IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CONSTITUTIONAL LIMITS ON DIGITAL SURVEILLANCE IN INDIA: PRIVACY, POWER, AND THE MODERN STATE UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Avinandini Sinha Vrinda Sambhava LL.B. 2nd Semester

MDU-CPAS, Gurugram

Abstract

The digital expansion of state power has generated profound friction between executive surveillance architecture and the fundamental right to privacy recognized in *Justice K.S. Puttaswamy v. Union of India*. This article critically examines the Digital Personal Data Protection Act, 2023 (hereinafter referred as DPDP Act), arguing that while the statute ostensibly safeguards informational privacy, it simultaneously institutionalizes expansive executive surveillance capabilities. Employing a doctrinal and comparative constitutional methodology, this research interrogates the DPDP framework against the tripartite proportionality standard embedded in Articles 14, 19, and 21 of the Indian Constitution.

The analysis specifically dissects the blanket exemptions under Section 17 of the DPDP Act, which grant the state broad, unregulated discretion to bypass data protection obligations in the name of national security and public order. By evaluating the potential chilling effect on democratic dissent and the absence of robust independent judicial oversight, the article demonstrates that the current legislative framework skews the liberty-security balance heavily toward the state. Ultimately, the paper concludes that without integrating rigorous procedural safeguards and strict necessity tests, the DPDP Act risks normalizing a surveillance-compatible constitutional order, thereby rendering the promise of informational self-determination largely symbolic.

Keywords:

Surveillance Constitutionalism; Proportionality Doctrine; Digital Personal Data Protection Act; Executive Overreach; Chilling Effect; Constitutional Morality; Article 21.

Introduction

In the contemporary digital age, the modern state has undergone a profound transformation, increasingly relying on data-driven frameworks to administer governance. The ubiquity of digital footprints has enabled the state to shift from targeted physical observation to pervasive, automated digital surveillance, functioning on preventive and predictive logic. This transition has fundamentally reconfigured the relationship between the citizen and the state. In a constitutional democracy, where the rule of law mandates a limited government, mass surveillance presents an existential threat to democratic accountability and individual liberty. When surveillance systems operate without robust transparency or procedural constraints, they engender a chilling effect on the freedom of speech, dissent, and association, thereby striking at the very foundation of an open, pluralistic society.

To shield the individual from the encroaching gaze of the state, Indian constitutional jurisprudence has formally entrenched the right to privacy as an inalienable fundamental right, intrinsic to the guarantee of life and personal liberty under Article 21 of the Constitution. At the heart of this constitutional protection lies the doctrine of informational privacy, which recognizes an individual's right to informational self-determination the ability to control the collection, use, and disclosure of personal data. Privacy, therefore, operates as a normative bulwark against arbitrary state intrusion, ensuring that human dignity and decisional autonomy are not subsumed by totalitarian excesses.

Responding to the imperatives of the digital economy and the constitutional mandate to protect informational privacy, India has embraced a statutory framework of data governance through the Digital Personal Data Protection Act, 2023. The legislation ostensibly seeks to balance the individual's right to protect personal data with the necessity of processing such data for lawful purposes. It mandates consent mechanisms, imposes obligations on data fiduciaries, and establishes an adjudicatory board. However, this legislative framework introduces profound constitutional frictions concerning the tension between individual liberty and the expansion of state power.

Current academic and policy discourse surrounding the DPDP Act predominantly evaluates its impact on commercial data processing, corporate compliance, and consumer rights. A critical research gap exists in examining the statute through the lens of surveillance constitutionalism. Specifically, there is an exigent need to doctrinally interrogate how the DPDP Act navigates the boundaries of executive power, the architecture of state surveillance, and the structural limitations imposed on constitutional privacy.

This article advances the central constitutional thesis that the DPDP Act, 2023, while formally acknowledging data protection, simultaneously institutionalizes and expands the surveillance capabilities of the Indian state. By incorporating broad, unregulated exemptions under Section 17 for the state and its instrumentalities, the Act structurally bypasses the rigorous requirements of procedural safeguards and the constitutional doctrine of proportionality. This paper critically analyzes whether these sweeping executive powers skew the liberty-security balance, risking the dilution of informational privacy into a mere illusion. Ultimately, the article evaluates whether the current legislative design threatens to transition the Indian democratic republic into a surveillance-compatible constitutional order.

Research Questions

To doctrinally interrogate the intersection of the Digital Personal Data Protection Act, 2023, and the evolving jurisprudence on surveillance constitutionalism, this article investigates the following central constitutional questions:

1. To what extent do the sweeping executive exemptions granted to state instrumentalities under Section 17 of the DPDP Act, 2023, violate the tripartite doctrine of proportionality specifically the tests of strict necessity and narrow tailoring established in *Justice K.S. Puttaswamy v. Union of India*?
2. Does the statutory architecture of the DPDP Act genuinely operationalize the fundamental right to informational self-determination, or does it structurally normalize an asymmetry of power by institutionalizing unregulated executive discretion to bypass data protection obligations?
3. In the absence of robust independent judicial oversight over digital interception, how does the aggregation of state surveillance capabilities generate a constitutional chilling effect on the fundamental freedoms of speech, expression, and association guaranteed under Article 19(1)(a) and 19(1)(c)?

