RIGHT TO PRIVACY: FROM K.S. PUTTASWAMY TO THE DIGITAL AGE CHALLENGES

Rishita Tripathi*

ABSTRACT

The right to privacy in India has traversed a remarkable judicial journey: from its ambiguous early treatment in M.P. Sharma v Kharak Sharma, through its gradual judicial recognition as an implicit facet of Article 21 of the Constitution, to its triumphant and unequivocal recognition as a fundamental right by the nine-judge constitutional bench in K.S Puttaswamy (Retd.) v. Union of India (2017). That landmark verdict, however, was not the conclusion of the story but its beginning. India now confronts the most complex chapter of privacy law in its history: the digital age. Pervasive state surveillance, the Aadhaar biometric ecosystem, algorithmic profiling by private corporations, data breaches of unprecedented scale, and the contested architecture of the Digital Personal Data Protection Act 2023 have collectively placed the right to privacy under severe strain. This article presents a comprehensive doctrinal and policy analysis of the right to privacy in India, tracing its constitutional evolution, examining the transformative significance of the Puttaswamy judgment, interrogating the adequacy of the legal framework for data protection, and confronting the digital age challenges that the law must urgently address. Drawing on comparative experience from the European Union, the United Kingdom, the United States, and Canada, and situating the analysis within international human rights norms, the article proposes a rights-based, sensitive framework for the governance of privacy in the Indian digital ecosystem.

INTRODUCTION

Privacy is one of the most debated and significant concepts in modern constitutional law. It sits at the crossroads of individual freedom and state authority, personal dignity and public interest, technological advancement and human vulnerability. In India, the recognition of privacy as a

*BA LLB (HONS), SECOND YEAR, LLOYD LAW COLLEGE.

fundamental right has been a long, hard-fought constitutional journey that continues to evolve. From the Supreme Court's initial reluctance to acknowledge an independent right to privacy to the landmark affirmation by the nine-judge bench in K.S. Puttaswamy (Retd.) v. Union of India judgment, the law has undergone more than six decades of development. For much of this period, Article 21 of the Constitution, which protects life and personal liberty except according to procedure established by law, was viewed mainly as a safeguard against arbitrary detention rather than as a broad guarantee of individual freedom.

The 2017 Puttaswamy judgment was transformative not only because it recognised privacy as a fundamental right, but also because of the depth and diversity of its nine concurring opinions. Justice D.Y. Chandrachud's lead opinion described privacy as encompassing informational privacy, decisional autonomy, bodily integrity and spatial privacy. Chief Justice J.S. Khehar traced the right to privacy to the natural rights tradition, while Justice R.F. Nariman drew upon international human rights principles to develop a rights-based framework. Together, these opinions establish privacy not as a peripheral constitutional guarantee, but as an essential component of human dignity and constitutional liberty.

Yet the judgment was delivered against the backdrop of challenges that continue to shape India's privacy landscape. The Aadhaar biometric programme was later substantially upheld by a five-judge bench. State surveillance capacities have expanded considerably, as highlighted by the Pegasus spyware revelations. The Digital Personal Data Protection Act 2023 has also faced criticism for granting broad exemptions to the state and providing limited protections to data principal rights. As a result, the constitutional promise of Puttaswamy remains a work in progress, continually being tested and refined through legislation, regulatory action, and judicial scrutiny.

THE HISTORICAL EVOLUTION OF PRIVACY JURISPRUDENCE IN INDIA

The Colonial Inheritance and Constitutional Silence: The Constitution of India, adopted in 1950, contains no explicit guarantee of the right to privacy. This absence was not simply an oversight. While the Constituent Assembly did discuss privacy concerns, no clear consensus emerged on the need to recognise it as a separate constitutional right. The framers were primarily focused on the pressing challenges of the time, securing independence, addressing deep social and economic inequalities, and establishing the foundations of democratic governance. As a result, individual rights were largely anchored in freedoms such as the right

to free speech under Article 19(1)(a) and the protection of life and personal liberty under Article 21.

India's colonial legal legacy further complicated the development of privacy protections. Laws such as the Indian Telegraph Act 1885, provisions relating to search and seizure under the Code of Criminal Procedure, and the Official Secrets Act 1923 were shaped by an administrative culture that prioritised state control and extensive surveillance over individual rights. Designed to monitor and govern a colonised population, these laws reflected a deep distrust of personal autonomy. Even after independence, they remained part of India's legal framework and continued to influence the relationship between citizens and the state for decades, creating significant obstacles to the recognition and protection of privacy as a constitutional value.

