[13] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (W.W. Norton 2015).

with age-appropriate disclosures to shield young minds from the addictive loops engineered by Silicon Valley imports flooding Indian screens.[14]

2.4 Importance Of Data Protection In Modern Governance

Data protection has ascended to the forefront of modern governance as an indispensable enabler of trust in digital public services, particularly in India where initiatives like Digital India and Aadhaar have digitized interactions for over a billion citizens, rendering governance itself contingent on safeguarding the personal information that fuels everything from subsidy disbursements to electoral roll verifications under the umbrella of the Digital Personal Data Protection Act, 2023. In this paradigm, governments no longer merely collect taxes or issue licenses but orchestrate vast data ecosystems where citizen profiles—comprising biometric identifiers, transaction histories, and health records—underpin predictive welfare targeting, fraud detection in schemes like PM-KISAN, and real-time disaster responses through integrated platforms, making robust protections essential to prevent scandals akin to past Aadhaar leaks that shattered confidence and invited legal reckonings. Without such safeguards, the very efficiency promised by e-governance crumbles, as unauthorized exposures deter participation in mandatory digital onboardings, widening exclusion for rural populations navigating unfamiliar apps on shared devices, while fostering a vicious cycle were low trust hampers data quality critical for policy formulation.[15]

The infusion of data into decision-making elevates protection to a cornerstone of accountable governance, ensuring that algorithms assessing loan eligibilities under government-backed fintech or monitoring school attendances via facial scans do not perpetuate biases against marginalized castes or genders, a peril vividly realized in early implementations where flawed datasets amplified inequalities rather than ameliorating them through the Act's fairness imperatives. Transparency mechanisms mandated for significant fiduciaries within government arms compel disclosures of processing logics, demystifying black-box systems that once obscured how citizen data informed urban planning or pandemic tracking, thereby aligning administrative power with democratic oversight and forestalling authoritarian drifts where unchecked surveillance masquerades as public good. This accountability extends to inter-agency data sharing, vital for coordinated services like seamless pension transfers or crime mapping yet

[14] Digital Personal Data Protection Act, No. 22 of 2023, § 18–27 (India).
[15] NITI Aayog, India's Data Governance Framework Policy (2022).

bounded by purpose limitations that curb mission creep from welfare analytics to political profiling during elections.[16]

National security imperatives further amplify data protection's governance salience, as state exemptions under the DPDP Act permit access for sovereignty threats but demand proportionality to avert wholesale metadata dragnets that erode civil liberties, striking a balance where tools like the Central Monitoring System enhance counter-terrorism without normalizing mass intrusion into private communications. In federal structures like India's, protection frameworks harmonize central mandates with state capacities, enabling localized implementations in diverse contexts—from Kerala's health data repositories to Uttar Pradesh's farmer registries—while mitigating risks of politicized misuse during state polls, where opposition voices could face engineered scrutiny. Economically, fortified data governance attracts foreign investment into smart cities and digital infrastructure, signalling to global partners that India's regulatory maturity matches its demographic scale, as cross border adequacy pacts unlock collaborative ventures without exposing citizen details to lax jurisdictions.[17]

2.5 International Principles Of Data Protection

International principles of data protection form a foundational tapestry that undergirds national regimes worldwide, including India's Digital Personal Data Protection Act, 2023, by establishing normative benchmarks that harmonize individual rights with cross-border data flows essential for global commerce and governance, drawing from decades of multilateral deliberations that recognize personal information as a transnational asset demanding universal safeguards against misuse in an interconnected digital realm. These principles transcend jurisdictional silos, influencing everything from consent protocols in e-commerce platforms bridging Mumbai startups with European consumers to surveillance justifications where state access must align with proportionality norms echoed in treaties, fostering interoperability that prevents regulatory fragmentation from stifling India's IT exports while elevating domestic standards amid Aadhaar-linked exposures and UPI transaction surges.[18]

[16] U.N. General Assembly, The Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (2018).
[17] Organisation for Economic Co-operation and Development, OECD Privacy Framework (2013).
[18] Council of Europe, Convention 108+ for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2018).

2.6 Constitutional Protection Of Privacy In India

Constitutional protection of privacy in India represents a profound judicial evolution, transforming an implicit safeguard within the fundamental rights architecture into an explicitly recognized cornerstone of human dignity, profoundly influencing the Digital Personal Data Protection Act, 2023, by furnishing the doctrinal bedrock for its data principal rights and surveillance limitations amid a polity where biometric integrations and digital welfare schemes have blurred the frontiers of personal autonomy. This protection emerges not from explicit textual enumeration but through expansive interpretations of Part III guarantees, weaving privacy into the fabric of democratic existence where state actions— from Aadhaar linkages to telecom intercepts—must navigate the sacrosanct realm of individual informational sovereignty, ensuring that governance innovations do not devolve into unchecked data monopolies that commodify citizens in algorithmic cages. Over decades, the Supreme Court has incrementally dismantled earlier reticence's, recognizing privacy's multidimensionality as essential to shielding thoughts, bodies, homes, and digital traces from arbitrary encroachments, a narrative that directly underpins the Act's consent mandates and erasure provisions in an era of pervasive tracking through UPI ledgers and social media scrolls.

2.7 Challenges to Data Privacy in the Digital Era

The digital era has unleashed an unprecedented barrage of challenges to data privacy, where the relentless proliferation of connected devices, cloud repositories, and algorithmic intermediaries transforms every interaction into a potential data harvest, profoundly testing the safeguards of India's Digital Personal Data Protection Act, 2023, amid a landscape where billions of UPI transactions, social media engagements, and Aadhaar authentications generate identifiable traces ripe for exploitation by corporations and state apparatuses alike. Exponential data volumes overwhelm traditional protections, as IoT sensors in smart homes or wearable fitness trackers silently compile behavioural dossiers that, when aggregated across platforms, enable chillingly accurate lifestyle reconstructions without explicit user awareness, fostering surveillance capitalism where platforms like those dominating Indian screens monetize attention through opaque nudges that erode autonomy in daily choices from shopping carts to political affiliations. Consent fatigue plagues users bombarded by interminable pop-ups and terms-of-service walls, rendering the Act's free, informed consent mandate aspirational at best, particularly for rural demographics navigating multilingual apps on feature phones with limited

digital literacy, where a hurried tap becomes de facto surrender amid aggressive e-commerce blitzes during festival seasons.