4. How does the contemporary Indian surveillance framework negotiate the constitutional friction between the legitimate security imperatives of the modern state and the inviolability of personal liberty under Article 21, and does the DPDP Act impermissibly skew this balance toward executive overreach?
5. Viewed through the lens of comparative constitutionalism and global data protection paradigms (such as the strict scrutiny applied to data retention in *Digital Rights Ireland*), do the blanket national security exemptions in the DPDP Act fail to satisfy the threshold of procedural due process essential for a lawful surveillance regime?
6. Does the prevailing legislative and administrative framework risk facilitating the transition of the Indian democratic republic into a surveillance-compatible constitutional order, thereby rendering the judicially recognized guarantee of constitutional privacy merely symbolic?

Research Methodology

This article adopts a rigorous doctrinal and critical constitutional methodology to evaluate the structural intersection of state surveillance capabilities and informational privacy. The research is fundamentally anchored in constitutional interpretation, employing a purposive and dynamic approach to assess the Digital Personal Data Protection Act, 2023, against the fundamental rights architecture of the Indian Constitution. Rather than providing a descriptive summary of the statutory framework, the methodology relies on critical legal analysis to doctrinally interrogate the asymmetries between executive discretion specifically the blanket exemptions under Section 17 of the Act and the constitutional limitations on state power.

The primary foundation of this analysis rests upon the text of the Constitution of India, particularly Articles 14, 19, and 21, alongside an extensive examination of judicial precedents. By undertaking a deep doctrinal exegesis of the Supreme Court's privacy jurisprudence, the study extracts the judicially evolved tests of strict necessity, narrow tailoring, and proportionality, applying them directly to the contemporary digital surveillance regime. Furthermore, the article integrates comparative constitutional analysis to contextualize the Indian surveillance architecture within global democratic norms. This primary legal analysis is supplemented by an array of secondary sources, including authoritative constitutional treatises, scholarly research articles, and academic commentary on digital constitutionalism and the modern surveillance state.

Constitutional Framework of Privacy, Liberty, and Surveillance in India

The constitutional architecture of India is fundamentally premised on the doctrine of limited government and the rule of law, which operate as structural bulwarks against the totalitarian excesses of a surveillance state. The Constitution does not merely delineate the contours of state power; it strictly circumscribes them, affirming that the state is not an absolute sovereign but a trustee of the people. In a democratic republic, the rule of law rejects the conception of a Dual State where governmental action enjoys immunity from legal control; instead, it demands that every executive and legislative intrusion into individual liberty be sanctioned by law and constrained by constitutional limitations.

To doctrinally evaluate the limits of state surveillance, it is imperative to analyze the normative interplay between Articles 14, 19, and 21 of the Constitution. Indian constitutional jurisprudence has evolved significantly from the early textualist interpretation in *A.K. Gopalan v. State of Madras*, which treated fundamental rights as isolated silos. This theory of exclusivity was dismantled by the Supreme Court in *R.C. Cooper v. Union of India* and subsequently in *Maneka Gandhi v. Union of India*, which established that fundamental rights form an integrated, cohesive code. Consequently, any state surveillance architecture must simultaneously satisfy the rigorous constitutional mandates of equality, freedom, and personal liberty.

Article 21 mandates that no person shall be deprived of life or personal liberty except according to the procedure established by law. While the framers consciously omitted the American due process clause to avoid judicial vagaries, the jurisprudential metamorphosis following *Maneka Gandhi* infused the concept of substantive and procedural due process into the Indian constitutional fabric. For a surveillance measure to be constitutionally valid, the mere existence of enacted law is insufficient. The procedure prescribed by such law must be right and just and fair and cannot be fanciful, oppressive, or arbitrary. Thus, state surveillance cannot be sustained by executive fiat or opaque administrative guidelines; it requires a legislative framework that provides robust procedural safeguards against unauthorized intrusion.

Article 14 ensures that state action is informed by reason and is free from the vice of arbitrariness. As articulated in *E.P. Royappa v. State of Tamil Nadu*, equality and arbitrariness are sworn enemies; where an act is arbitrary, it is inherently unequal and thus violates the rule of law. This equalizing principle permeates Art 21, meaning that any law authorizing surveillance must inherently lack arbitrariness. Furthermore, the Supreme Court has expanded this doctrine to include manifest arbitrariness as a ground for invalidating legislation. A surveillance regime that confers unregulated or unfettered discretion upon the executive, lacking clear guidelines or independent oversight mechanisms, suffers from manifest arbitrariness and falls foul of Art 14.

Surveillance strikes directly at the heart of the freedoms guaranteed under Article 19, particularly the freedom of speech and expression under Article 19(1)(a) and the freedom of movement under Article 19(1)(d). The psychological restraint engendered by continuous monitoring casts a shroud of surveillance, forcing citizens into expected grooves of behaviour. This phenomenon is constitutionally recognized as the chilling effect, which poses a grave danger to democratic participation, dissent, and the unhindered fulfilment of personal autonomy.

To justify any restriction on Article 19 freedoms, the state must demonstrate that the surveillance measure falls within the permissible grounds of clauses (2) to (6) and constitutes a reasonable restriction. The ultimate metric for determining this reasonableness is the doctrine of proportionality, which requires the state to strike a delicate balance between individual liberties and legitimate state interests. As synthesized in *Modern Dental College and Research Centre v. State of M.P.* and reaffirmed in *K.S. Puttaswamy*, proportionality mandates a four-pronged inquiry: (i) the measure restricting the right must serve a legitimate state aim; (ii) the means adopted must be rationally connected to the fulfilment of that purpose; (iii) there must be no less restrictive but equally effective alternative (the test of necessity); and (iv) the measure must not have a disproportionate impact on the right-holder (balancing stage).

In the context of state surveillance, the proportionality standard dictates that the indiscriminate or blanket collection of data is inherently unconstitutional. The state must prove that its intelligence-gathering mechanisms are narrowly tailored, strictly necessary for a compelling public interest (such as national security or the prevention of serious crime), and accompanied by independent oversight. Without these strict constitutional guardrails, surveillance power invariably transitions from a tool of security to an instrument of democratic subversion.

Evolution of Privacy Jurisprudence in India

The trajectory of privacy jurisprudence in India reflects a profound jurisprudential metamorphosis, transitioning from an era of strict textual formalism to a regime of transformative constitutionalism. In its formative decades, the Supreme Court of India was reluctant to explicitly recognize a fundamental right to privacy, constrained by a positivist reading of the Constitution. In *M.P. Sharma v. Satish Chandra*, an eight-judge bench declined to import the principles of the American Fourth Amendment into the Indian constitutional framework, concluding that the drafters had deliberately omitted an explicit guarantee of privacy against state search and seizure under Article 20(3).

This restrictive paradigm persisted in *Kharak Singh v. State of U.P.*, where a six-judge bench examined police surveillance regulations. The majority exhibited a doctrinal paradox: while it struck down nocturnal domiciliary visits as a violation of ordered liberty and the sanctity of the home, it simultaneously maintained that the right to privacy was not a constitutionally guaranteed right. However, the intellectual groundwork for future evolution was laid by Justice Subba Rao's prophetic dissent. He persuasively argued that privacy is an essential ingredient of personal liberty under Article 21, cautioning that psychological restraints and encroachments on private life limit freedom just as severely as physical confinement.

As Indian constitutional interpretation moved away from the siloed approach of the 1950s toward an integrated reading of fundamental rights, the judicial posture on privacy softened. In *Gobind v. State of M.P.*, the Court proceeded on the assumption that a limited right to privacy emanates from the penumbral zones of Articles 19 and 21. Significantly, *Gobind* introduced the requirement that any state intrusion into privacy must be justified by a compelling State interest and must be narrowly tailored, thereby planting the early seeds of the proportionality doctrine in Indian privacy law. This evolutionary arc gained structural clarity in *PUCL v. Union of India*, where the Court unequivocally held that telephonic conversations constitute an intimate facet of a person's private life. By shielding communication privacy against arbitrary executive wiretapping, *PUCL* formally anchored the right to privacy within the protective ambit of Article 21, insisting on stringent procedural safeguards against executive overreach.

The piecemeal and assumed nature of constitutional privacy was definitively laid to rest by the landmark nine-judge bench decision in *Justice K.S. Puttaswamy v. Union of India*. Explicitly overruling the early orthodoxies of *M.P. Sharma* and *Kharak Singh*, the Court declared privacy to be an inalienable, natural right inherent in the human personality. *Puttaswamy* delinked privacy from mere spatial or proprietary constructs, elevating it to the constitutional core of human dignity. The judgment systematically categorized privacy into three distinct yet overlapping domains: spatial control, decisional autonomy, and informational control.

Crucially, *Puttaswamy* established informational privacy as a vital constitutional shield in the digital age. The Court recognized that in an era of data ubiquity, the aggregation of electronic tracks can construct exhaustive profiles of an individual's personal life, tastes, and political affiliations. Unauthorized state access to this aggregated data destroys individual autonomy and engenders a chilling effect on democratic dissent. Consequently, the Court mandated that any legislative or executive encroachment upon privacy must survive a rigorous tripartite standard of proportionality. The state must demonstrate: (i) legality (the existence of a valid law); (ii) a legitimate state aim (to preclude manifest arbitrariness); and (iii) proportionality (a rational nexus between the object and the means, ensuring that the state adopts the least restrictive measure to impair the right as little as possible).

Ultimately, this doctrinal evolution represents a transition from viewing privacy as a mere common law privilege to recognizing it as an indispensable condition for the realization of fundamental freedoms. The jurisprudence now demands that the state not only refrain from arbitrary intrusions but also fulfill its positive obligation to protect the informational self-determination of its citizens.