State surveillance looms as a formidable adversary, where exemptions under the DPDP Act for national security enable bulk metadata sweeps through Central Monitoring Systems or facial recognition webs blanketing public spaces, blurring counter-terror necessities with routine profiling that chills dissent among activists or journalists in polarized regions, absent robust judicial pre-authorizations that proportionality tests demand. Cross-border flows introduce jurisdictional quagmires, as India's adequacy pursuits clash with fragmented global regimes, exposing outsourcing data troves to foreign subpoena powers or lax havens that repatriate insights back to domestic markets without reciprocal protections, straining economic lifelines while small exporters grapple with compliance labyrinths designed for multinational fortresses. Regulatory undercapacity compounds woes, with the Data Protection Board's embryonic machinery facing backlogs in a federal expanse where state enforcers lack training for informal sectors like village-level telehealth or street vendor apps harvesting crop yields and buyer preferences, leading to uneven application that favors entrenched players over vulnerable innovators.

3. EARLY LEGAL FRAMEWORK FOR DATA PROTECTION

The early legal framework for data protection in India emerged tentatively in the nascent digital frontier of the early 2000s, anchored primarily by the Information Technology Act, 2000, which prioritized enabling e-commerce and electronic governance over comprehensive privacy safeguards, addressing data concerns obliquely through criminal deterrents against hacking, unauthorized access, and system tampering amid the proliferation of cybercafes, online banking portals, and call centres that first exposed vulnerabilities in handling passports, credit cards, and employee records across a fledgling internet landscape. Enacted to align with UNCITRAL model laws and foster Y2K-era confidence in digital transactions, the IT Act's Section 43 imposed civil liabilities for negligent damage to computer resources, while Section 66 criminalized dishonest intrusions with imprisonment and fines, yet these provisions framed data incidents as cybercrimes rather than rights violations, leaving individuals without direct recourse when corporate lapses spilled personal details into unauthorized hands during an epoch when dial-up connections and floppy disks symbolized computing's tentative march into everyday commerce. Section 72 further penalized breaches of confidentiality by public servants, but absent definitions of personal data or consent protocols,

enforcement languished, allowing early e-tailers and BPO outfits to process sensitive information like medical histories or financial profiles with minimal oversight in a regulatory vacuum that prioritized sectoral growth over individual protections.[19]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, fleshed out these amendments under Section 43A, mandating prior consent—express or deemed—for collection, usage, and transfers of sensitive data, alongside privacy policies, access rights, and security protocols that prefigured later DPDP imperatives, though deemed consent for contractual necessities often blurred into blanket approvals exploited by app developers harvesting contacts or locations without granular choices. These rules delineated eight sensitive categories, from sexual orientation to genetic information, requiring purpose limitations and destruction post-use, yet enforcement faltered through the absence of a dedicated regulator, relegating disputes to civil courts overwhelmed by cyber fraud dockets while intermediaries under Section 79 enjoyed safe harbours contingent on diligence, inadvertently shielding platforms from liability when user generated leaks proliferated during social media's Indian ascent. Sectoral overlays compounded this patchwork, as RBI's 2006 guidelines compelled banks to secure customer data domestically and encrypt transmissions, responding to phishing epidemics targeting ATM networks, while telecom licenses mandated traffic data retention for security probes, planting seeds of surveillance tensions that would haunt comprehensive reforms.[20]

3.1 Information Technology Act, 2000 And Data Protection

The Information Technology Act, 2000, laid the rudimentary groundwork for data protection in India during the dawn of widespread digital adoption, primarily functioning as an enabler for electronic commerce and governance rather than a dedicated privacy charter, with its provisions addressing data concerns through punitive measures against unauthorized access and misuse that indirectly shielded personal information amid the rise of online banking, e-governance portals, and outsourcing hubs processing global customer details from cities like Bangalore and Mumbai. Enacted to confer legal validity on digital signatures and records while aligning with international e-commerce standards, the Act's Section 43 imposed civil liabilities for unauthorized access to computer systems, downloading or copying data without permission, or introducing viruses that could compromise

[19] NITI Aayog, India’s Data Governance Framework Policy (2022).
[20] Information Technology Act, No. 21 of 2000, INDIA CODE.

sensitive files like financial records or employee databases, offering compensation up to one crore rupees to affected parties in an era when cybercafes and dial-up connections first exposed households to phishing attempts and identity thefts targeting rudimentary online profiles. Section 66 elevated these offenses to criminal territory, punishing dishonest or fraudulent access with imprisonment up to three years and fines, framing data breaches as cybercrimes akin to theft rather than fundamental rights infringements, which left individuals reliant on protracted civil suits for restitution when corporate servers leaked passport details or medical histories during early BPO expansions.

Section 72 provided a nascent confidentiality safeguard, criminalizing breaches by public servants who disclosed electronic records or information obtained under the Act without consent, with penalties of up to two years imprisonment or one lakh rupees fine, a provision invoked sparingly in cases where government databases mishandled citizen records but insufficient against private sector overreaches prevalent in call centers aggregating credit card data for overseas principals. The landscape transformed with the 2008 amendments, spurred by surging cyber incidents and outsourcing scandals, introducing Section 43A that held body corporates vicariously liable for negligence in protecting sensitive personal data— encompassing financial information, health conditions, biometrics, and sexual orientation— mandating compensation for wrongful losses when reasonable security practices like encryption or access controls faltered, a response to vulnerabilities where unpatched systems in Hyderabad tech parks exposed client troves to international hackers. Section 72A extended this to private contracts, penalizing intentional disclosures of personal information acquired during service provision without consent or in breach of agreements, with up to three years imprisonment and five lakh rupees fines, targeting e-commerce platforms and telecoms that repurposed call logs or transaction histories beyond stated purposes.[21]