Critical Constitutional Analysis of the Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, was ostensibly intended to fulfil the positive constitutional obligation of the Indian State to secure informational privacy, a mandate crystallized in *Justice K.S. Puttaswamy v. Union of India*. However, a rigorous doctrinal evaluation reveals a statutory architecture that fundamentally prioritizes the facilitation of data processing and the centralization of state power over the protection of individual constitutional liberties. Rather than establishing a resilient rights-based framework, the Act structurally embeds executive dominance, raising profound questions regarding its compatibility with the constitutional guarantees of Articles 14 and 21.

At the conceptual core of informational privacy is the doctrine of informational self-determination the inviolable right of an individual to control the collection, dissemination, and processing of their personal data. Facially, Section 6 of the DPDP Act acknowledges this by mandating that a Data Principal’s consent must be free, specific, informed, unconditional and unambiguous with a clear affirmative action. However, this statutory commitment to decisional autonomy is heavily diluted by the parallel framework of certain legitimate uses under Section 7.

Section 7 effectively overrides the requirement of consent when the State or its instrumentalities process data for the provision of any subsidy, benefit, service, certificate, license, or permit. Furthermore, data processing is deemed legitimate for the performance of any state function under law or in the interest of sovereignty, integrity, and security of the State. By classifying expansive state data collection as a legitimate use, the Act creates a structural presumption in favor of the State, functionally bypassing the individual’s right to consent. Constitutionally, this framework fails the *Puttaswamy* necessity and narrow-tailoring tests. Instead of requiring the State to demonstrate a compelling necessity for each category of non-consensual data processing, the Act statutorily normalizes indiscriminate data assimilation. The resultant architecture undermines informational autonomy, reducing the citizen to a passive subject of data-driven governance rather than a sovereign rights-holder.

The DPDP Act imposes a series of obligations on Data Fiduciaries under Section 8, including the implementation of appropriate technical and organizational measures, security safeguards to prevent data breaches, and the obligation to erase data once its specified purpose is served. Significant Data Fiduciaries are subjected to additional compliance requirements, such as appointing a Data Protection Officer and an independent data auditor.

While these obligations create a superficial matrix of corporate accountability, the statute suffers from a glaring remedial vacuum. Crucially, the DPDP Act repeals Section 43A of the Information Technology Act, 2000, which previously provided a statutory right to compensation for individuals affected by a data fiduciary's failure to protect sensitive personal data. Under the new regime, the Data Protection Board of India is empowered to impose severe monetary penalties for non-compliance, but these penalties are credited entirely to the Consolidated Fund of India. The Act contains no provision for compensating the aggrieved Data Principal.

This statutory omission fundamentally offends the constitutional principle of *ubi jus ibi remedium* (where there is a right, there must be a remedy). By transforming data breaches from a violation of individual constitutional privacy into a mere regulatory infraction punishable by fines payable to the State, the Act strips informational privacy of its compensatory deterrent. A privacy framework that penalizes corporate negligence without restoring the victim fails to genuinely protect the citizen's Article 21 rights.

A constitutionally adequate surveillance and data protection regime necessitates an independent regulatory authority capable of shielding citizens from both corporate exploitation and state overreach. The DPDP Act entirely fails to satisfy this institutional requirement. The adjudicatory body created under the Act, the Data Protection Board of India, lacks structural and functional independence. According to Sections 19 and 20 of the Act, the Chairperson and Members of the Board are appointed exclusively by the Central Government, and their tenure, terms, and conditions are dictated by executive rule-making.

In a constitutional democracy, where the State is the largest data fiduciary and the primary entity capable of mass surveillance, investing the executive with absolute control over the data protection regulator violates the doctrine of separation of powers and the rule of law. Without robust, independent, and judicial oversight, the Board is rendered an extension of the executive apparatus rather than an impartial guardian of fundamental rights. This institutional design directly contravenes the comparative constitutional standards established in jurisdictions with mature data protection frameworks, such as the European Union's GDPR, which mandate strictly independent supervisory authorities to oversee state and non-state data processing.

Finally, the statute fails to grapple with the complexities of modern technological governance, specifically algorithmic decision-making and artificial intelligence. The DPDP Act applies to automated processing of digital personal data but lacks specific safeguards against algorithmic bias or provisions mandating human review of automated decisions that significantly affect Data Principals. As the State increasingly relies on algorithmic profiling for predictive governance and resource allocation, the failure to mandate algorithmic transparency or the right to an explanation renders the legislation constitutionally anachronistic.

In totality, a critical constitutional analysis of the DPDP Act, 2023, demonstrates that the statute fails to operationalize the *Puttaswamy* mandate. Rather than constructing a rights-based bulwark against informational asymmetry, the Act codifies broad executive discretion, dilutes the consent architecture, removes compensatory remedies, and establishes a subordinate regulatory board. Consequently, the Act does not cure the constitutional friction between individual liberty and state power; instead, it legally fortifies the digital administrative state, leaving the fundamental right to informational privacy inadequately protected against systematic state and corporate encroachment.

Section 17 Exemptions and Expansion of Executive Surveillance Power

Section 17(2)(a) of the Digital Personal Data Protection (DPDP) Act, 2023, empowers the Central Government to exempt any instrumentality of the State from the application of the Act on broad grounds, including the sovereignty and integrity of India, security of the State, and maintenance of public order, Constitutionally, this provision operates as a statutory carte blanche, carving out an expansive zone of immunity for the state's surveillance architecture. By granting the executive the unregulated prerogative to bypass fundamental data protection obligations such as purpose limitation, data minimisation, and storage limitation Section 17 institutionalizes a severe asymmetry of power. The constitutional peril lies not merely in the existence of an exemption, but in its structural absoluteness, which permits the state to consolidate vast repositories of personal data without concurrent procedural safeguards or transparency,

The most glaring constitutional deficit of Section 17 lies in its failure to satisfy the proportionality standard entrenched in *Justice K.S. Puttaswamy v. Union of India*. While national security and public order are undoubtedly legitimate state aims, the doctrine of proportionality strictly mandates that the means adopted must be narrowly tailored to impair the right as little as possible. Section 17(2)(a) eschews targeted, case-by-case exemptions in favor of wholesale, blanket immunities for notified instrumentalities. This dragnet approach inherently violates the necessity and least restrictive means tests. As held in *Puttaswamy*, an invasion of privacy must be strictly proportionate to the need for such interference. An overarching exemption that extinguishes the applicability of the entire data protection framework for state agencies is manifestly disproportionate, as it facilitates indiscriminate surveillance and data aggregation without requiring the state to prove that a less restrictive alternative was unavailable.

Finally, the architecture of Section 17 amounts to an excessive delegation of legislative power. While the legislature can delegate ancillary functions, it cannot abdicate its essential legislative function by conferring unguided discretion upon the executive. By leaving the determination of both the exempted entities and the extent of the exemption entirely to executive notification, the DPDP Act evades constitutional accountability. It enables the executive to continually expand its digital surveillance footprint unchecked, transforming the statute from a shield for informational privacy into a sword for state monitoring. Without integrating rigorous judicial oversight and strict necessity tests directly into the statutory text, Section 17 dismantles the carefully calibrated constitutional limits on state power, authorizing the expansion of executive surveillance under the guise of statutory exemption.

Proportionality, Necessity, and Constitutional Validity of Digital Surveillance

To constitutionally validate any state intrusion into fundamental liberties, the Supreme Court of India has firmly entrenched the doctrine of proportionality as the ultimate metric of judicial review. As articulated in the nine-judge bench decision in *Justice K.S. Puttaswamy v. Union of India* and subsequently elaborated in the Aadhaar constitutional challenge, any encroachment upon privacy must survive a rigorous touchstone. The Supreme Court, building upon this foundation in *Anuradha Bhasin v. Union of India*, adopted the four-pronged proportionality test derived from Aharon Barak's structural framework: (i) the measure must have a legitimate state goal; (ii) there must be a rational nexus between the measure and the goal; (iii) the measure must be strictly necessary, meaning there exists no less restrictive alternative; and (iv) the measure must survive the balancing stage, ensuring the restriction is proportionate to the social importance of the objective,,.

The necessity prong demands that the state adopt the least intrusive measure capable of attaining its desired objective, ensuring that the fundamental right is impaired as little as possible. By statutorily granting wholesale, blanket exemptions to state instrumentalities, the DPDP framework fundamentally abandons the principle of data minimization in favor of unregulated data assimilation.

Comparative constitutional jurisprudence provides crucial guidance on this deficiency. In *Digital Rights Ireland*, the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive precisely because it mandated blanket, undifferentiated data retention. The CJEU observed that indiscriminate data collection, without objective criteria limiting access to what is strictly necessary for preventing serious crime, constitutes a disproportionate interference with privacy, Similarly, in *Tele2 Sverige AB*, the CJEU ruled that national legislation permitting general and indiscriminate retention of electronic communications applies to persons for whom there is no evidence suggesting a link to criminal conduct, thereby violating the necessity mandate. The DPDP Act mimics this fatal overbreadth. Rather than prescribing targeted, case-by-case intelligence gathering, the statutory exemptions effectively treat the entire populace as subjects of continuous monitoring, failing the necessity test by discarding less restrictive alternatives.

The final, and most critical, component of the proportionality inquiry is the balancing stage, which evaluates whether the deleterious effects of the measure are proportionate to the importance of the state's objective. This stage is inextricably linked to the presence of procedural guarantees against abuse. As the Supreme Court warned in *Anuradha Bhasin*, substantive justice under fundamental rights analysis cannot be achieved if procedural justice is sacrificed on the altar of state expediency.