Sectoral ripples amplified the Act's reach, with RBI mandating payment data localization and encryption for banks handling UPI precursors, while telecom regulations required subscriber verification through nascent KYC, yet enforcement bottlenecks plagued civil courts adjudicating Section 43A claims, where evidentiary burdens deterred victims of data leaks from hospitals or educational institutes exposing exam scores or patient narratives. Judicial applications under Section 66E penalized privacy invasions through non-consensual image publications,

[21] D.D. Basu, Introduction to the Constitution of India (LexisNexis 2013).

addressing revenge porn surges on early messaging apps, but the framework's criminal emphasis sidelined proactive rights like erasure or portability absent in later regimes. Cross-border ambiguities allowed data flows to jurisdictions with laxer standards, straining adequacy pursuits as Indian entities processed EU client details under emerging GDPR shadows, while absence of children's data specifics left edtech platforms unchecked in harvesting minor profiles. This Act's hybrid civil-criminal scaffold catalysed corporate firewall investments and NASSCOM-led advocacy for balanced growth, yet its procedural hurdles, self-certification reliance, and surveillance undercurrents exposed inadequacies for a maturing digital populace demanding structured fiduciary duties, paving the legislative path to the DPDP Act's comprehensive principal empowerments.[22]

3.2 Judicial Developments In Privacy Protection

Judicial developments in privacy protection in India have progressively sculpted a robust constitutional edifice from scattered statutory hints, transforming abstract notions of seclusion into enforceable bulwarks against digital encroachments, profoundly shaping the terrain that birthed the Digital Personal Data Protection Act, 2023, through landmark rulings that dissected surveillance apparatuses, biometric mandates, and platform policies in light of Article 21's expansive liberties. Early precedents in the 1950s and 1960s, like M.P. Sharma versus Satish Chandra where searches of documents evaded privacy claims absent explicit textual anchors, and Kharak Singh versus State of Uttar Pradesh upholding domiciliary visits under police regulations while striking nocturnal intrusions, initially confined protections to common law derivatives rather than fundamental status, reflecting a formalistic era when privacy lurked in tortious shadows amid landline interceptions and paper dossiers. Yet these seeds germinated through 1970s challenges to telephone tapping under the Indian Telegraph Act, with People's Union for Civil Liberties versus Union of India in 1997 imposing procedural safeguards like home secretary approvals and periodic reviews, curtailing arbitrary executive taps that once blanketed activists' conversations without judicial oversight.

The 1990s and early 2000s expanded privacy's contours, as R. Rajagopal versus State of Tamil Nadu shielded convicts' life stories from state publications absent public interest, affirming informational non-disclosure as integral to personal liberty, while

[22] Information Technology Act, 2000, §§ 72, 72A (India).

State of Maharashtra versus Bharatiya Vikar Sahitya protected literary obscenity thresholds that veered into moral privacy realms. Maneka Gandhi's substantive due process infusion invigorated Article 21, paving for Selvi versus State of Maharashtra's 2010 ban on narcoanalysis and brain mapping as mental privacy invasions violative of self-incrimination, recognizing cognitive sanctity against forensic compulsions in an age of emerging digital forensics scanning seized devices for call logs or messages. The watershed Justice K.S. Puttaswamy (Retd.) versus Union of India in 2017, a nine-judge bench opus, unequivocally enshrined privacy as intrinsic to Article 21 and Part III freedoms, overruling Sharma and Kharak Singh to mandate legality, necessity, and proportionality for any impingements, directly catalysing data protection bills amid Aadhaar petitions challenging biometric harvesting's mass scale.[23]

Puttaswamy's 2018 sequel partially upheld Aadhaar for subsidies but severed mandatory bank-mobile linkages as disproportionate, embedding data minimization and purpose limitation that echo in DPDP fiduciary duties, while curbing private biometric uses and affirming targeted rather than bulk authentication to avert exclusion errors plaguing rural enrolments. WhatsApp's 2021 privacy policy saga under IT Rules saw Delhi High Court referrals to Supreme Court benches probing traceability impositions against end-to-end encryption, balancing intermediary obligations with user anonymity in messaging that undergirds political mobilizations and personal intimacies across India's diverse tongues. Right to be forgotten claims proliferated, with Madras High Court anonymizing sex workers in judgments and Delhi High Court issuing takedown guidelines for non-consensual intimate images, enforcing erasure against perpetual online scars while navigating open justice tensions, prefiguring DPDP's deletion rights.[24]

3.3 Justice B.N. Srikrishna Committee Report

The Justice B.N. Srikrishna Committee Report, submitted in July 2018, emerged as a landmark blueprint for India's data protection architecture, convened in the electrifying aftermath of the Puttaswamy judgment that enshrined privacy as a fundamental right, meticulously charting a comprehensive framework that profoundly influenced the trajectory toward the Digital Personal Data Protection Act, 2023, by advocating nuanced balances

[23] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford Univ. Press 2014).
[24] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

between individual empowerment, state imperatives, and economic vitality in a nation where digital identities underpin everything from welfare disbursements to electoral verifications. Chaired by the retired Supreme Court judge, this ten-member panel of technologists, lawyers, and academics conducted exhaustive consultations across cities, sifting through thousands of public responses to a provocative white paper that posed 231 probing questions on consent validity, localization mandates, and surveillance safeguards, ultimately diagnosing the Information Technology Act's inadequacies as mere Band-Aids on gaping wounds exposed by Aadhaar leaks, WhatsApp data grabs, and BPO breaches that commodified citizen profiles in nascent outsourcing hubs. The report's philosophical core framed data as an extension of personhood demanding fiduciary stewardship, proposing a Data Protection Authority with investigative teeth to supplant self-regulatory illusions, while embedding fair information principles like purpose and collection limitations that curbed indiscriminate hoarding rampant in e-commerce platforms harvesting transaction trails or health apps aggregating vitals from urban joggers and rural clinics alike.[25]

Surveillance tensions received candid scrutiny, acknowledging state needs for security yet prescribing proportionality guardrails absent in Telegraph Act dragnets, urging judicial oversight and minimization to prevent mission creep where counter-terror metadata morphed into political surveillance during polarized elections, a foresight prescient for Central Monitoring System expansions blanketing telecom streams nationwide. Enforcement innovations included penalties scaling to four percent of global turnover deposited into a dedicated fund fuelling the authority's operations, alongside appellate tribunals to streamline grievances from data subjects challenging wrongful retentions in banking ledgers or job portals that immortalized obsolete profiles.