The total absence of procedural safeguards in the DPDP Act such as prior judicial scrutiny, clear limits on the duration of data retention by intelligence agencies, and stringent protocols for data destruction renders the law structurally imbalanced. By subordinating constitutional privacy to opaque administrative discretion, the DPDP Act fails to maintain the equitable balance between the state's security imperatives and the individual's fundamental right to informational self-determination. Consequently, the unchecked surveillance powers sanctioned by the DPDP framework do not pass constitutional muster under the doctrine of proportionality.

Chilling Effect, Democratic Participation, and Constitutional Freedoms

The institutionalization of digital surveillance under the Digital Personal Data Protection Act (DPDP Act), 2023, transcends the paradigm of individual informational privacy, manifesting as a grave structural constitutional concern that strikes at the very core of India's democratic culture. When the state possesses the technological capacity to aggregate metadata and construct exhaustive profiles of citizens' political, religious, and social associations without the friction of traditional physical surveillance, the resulting power asymmetry fundamentally re-engineers the relationship between the governing and the governed. This architecture of monitoring does not merely infringe upon discrete constitutional rights; it threatens the structural probity of a liberal democratic order by silently influencing behaviour and stifling the unhindered exercise of fundamental freedoms.

The most pernicious consequence of pervasive state monitoring is the generation of a psychological restraint on the citizenry, triggering the chilling effect doctrine deeply embedded in free speech jurisprudence. As articulated by the Supreme Court in *Shreya Singhal v. Union of India*, laws that cast a wide and vaguely defined net over digital communications inevitably trap protected and innocent speech, generating a chilling effect on the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a). The Court emphasized that the law must not be utilized in a manner that produces a chilling effect on legitimate expression, noting that a culture of open dialogue and the free flow of opinions are essential prerequisites to sustain the collective life of an informed citizenry. When citizens operate under the panoptic anxiety of constant state observation, they inherently self-censor. This coerced conformity suppresses heterodox thought and controversial opinions, irreparably damaging the democratic marketplace of ideas.

This chilling effect reverberates severely through the realms of journalism, political dissent, and civil society participation. The vitality of a free press relies intrinsically on the ability of journalists to maintain confidential sources and conduct investigations free from the threat of state espionage. unregulated executive surveillance capabilities, such as those facilitated by the broad exemptions under the DPDP Act, jeopardize these protections by leaving digital footprints and communications vulnerable to state aggregation. Similarly, political participation and the freedom of association under Article 19(1)(c) are deeply compromised when the state can map the networks of political opponents and dissenting groups. A democratic polity demands that individuals possess the autonomy to organize and challenge governmental policies without the apprehension of being constantly watched and catalogued.

Ultimately, the normalization of state surveillance offends the doctrine of constitutional morality. Constitutional morality demands the preservation of a pluralistic, heterogeneous society where minority voices, distinct identities, and unpopular dissent are shielded from majoritarian homogenization and authoritarian coercion. By its very nature, an intrusive surveillance regime seeks to normalize behavioural patterns and enforce societal conformity through the implicit threat of monitoring. It reflects a punitive, moralistic view of governance that treats the populace as permanent subjects of suspicion rather than sovereign rights-holders. A constitutional democracy cannot survive if its citizens are encaged within invisible threads of digital tracking, rendering their fundamental liberties contingent upon state benevolence. Therefore, subjecting state surveillance power to rigorous constitutional constraints is not merely a question of protecting personal data; it is an existential imperative for preserving the democratic, anti-authoritarian soul of the Indian Constitution.

Comparative Constitutional Perspectives on Privacy and Surveillance

To situate India's surveillance architecture within the global discourse on digital constitutionalism, a doctrinal comparison with mature privacy jurisdictions exposes the structural inadequacies of the Digital Personal Data Protection (DPDP) Act, 2023. Global constitutional courts have increasingly transitioned from a culture of executive authority to a culture of justification, imposing stringent substantive and procedural constraints on state data collection.

In German constitutional jurisprudence, the Federal Constitutional Court's landmark *Volkszählungsurteil* (Federal Census Act Case) formally entrenched the doctrine of informational self-determination as an emanation of human dignity and personal freedom under Articles 1(1) and 2(1) of the Basic Law. The Court mandated that data processing must strictly adhere to the principle of proportionality, warning that a social order where individuals cannot ascertain who knows what about them is incompatible with a democratic society. Conversely, the DPDP Act's blanket exemptions under Section 17(2)(a) statutorily preclude informational self-determination by liberating state instrumentalities from the obligations of transparency and purpose limitation.

Similarly, European Union privacy jurisprudence demands rigorous scrutiny of executive surveillance. In *Digital Rights Ireland*, the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive, ruling that the indiscriminate and generalized retention of metadata without objective criteria limiting state access constitutes a disproportionate interference with Articles 7 and 8 of the EU Charter. The CJEU established that surveillance measures must be strictly necessary, narrowly tailored, and subject to prior review by an independent administrative or judicial body. Furthermore, the European Court of Human Rights in *S and Marper v. United Kingdom* unequivocally rejected the blanket retention of biometric data as failing to strike a fair balance between public interest and private life. While the EU's General Data Protection Regulation (GDPR) mandates strict necessity and independent oversight even for state security processing, India's DPDP framework lacks both an independent supervisory authority to pre-screen interception requests and a statutory prohibition against indiscriminate data aggregation.

American digital privacy jurisprudence offers equally critical doctrinal lessons regarding procedural safeguards. In *Carpenter v. United States*, the U.S. Supreme Court profoundly curtailed the third-party doctrine, recognizing that individuals possess a legitimate expectation of privacy in the exhaustive chronicle of their physical movements captured by historical cell-site location information (CSLI). The Court ruled that the acquisition of such data constitutes a Fourth Amendment search, mandating the state to secure a judicial warrant supported by probable cause rather than relying on mere statutory authorization. *Carpenter* doctrinally establishes that pervasive digital tracking by the state requires independent, prior judicial authorization.

Contemporary Challenges and Constitutional Concerns

The intersection of digital surveillance capabilities, expansive data processing statutes like the Digital Personal Data Protection Act, 2023, and biometric aggregation frameworks presents unprecedented challenges to the constitutional order. As the state transitions toward a technology-driven administrative apparatus, several unresolved constitutional concerns emerge, threatening to permanently alter the relational dynamics between the sovereign and the citizen.

Modern surveillance and state administration increasingly rely on complex digital technologies, including algorithmic monitoring, metadata analysis, and cross-platform data aggregation. A primary constitutional concern is the technological opacity inherent in these systems, which frequently operate as black boxes. This opacity makes it nearly impossible for citizens to comprehend how their data is collected, analysed, or utilized for automated decision-making.

The prevailing data governance and surveillance frameworks suffer from a severe concentration of power within the executive, heavily reliant on delegated legislation and executive discretion. Oversight mechanisms are predominantly internal and executive-controlled, exhibiting a glaring absence of independent or judicial involvement. For instance, authorities tasked with administering major data projects often lack the institutional autonomy required to credibly enforce data protection norms or penalize state transgressions.

Perhaps the most profound long-term implication for constitutional democracy is the normalization of mass surveillance. Traditional surveillance mechanisms were confined to targeted criminal investigations requiring an individualized threshold of suspicion. However, modern digital governance relies on a preventive and predictive logic, where data is indiscriminately collected and analyzed to identify potential threats or behavioral patterns. This paradigm shift blurs the constitutionally vital distinction between suspected offenders and ordinary citizens, subjecting the entire populace to continuous observation.

This normalizes a regime where citizens are treated as permanent subjects of suspicion, ensnared in the invisible threads of a biometric and digital web. Such pervasive monitoring exerts a chilling effect on the fundamental rights of speech, dissent, and association. Ultimately, unchecked executive surveillance and the absence of comprehensive, rights-based data protection laws risk undermining the constitutional balance between state authority and individual rights. If privacy is not vigorously reaffirmed as a structural safeguard, democratic citizenship will be critically weakened, and the constitutional guarantee of liberty will be reduced to a fragile illusion.

Recommendations and Constitutional Safeguards

To salvage the Digital Personal Data Protection Act, 2023, from the vice of unconstitutionality, the legislative architecture must be re-engineered to structurally integrate the *Puttaswamy* proportionality mandate. Foremost, the blanket executive exemptions under Section 17 must be repealed and replaced with a regime of narrowly tailored, case-by-case authorizations. Any state interception, algorithmic monitoring, or access to personal data must require *prior judicial oversight*, mirroring the stringent warrant requirements entrenched in comparative constitutional jurisprudence. Such a procedural guarantee ensures that executive surveillance is independently subjected to the strict necessity and least-restrictive-means tests before the constitutional threshold of privacy is breached.

Furthermore, the Data Protection Board of India must be emancipated from executive dominance. To satisfy the structural demands of the rule of law, the Board must be reconstituted as a functionally independent regulatory institution. Equipping the Board with adjudicatory autonomy and insulating its appointment process from unilateral executive control is imperative for it to credibly oversee the State, which remains the largest data fiduciary. Statutorily, the Act must be amended to expressly bind state instrumentalities to the doctrines of data minimization and purpose limitation, categorically prohibiting the indiscriminate aggregation of citizen metadata.

Finally, to mitigate the opacity of contemporary technological governance, the legal framework must mandate algorithmic transparency and institute rigorous parliamentary accountability mechanisms. Establishing a permanent parliamentary oversight committee to review the deployment of surveillance technologies and intelligence-gathering operations is indispensable to restoring democratic equilibrium. By anchoring data governance in these substantive and procedural constitutional safeguards, the Indian legal framework can genuinely secure informational self-determination and prevent the normalization of a surveillance-compatible state.