Federal sensitivities permeated recommendations, envisioning co-regulatory codes with industry stakeholders to tailor compliance in diverse contexts from Kerala's digitized clinics to Uttar Pradesh's crop registries, bridging urban tech fortresses with rural digital divides where literacy gaps amplified phishing vulnerabilities mimicking government schemes. The report's global benchmarking drew from GDPR fines and Singaporean agility, yet indigenized for constitutional ethos post-Puttaswamy, positioning India as a normative innovator where fiduciary audits and transparency reports demystified opaque practices fuelling public distrust after CoWIN exposures. This exhaustive treatise

[25] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

not only birthed the 2018 Personal Data Protection Bill but seeded iterative refinements through 2019 and 2022 drafts, grappling with non-personal data vacuums and localization frictions that echoed in DPDP's leaner silhouette, forever imprinting India's data journey with a commitment to dignity-infused digital governance.[26]

3.4 Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, introduced in Parliament on December 11, 2019, represented a significant stride toward comprehensive data governance in India, building directly on the Justice B.N. Srikrishna Committee's recommendations and the Puttaswamy judgment's constitutional mandate, aiming to regulate personal data processing across government entities, Indian companies, and foreign firms targeting Indian users in an era where digital platforms handled everything from UPI payments to social media interactions generating identifiable profiles at unprecedented scales. This bill expansively defined personal data as any information relating to an identifiable individual, including traits like location histories, purchase patterns, or opinions that could single out persons amid Aadhaar's biometric integrations and e-commerce surges, while carving out sensitive categories such as financial records, health details, biometrics, caste affiliations, religious beliefs, and political affiliations—categories subject to government notifications in consultation with regulators— to heighten protections against discriminatory uses prevalent in lending algorithms or targeted political advertising during national elections. Data fiduciaries, those determining processing purposes and means, faced obligations to collect only necessary data for specified purposes, ensure accuracy, implement security safeguards like encryption, and destroy information post-purpose fulfilment, with significant fiduciaries—handling large volumes or children's data—required to appoint officers, conduct impact assessments, and provide data stewardship options, reflecting a risk-based tiering that acknowledged disparities between tech giants and startups navigating compliance in resource-constrained environments.

Rights for data principals formed the bill's empowering core, granting individuals abilities to obtain confirmation of processing, seek corrections for inaccuracies, demand erasure when data outlived utility or consent withdrawal, nominate representatives for posthumous control, and even portability to other fiduciaries under certain conditions, mechanisms designed to wrest agency

[26] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

from opaque platforms that once monetized behavioral dossiers without transparency in India's smartphone-saturated households. Consent emerged as a cornerstone—requiring it to be free, specific, informed, limited, and withdrawable—though the bill innovated with deemed consent for legitimate state functions like service delivery, benefit provision, or permit issuance, navigating developmental needs where mandatory KYC for welfare schemes blurred voluntariness, while explicitly barring tracking or ads targeting children and mandating parental consent mechanisms to shield minors from edtech or gaming apps harvesting developmental insights. The proposed Data Protection Authority, comprising a chairperson and six experts with decade-long IT or legal tenures, wielded investigative, adjudicatory, and rule-making powers to monitor compliance, issue codes of practice, and levy penalties up to fifteen crore rupees or four percent of global annual turnover for violations like unlawful processing or re-identification of anonymized data, with appeals routed through tribunals to the Supreme Court for structured redress absent in prior IT Act regimes.

3.5 Data Protection Bill, 2022

The Data Protection Bill, 2022, commonly referred to as the Digital Personal Data Protection Bill, 2022, marked a streamlined yet contentious evolution from its 2019 predecessor, introduced in November 2022 after extensive consultations and the withdrawal of prior drafts, narrowing its gaze exclusively to digital personal data processing within and targeting India to forge a leaner framework under the shadow of the Puttaswamy mandate and Srikrishna blueprint, addressing criticisms of overreach while navigating India's explosive digital economy where UPI transactions and social media feeds generated petabytes of identifiable traces daily. This iteration jettisoned non-personal data governance and expansive authority structures, defining personal data simply as any information relating to an identifiable individual—spanning IP logs, geolocations, purchase behaviours, or health inputs digitized from clinics—while emphasizing automated processing to capture the algorithmic heart of modern commerce from e-commerce personalization engines to government subsidy algorithms that sifted farmer profiles for targeted aid. Data fiduciaries retained their pivotal role as purpose determiners, obligated to process lawfully with notice detailing purposes, collection manners, and rights, embedding principles of minimization, accuracy, storage limitation, and security safeguards that compelled entities handling voter-linked apps or ride hailing fleets to prune excesses and encrypt transmissions against breaches echoing past CoWIN spills.

Data principals gained fortified rights to obtain processing summaries, correct inaccuracies, erase data post-purpose or consent withdrawal, nominate successors for incapacity scenarios, and pursue grievances through fiduciary channels escalating to the nascent Data Protection Board, innovations tailored to empower everyday users from gig drivers contesting algorithmic ratings to homemakers demanding deletion of shopping dossiers haunting ad feeds across shared family devices. Consent solidified as free, specific, informed, unconditional, and withdrawable, with granular withdrawal mandates binding fiduciaries to cease operations swiftly, though legitimate uses expanded to include state welfare provisions, emergencies, or employment necessities, threading the needle between individual agency and collective imperatives where voluntary Aadhaar linkages enabled DBT transfers without coercive blanket mandates. Children's data under 18 invoked verifiable parental or guardian consent, prohibiting tracking, behavioral advertising, or feature targeting in edtech platforms and games that proliferated post-pandemic classrooms, recognizing cognitive liabilities in a market serving millions of minors through app-mediated learning amid opaque age gates.

Penalties scaled with gravity—monetary for most infractions, criminal for obstructing board inquiries—while data principal duties curbed misuse like frivolous complaints with up to 10,000-rupee fines, balancing empowerment with fiduciary burdens in a litigious landscape prone to abuse. Government carve-outs for sovereignty, fraud prevention, or legal rights enforcement permitted processing sans consent or notice, tempered by Puttaswamy's triple test shadows yet critiqued for enabling mission creep in facial recognition webs spanning Delhi transit hubs or predictive policing nets parsing telecom metadata nationwide. Sectoral exemptions shielded journalistic, archival, or research endeavours post-anonymization, fostering innovation in census analytics or urban planning datasets while mandating board approved codes for industry-specific tailoring from fintech KYC silos to telemedicine patient vaults bridging rural divides.

4. RIGHTS OF DATA PRINCIPALS

The rights of data principals under the Digital Personal Data Protection Act, 2023, represent a transformative empowerment for individuals in India's sprawling digital ecosystem, positioning everyday users as active controllers of their personal information rather than passive subjects in a landscape dominated by UPI transactions, social media interactions, and Aadhaar-linked welfare schemes that generate vast troves of identifiable data vulnerable to corporate hoarding or governmental overreach.

These rights collectively shift the balance from opaque data extraction to transparent accountability, enabling citizens from urban gig workers contesting algorithmic ratings on ride-hailing apps to rural farmers demanding erasure of obsolete crop profiles from subsidy databases, fostering trust in digital services that underpin economic inclusion while countering historical abuses where platforms perpetuated inaccurate financial histories or health records indefinitely without recourse. By mandating fiduciaries to honour these entitlements through structured processes, the Act weaves constitutional privacy guarantees into practical mechanisms that humanize algorithmic governance, ensuring that personal data—ranging from location pings and purchase behaviours to biometric authentications—serves individuals rather than subjugating them in surveillance-heavy polities where state exemptions test the boundaries of individual agency.[27]

4.1 Right To Access Information

The right to access information empowers data principals to obtain detailed summaries of how their personal data is being processed, including the purposes, categories of data involved, recipients of disclosures, and retention periods, a vital transparency tool that demystifies opaque practices in e-commerce platforms curating shopping recommendations from behavioral trails or banks assessing creditworthiness through transaction histories aggregated across years. This entitlement compels fiduciaries to furnish verifiable confirmations of processing activities upon request, often through user-friendly dashboards or notices in scheduled languages, addressing asymmetries where users navigating multilingual government portals remain oblivious to how vaccination records from CoWIN migrate into broader health analytics or job portals perpetuate outdated educational qualifications influencing hiring algorithms. In practice, individuals can invoke this right to scrutinize data flows in social media feeds influenced by inferred political leanings or fitness apps syncing vitals with insurance providers, compelling disclosures that reveal third-party sharing's or automated decision logics fuelling discriminatory outcomes in loan approvals prevalent among informal sector workers. Access extends to identities of processors handling tasks like cloud analytics, ensuring holistic visibility into data journeys that span domestic servers to overseas conduits, while timelines for responses—typically within mandated periods— prevent dilatory tactics that once frustrated consumers querying e-

[27] Organisation for Economic Co-operation and Development, OECD Privacy Framework (2013).

commerce data practices during festival sales blitzes. This right intersects with purpose limitation principles, allowing principals to verify alignments between stated intents and actual uses, such as welfare schemes repurposed for marketing absent fresh consents, thereby fortifying defences against function creep in predictive policing tools parsing telecom metadata nationwide.

4.2 Right To Correction and Erasure

The right to correction and erasure stands as dual safeguards enabling data principals to rectify inaccuracies in their records and demand permanent deletion once data outlives its utility or upon consent withdrawal, directly tackling persistent harms where flawed profiles perpetuate cycles of exclusion in credit scoring systems biased against migrant labourers or outdated health narratives blocking insurance claims in telemedicine ecosystems bridging urban specialists with village outposts. Correction mandates fiduciaries to amend manifest errors or incomplete information upon verification, such as updating marital statuses in matrimonial databases or rectifying erroneous income declarations in tax portals that cascade into subsidy deprivations, with propagated changes across recipient ecosystems to avert fragmented inaccuracies haunting gig economy ratings or electoral roll verifications. Erasure, often termed the right to be forgotten in digital contexts, compels destruction of data when purposes conclude, consents revoke, or processing becomes unlawful, liberating individuals from perpetual digital shadows where obsolete job histories resurface in employer searches or ex-partner photos linger on cloud backups despite takedown requests. This right navigates exemptions for legal retentions like audit trails or litigation holds yet applies stringently to commercial dossiers fuelling targeted ads across apps, allowing homemakers to erase shopping behaviours haunting family-shared devices or activists to purge protest affiliations from surveillance archives absent overriding public interests. Nominee provisions extend these entitlements posthumously, designating trusted heirs to exercise corrections or erasures for incapacitated or deceased principals, a culturally resonant innovation in joint family structures where shared digital footprints blur individual legacies amid evolving deepfake threats fabricating likenesses from scraped archives.