Conclusion

The digital transformation of the Indian state has fundamentally reconfigured the relationship between the sovereign and the citizen, risking the repositioning of the individual from a sovereign rights-holder to a subject of perpetual dataveillance. This article has demonstrated that the Digital Personal Data Protection Act, 2023, fails to cure the constitutional friction between state power and informational privacy. Rather than functioning as a robust bulwark against executive overreach, the statutory framework structurally enables the expansion of state surveillance capabilities. By embedding unregulated exemptions under Section 17 and deliberately omitting independent prior judicial oversight, the Act subordinates the fundamental right to informational self-determination to the expansive imperatives of state security and administrative expediency.

Evaluated through the rigorous tripartite proportionality standard established in *Justice K.S. Puttaswamy v. Union of India*, the current data governance architecture is constitutionally deficient. It upsets the delicate liberty-security balance by sacrificing structural due process at the altar of technological governance. In a constitutional democracy, digital administration cannot be permitted to metamorphose into an instrument of algorithmic monitoring and behavioral control. The chilling effect generated by unchecked digital power threatens the foundational democratic guarantees of free speech, political participation, and individual autonomy.

The future of Indian privacy jurisprudence now hinges on the constitutional courts' willingness to strictly enforce the doctrines of necessity and narrow tailoring against state data processing. For the judicially recognized right to privacy to retain its normative vitality, it must be insulated from the shifting sands of majority governments. Ultimately, a surveillance-compatible state is inherently incompatible with a liberal constitutional republic. If the Constitution is to remain a resilient shield against totalitarian excesses, preserving the inviolability of the human personality against digital aggregation must be recognized not merely as a statutory objective, but as the defining constitutional imperative of the modern era.

References

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
3. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
4. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
6. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
7. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.
8. Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722.
9. S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574.
10. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.
11. ADM Jabalpur v. Shivkant Shukla, (1976) 2 SCC 521.
12. Selvi v. State of Karnataka, (2010) 7 SCC 263.
13. State of Uttar Pradesh v. Raj Narain, (1975) 4 SCC 428.
14. Carpenter v. United States, 585 U.S. 296 (2018).
15. Digital Rights Ireland Ltd v. Minister for Communications, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238.
16. Usha Tandon C Neeraj Kumar Gupta, Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023, 6(2) Legal Issues in the Digital Age 87 (2025).
17. Karishma Sundara C Nikhil Narendran, The Digital Personal Data Protection Act, 2023: Analysing India's Dynamic Approach to Data Protection, 24(5) Computer Law Review International 129 (2023).
18. Sana Athar et al., Nobody Should Control the End User: Exploring Privacy Perspectives of Indian Internet Users in Light of DPDPA, Max Planck Institute for Informatics C IIT Bombay (2024).
19. Yvonne McDermott, Conceptualizing the Right to Data Protection in an Era of Big Data, Big Data C Society 1 (2017).
20. Aditi Kanoongo C Harshitha Adari, Unpacking India's Digital Personal Data Protection Act: A New Dawn or a False Start?, Oxford Human Rights Hub (Aug. 22, 2023).
21. Nishant Shah, Identity and Identification – The Individual in the Time of Networked Governance, Socio-Legal Review (2015).
22. Reetika Khera, Impact of Aadhaar on Welfare Programmes, 52(50) Economic C Political Weekly (2017).

23. Jean Drèze, Nazar Khalid, Reetika Khera C Anmol Somanchi, Aadhaar and Food Security in Jharkhand: Pain without Gain?, 52(50) Economic C Political Weekly (2017).

24. Aharon Barak, Proportionality: Constitutional Rights and Their Limitation (Cambridge University Press 2012).

25. Granville Austin, The Indian Constitution: Cornerstone of a Nation (Oxford University Press 1966).

26. H.M. Seervai, Constitutional Law of India: A Critical Commentary (4th ed., N.M. Tripathi Private Limited 1993).

27. J.N. Pandey, The Constitutional Law of India (10th ed., Central Law Agency 1980).

28. Uday S. Mehta, Constitutionalism, in The Oxford Companion to Politics in India 15 (Niraja Gopal Jayal C Pratap Bhanu Mehta eds., Oxford University Press 2010).

29. Upendra Baxi, The Right To Be Human: Some Heresies, 13 India International Centre Quarterly (1986).

30. Samuel D. Warren C Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 193 (1890).

31. Daniel J. Solove, Understanding Privacy (Harvard University Press 2008).

32. Gautam Bhatia, State Surveillance and the Right to Privacy in India: A Constitutional Biography, 26(2) National Law School of India Review 127 (2014).

33. Bert-Jaap Koops et al., A Typology of Privacy, 38(2) University of Pennsylvania Journal of International Law 496 (2017).

34. Bhairav Acharya, The Four Parts of Privacy in India, 50(22) Economic C Political Weekly 32 (2015).

35. Christina P. Moniodis, Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy, 15(1) Yale Journal of Law C Technology 153 (2012).

36. Alan F. Westin, Privacy and Freedom, 25(1) Washington C Lee Law Review 166 (1968).

37. Planning Commission of India, Report of the Group of Experts on Privacy (Oct. 16, 2012) (Chaired by Justice A.P. Shah).