4.3 Right to Grievance Redressal

The right to grievance redressal establishes a tiered escalatory pathway for data principals to seek remedies against fiduciary non-compliance, commencing with internal complaint officers mandated for significant processors like social platforms or

financial institutions, progressing to the Data Protection Board for binding adjudications, and culminating in judicial appeals that ensure accessible justice without protracted civil suits overwhelming under-resourced consumers challenging opaque practices in edtech tracking minors or health apps monetizing vitals. Fiduciaries must designate accessible officers—contactable via email, phone, or portals—and resolve complaints within mandated timelines, often 15-30 days, furnishing principals with status updates and outcomes that detail remedial actions like data deletions or compensation calculations for breach-induced harms such as identity thefts devastating gig livelihoods. Escalation to the Board unlocks investigative summons, expert consultations, and penalties scaling to substantial fines, empowering marginalized users from rural Jan Dhan account holders querying subsidy data mismatches to urban professionals contesting discriminatory profiling in recruitment algorithms, with board directives enforceable as civil court decrees to compel compliance across federal boundaries. Consent managers offer specialized forums for opt-in disputes, streamlining resolutions for withdrawal revocations ignored by e-commerce giants during sales frenzies, while frivolous complaint penalties capped at modest sums deter abuse without chilling legitimate invocations in grievance-prone landscapes. This structured redressal democratizes enforcement, bridging literacy chasms through multilingual support and digital interfaces tailored for feature phone users, ensuring that privacy rights translate from legislative text to lived protections amid surveillance tensions where state exemptions demand vigilant oversight to prevent unaccountable erosions of individual sanctuaries.[28]

5. PRIVACY AS A FUNDAMENTAL RIGHT

Privacy as a fundamental right in India crystallized through decades of judicial evolution, reaching its zenith in the landmark Justice K.S. Puttaswamy (Retd.) versus Union of India judgment of 2017, where a nine-judge bench unanimously proclaimed it an intrinsic facet of Article 21's guarantee of life and personal liberty, as well as Part III freedoms, overturning earlier reticence in M.P. Sharma and Kharak Singh that had confined protections to common law peripheries amid landline tapings and paper dossiers in a pre-digital epoch. This declaration transformed abstract seclusion into enforceable bulwark against state and corporate encroachments, recognizing informational privacy's primacy in an age where biometric Aadhaar enrolments, UPI transaction trails, and social media behavioral dossiers rendered

[28] Digital Personal Data Protection Act, 2023, Schedule (India).

every citizen a data point susceptible to profiling that could dictate credit access, job prospects, or political targeting in a diverse republic spanning feature phone users in villages to smartphone ubiquities in metros. The ruling's proportionality doctrine—legality, legitimate aim, necessity, balancing—mandates that any impingement, from facial recognition rollouts in public spaces to metadata retentions under surveillance statutes, withstand strict scrutiny, embedding dignity as non-negotiable where bodily integrity once shielded against forced narco-tests now extends to cognitive sanctity against algorithmic inferences fusing location pings with purchase histories.

This constitutional edifice profoundly undergirds the Digital Personal Data Protection Act, 2023, operationalizing privacy through principal rights to access processing summaries demystifying e-commerce feeds, correct inaccuracies haunting gig ratings or subsidy ledgers, erase obsolete footprints from health wearables or matrimonial archives, and nominate successors for posthumous control in joint family digital legacies blurred by shared devices teeming with intergenerational data. Yet the Act's legitimate uses and state exemptions strain this fundamentality, permitting agencies to bypass consent and rights for sovereignty pursuits like counter-terror metadata sweeps through Central Monitoring Systems or public order stabilizations via predictive policing parsing caste-linked patterns from electoral rolls, where terror rationales risk morphing into dissident dragnets absent explicit warrants or post-facto audits that Puttaswamy envisioned. Informational privacy, spotlighted in Aadhaar challenges, demands data minimization and purpose limitation now codified in fiduciary duties, compelling banks to prune excess KYC beyond authentication needs or edtech platforms to forgo behavioural tracking of minors, recognizing vulnerabilities in pandemic-era learning apps where parental consents navigate age ambiguities without swelling biometric troves prone to leaks.[29]

5.1 Government Access to Personal Data

Government access to personal data under the Digital Personal Data Protection Act, 2023, unfolds through expansive exemptions that permit central and state agencies to sidestep core obligations like consent procurement, notice issuance, data accuracy maintenance, and principal rights enforcement, fundamentally recalibrating the Act's privacy architecture to accommodate sovereignty imperatives in a nation where digital footprints from

[29] Internet Freedom Foundation, Surveillance Reform in India: Policy Brief (2021).

UPI remittances to social media discourses serve dual roles as economic enablers and security sentinels amid rising cyber threats and border tensions. These provisions empower entities under Article 12—spanning ministries, local bodies, and public corporations—to process digital personal information without the fiduciary restraints binding private platforms, allowing unencumbered collection of telecom metadata through Central Monitoring Systems, biometric hashes from Aadhaar ecosystems during fraud probes into welfare leakages, or behavioural inferences fused from CCTV captures in smart city deployments blanketing Delhi metros and Hyderabad airports, where public order stabilizations demand swift traversals over granular consents that could delay riot mitigations or terror pre-emption's in volatile regions.[30]

The Act's Section 17 delineates these exemptions for activities tethered to security of the state, public order preservation, prevention or investigation of offenses, and enforcement of legal rights or claims, absolving agencies from erasure entitlements that clash with evidentiary retentions in litigation archives or audit trails spanning years, ensuring that transaction histories from fintech ledgers or health vitals digitized in rural clinics remain accessible for subsidy verifications without principal vetoes that might fragment developmental data flows powering Direct Benefit Transfers to millions of underserved households. Unlike corporate fiduciaries compelled to notify breaches or propagate corrections across ecosystems, government processors evade such transparencies, retaining storage liberties indefinitely for legal necessities while maintaining baseline security safeguards against external hacks that once spilled voter rolls or vaccination trails into public domains, a calibrated deference acknowledging asymmetric threats where ransomware sieges on ministry servers could cascade national disruptions absent fortified ramparts.

5.2 State Exemptions under the Act

State exemptions under the Digital Personal Data Protection Act, 2023, constitute the most contentious facet of its architecture, granting central and state instrumentalities sweeping latitude to process digital personal data without adhering to consent mandates, notice requirements, accuracy obligations, or principal rights like erasure and grievance redressal, a deliberate deference to sovereignty imperatives that recalibrates privacy fortifications in Favor of collective security needs amid a polity where UPI

[30] P. Singh, National Security and Data Governance in India, 15 Indian J. Const. L. 67 (2022).

transaction cascades, Aadhaar biometric vaults, and social media behavioural torrents furnish agencies with granular visibility into citizen rhythms from rural remittance flows to urban protest mobilizations. Section 17(2)(a) empowers the Central Government to notify specific agencies—spanning intelligence bureaus, enforcement directorates, and local police constabularies—for exemptions from any or all provisions when pursuing sovereignty and integrity safeguards, national security fortifications, foreign relations preservations, public order maintenances, or incitement preventions to cognizable offenses, allowing untrammelled accesses to telecom metadata through Central Monitoring Systems, facial scan fusions from smart city CCTV grids blanketing Delhi transit hubs, or predictive analytics parsing caste-linked mobility patterns during festival crowd controls in Varanasi without the procedural hurdles binding private fiduciaries like e-commerce platforms compelled to honour granular opt-outs.[31]

These exemptions extend to legal rights enforcement and claim adjudications, absolving state processors from storage limitations or correction propagations that clash with evidentiary retentions spanning litigation archives or fraud probes into welfare subsidy siphons, ensuring that transaction histories from fintech ledgers or health narratives digitized in telemedicine silos linking urban specialists with village outposts remain intact for prosecutorial needs without principal vetoes fragmenting investigative chains in cybercrime dockets overwhelming understaffed thanas across Uttar Pradesh heartlands. Unlike corporate entities facing Data Protection Board summons for breach non-notifications, exempted agencies evade such accountabilities, retaining indefinite data hoards for audit trails while implementing baseline security ramparts against external hacks that once flooded voter rolls or vaccination trails into public bazaars, a calibrated asymmetry acknowledging asymmetric threats where ransomware barrages on ministry clouds could cascade disruptions absent fortified perimeters tailored for classified troves.

5.2 National Security and Data Protection

National security considerations permeate the Digital Personal Data Protection Act, 2023, embedding exemptions that prioritize state imperatives over individual privacy entitlements in a geopolitical landscape scarred by cross-border terrorism, cyber incursions from adversarial neighbours, and internal insurgencies demanding real-time intelligence dominance

[31] Daniel J. Solove, Understanding Privacy (Harvard Univ. Press 2008).

through India's sprawling digital infrastructure where Aadhaar biometrics underpin identity verifications, UPI transaction ledgers reveal hawala financing trails, and social media sentiment analytics forecast communal flare-ups during festival seasons or electoral frenzies. Section 17(2)(a) grants the Central Government sweeping authority to notify agencies—from intelligence bureaus to paramilitary forces—for complete exemptions from consent protocols, notice obligations, accuracy maintenances, and principal rights like erasure or grievance redressal when pursuing sovereignty safeguards, integrity preservations, or public order stabilizations, enabling unencumbered fusions of telecom metadata vacuumed by Central Monitoring Systems with facial scans from 10,000-plus CCTV nodes blanketing Delhi's transit corridors to pre-empt suicide bombings or riot escalations in sensitive Uttar Pradesh districts without the procedural delays that judicial warrants impose on routine policing.

This deference acknowledges asymmetric threats post-Mumbai 2008 sieges and Pulwama 2019 blasts, where split-second accesses to encrypted WhatsApp exchanges or location pings from ride-hailing apps tracing suspect mobilities outpace targeted intercepts orthogonal to Puttaswamy's proportionality doctrine demanding minimal intrusions over blanket collections that ensnare innocents in dragnet peripheries. Government processors retain storage liberties indefinitely for evidentiary chains in National Investigation Agency dossiers spanning terror financing probes or cross-border infiltrations, evading fiduciary duties binding private banks compelled to propagate corrections across KYC ecosystems or e-commerce platforms honouring withdrawal revocations mid-sales blitzes, ensuring that genomic profiles from forensic databases or pilgrimage registrations at Kumbh melas fuel predictive nets forecasting radicalization risks without principal vetoes fragmenting intelligence mosaics vital for border securitizations along LOC skirmish zones.

5.3 Risks of Mass Surveillance

Mass surveillance risks under the Digital Personal Data Protection Act, 2023, loom large due to expansive state exemptions that erode individual privacy fortifications while enabling bulk data harvesting justified under national security veils, potentially transforming India's digital polity—saturated with Aadhaar biometrics, UPI transactional deluges, and social media behavioural cascades—into a panopticon where telecom metadata vacuumed by Central Monitoring Systems fuses seamlessly with facial scans from CCTV grids blanketing urban thoroughfares, allowing predictive algorithms to profile dissent trajectories from encrypted WhatsApp clusters or location pings during protest

mobilizations without the granular consents or erasure rights afforded to ordinary citizens contesting corporate dossiers. These provisions risk normalizing indiscriminate collections that ensnare innocents in precautionary dragnets, as agencies bypass notice mandates and accuracy obligations, perpetuating inaccuracies in security troves—like misidentified Northeastern features in biased facial rollouts at airport lounges—that cascade into wrongful detentions or travel blacklists affecting migrant labourers whose mobility patterns inadvertently mirror suspect rhythms, amplifying chilling effects where self-censorship stifles farmers voicing subsidy grievances on rural WhatsApp groups or journalists critiquing policy lapses amid electoral polarizations.

Function creep emerges as a pernicious hazard, where counter-terror rationales morph into routine political monitoring, echoing Pegasus scandals where zero-click infiltrations extracted opposition leaders' chats during farm law agitations, now potentially legitimized through DPDP's sovereignty exemptions lacking judicial warrants or proportionality audits that Puttaswamy jurisprudence demands, enabling mission creep from terror financing probes parsing hawala remittances to precautionary surveillances over minority neighbourhoods during CAA flare-ups. Data retention sans sunset clauses swells indelible archives, thwarting principal erasures as security imperatives clash with rights to purge obsolete health narratives from telemedicine silos or job profiles haunting gig ratings, fostering perpetual digital immortality that haunts activists' footprints across cloud backups even post-threat neutralizations, while re-identification perils from pseudonymized aggregates—like census caste inferences fused with electoral rolls—fuel discriminatory policing skewing against marginalized communities in Uttar Pradesh heartlands.

5.4 Impact of Surveillance on Individual Liberty

Surveillance mechanisms in India, amplified by the Digital Personal Data Protection Act's state exemptions, exert profound erosive pressures on individual liberty, transforming everyday digital interactions—from UPI remittances threading rural economies to social media conversations shaping public discourse—into unwitting contributions to omnipresent monitoring architectures that instil pervasive chilling effects, curtailing spontaneous expressions of dissent, intimate associations, and autonomous decision-making in a republic where Aadhaar biometrics underpin identity assertions while Central Monitoring Systems vacuum telecom metadata streams without the procedural safeguards that Puttaswamy's proportionality doctrine envisions. This omnipresence fosters self-

censorship among journalists hesitating to probe corruption scandals via digitized procurement trails, activists muting farm subsidy critiques on WhatsApp clusters fearing algorithmic flagging, or urban professionals tempering political posts during electoral frenzies lest facial recognition grids blanketing metro corridors correlate online rants with offline mobilities, effectively hollowing Article 19(1)(a)'s free speech guarantees through anticipated repercussions that ripple from precautionary detentions to employment blacklists in gig platforms parsing behavioural profiles for loyalty scores.

Intimate spheres suffer insidious encroachments, as bulk metadata retentions—orthogonal to DPDP's erasure rights for private fiduciaries—immortalize relational graphs mapping spousal communications, familial remittances, or healthcare consultations digitized in telemedicine silos linking village outposts with urban specialists, enabling inferences into private lives where location pings reveal extramarital liaisons or health vitals betray reproductive choices vulnerable to moralistic interventions in conservative heartlands. Joint family dynamics prevalent across India amplify these intrusions, with shared household devices teeming intergenerational footprints blurring individual sanctuaries as parental edtech tracking inadvertently exposes minors' developmental curiosities to security troves, while nominees navigating posthumous erasures clash against indelible archives retained for evidentiary chains spanning decades, perpetuating digital afterlives that haunt kin through caste-linked inferences fused from electoral rolls and census aggregates.

6. CONCLUSION

The Digital Personal Data Protection Act, 2023, distils constitutional privacy into pragmatic mechanisms humanizing algorithmic empires from UPI veins powering informal inclusions to social feeds shaping electoral discourses, navigating surveillance tensions with developmental pragmatism threading legitimate uses without coercive shadows while institutional evolutions promise remedying capacity chasms ensuring principal empowerments cascade across federal expanses. Global lessons infuse iterative refinements fortifying oversight against mission creeps, recalibrating collective shields with individual sanctuaries in data-saturated democracies pulsing from policy sanctums to everyday intimacies across India's vigilance-veiled republic.

BIBLIOGRAPHY

Books

1. Puttaswamy, K.S. (Ed.). (2018). Privacy and the Constitution of India. Oxford University Press, New Delhi.

2. Solove, D.J., & Schwartz, P.M. (2020). Privacy Law Fundamentals. IAPP Publishing, Portsmouth, NH.

3. Cohen, J.E. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press, New York.

4. Basu, D.D. (2020). Introduction to the Constitution of India. LexisNexis, Nagpur.

5. Ray, B.B., & Acharya, M. (2021). Data Protection and Privacy in Healthcare: Indian and Global Perspectives. Springer, Singapore.

6. Saran, S. (2023). Digital India: Technology and Governance. Penguin Random House India, New Delhi.

7. Ganguly, S. (2021). India's Surveillance Dilemma: Security vs. Liberty. Routledge, London.

Statutes

1. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Government of India.

2. Information Technology Act, 2000 (as amended in 2008), Government of India.

3. Indian Telegraph Act, 1885, Government of India.

4. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Government of India.

Reports

1. PRS Legislative Research. (2023). The Digital Personal Data Protection Bill, 2023: A PRS Analysis. PRS India, New Delhi.

2. Internet Freedom Foundation. (2023). Analysis of the Digital Personal Data Protection Act, 2023. IFF, Mumbai.

3. Centre for Internet and Society. (2023). DPDP Act 2023:

Surveillance and Privacy Implications. CIS, Bengaluru.

4. Data Security Council of India. (2024). DPDP Act Compliance Framework Report.

5. DSCI, New Delhi.

6. European Data Protection Board. (2023). Guidelines on Territorial Scope of GDPR.

7. EDPB, Brussels.

8. Status of Policing in India Report 2023. Surveillance and the Question of Privacy. Commonwealth Human Rights Initiative, New Delhi.

9. Ministry of Electronics and Information Technology. (2024). DPDP Rules Draft Report. MeitY, New Delhi.

Articles And Papers

1. Chander, A., & Lê, U.P. (2023). "Data Nationalism and DPDP Exemptions." Harvard International Law Journal, 64(2), 345-378.

2. Malhotra, A. (2024). "Surveillance Backdoors in India's DPDP Act." Indian Journal of Law and Technology, 15(1), 89-112.

3. Kuner, C. (2023). "DPDP Act vs GDPR: Adequacy Prospects." International Data Privacy Law, 13(4), 289-305.

4. Ray, S. (2024). "Puttaswamy and DPDP Surveillance Exemptions." Economic and Political Weekly, 59(12), 34-40.

5. Ganguly, S. (2024). "National Security Overrides in DPDP." India Quarterly, 80(1), 56-72.

6. Basu, T. (2023). "Children's Data Under DPDP Act." Journal of Indian Law and Society, 14(2), 112-135.

7. Saran, S. (2023). "Digital Sovereignty and Cross-Border Flows." India Review, 22(3), 267-285.

8. Jain, R. (2023). "Data Protection Board Independence." National Law School of India Review, 35(2), 189-210.

Websites Referred

1. PRS Legislative Research. (2026). "Digital Personal Data Protection Bill, 2023."

https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

2. Internet Freedom Foundation. (2023). "DPDP Act Analysis." https://internetfreedom.in/dpdpact-2023/

3. Data Protection Board of India (Official Portal). (2026). https://dataprotectionboard.gov.in/

4. European Data Protection Board. (2023). "GDPR Guidelines." https://edpb.europa.eu/