M.P. Sharma and Kharak Singh: Early Ambiguity: The Supreme Court's first significant encounter with the question of privacy came in M.P. Sharma v Satish Chandra (1954), where an eight-judge bench considered a challenge to the state's search and seizure powers. The court held that the Indian Constitution did not recognise a right to privacy comparable to that guaranteed by the Fourth Amendment of the United States Constitution. Although this observation was made in the course of a broader discussion and was not central to the decision, it cast a long shadow over Indian constitutional jurisprudence and influenced judicial thinking on privacy for decades.

A more significant confrontation with the issue arose in Kharak Singh v State of Uttar Pradesh (1963). The petitioner challenged police surveillance measures that authorised domiciliary visits and the maintenance of history sheets. While a six-judge bench struck down the practice of domiciliary visits as violating personal liberty under Article 21, it stopped short of recognising privacy as an independent constitutional right. However, Justice Subba Rao's powerful dissent took a different view, arguing that the Constitution did not protect a right to privacy. Though a minority opinion at the time, his reasoning proved remarkably prescient and was ultimately vindicated more than fifty years later in Puttaswamy.

Gobind, Rajagopal, and the Developing Jurisprudence (1975): In Gobind v. State of Madhya Pradesh (1975), Justice Mathew, speaking for a three-judge bench, took an important step forward in the development of privacy jurisprudence. For the first time, the court acknowledged that the right to privacy is implicit within the right to life and personal liberty guaranteed under Article 21, although it recognised that this right could be restricted where a

compelling state interest existed. Drawing extensively from American constitutional jurisprudence, the judgment laid the intellectual and doctrinal foundations upon which later privacy decisions would build.

The scope of privacy protection was further expanded in R. Rajagopal v State of Tamil Nadu (1994), where the Court considered the issue of unauthorised publication of an individual's autobiography. It held that every person has a right to safeguard the privacy of their own life, as well as that of their family members, subject to considerations of legitimate public interest. This decision marked a significant recognition of privacy as a protection against unwarranted intrusion by both the State and private actors.

A few years later, in People's Union for Civil Liberties v Union of India (1997), the Supreme Court addressed the growing concern of telephone surveillance. The court unequivocally affirmed that the right to privacy forms an integral part of the rights to life and personal liberty under Article 21. It also introduced procedural safeguards governing telephone interception under Section 5(2) of the Telegraph Act, thereby establishing the first meaningful judicial framework for regulating state surveillance through the lens of privacy rights.

K.S. PUTTASWAMY VS UNION OF INDIA: THE LANDMARK JUDGMENT

Genesis of the Litigation: The Puttaswamy litigation arose from a constitutional challenge to the Aadhar biometric programme, which required individuals to provide biometric information for individuals to provide biometric information for inclusion in a nationwide identity database. Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, questioned the programme on several grounds, one of the most significant being that it alleged infringement of the right to a response. The government of India argued that no fundamental right to privacy existed under the Constitution, relying on the earlier decisions in M.P. Sharma and Kharak Singh, delivered by eight-judge benches respectively. Given the importance of this issue and the conflicting strands of judicial reasoning that had emerged over the years, a three-judge bench referred the matter to a nine-judge bench for an authoritative determination of whether privacy constitutes a fundamental right under the Indian Constitution.

The Unanimous Holding and the Six Opinions: On August 24, 2017, the nine-judge bench delivered a historic and unanimous verdict, holding that the right to privacy is a fundamental right protected under Part III of the Constitution. The judgment brought together diverse constitutional philosophies while arriving at the same conclusion. Chief Justice Khekhar traced

privacy to the natural law tradition, viewing it as an inherent and inalienable aspect of human existence. Justice Nariman located the right within both the constitutional framework and international human rights jurisprudence, while Justice Chandrachud described privacy as a multidimensional right encompassing spatial privacy, informational privacy, and decisional autonomy.

At the same time, the court made it clear that the right to privacy is not absolute. Any restriction on privacy must satisfy the constitutional standard of proportionality. According to the court, a limitation on privacy must pursue a legitimate state objective, bear a rational connection to that objective, be necessary and represent the least restrictive means available, and avoid imposing a disproportionate burden on the individual. This four-pronged proportionality test, which had earlier been articulated in a modern dental college, now serves as the principal framework for evaluating the constitutional validity of measures that interfere with privacy rights. It ensures that while the state may pursue legitimate public interests, such action must remain balanced, justified, and respectful of individual liberty.

Privacy, Dignity, and Informational Self-Determination: One of the most significant contributions of Puttaswamy was its firm grounding of privacy in the constitutional value of human dignity. Justice Chandrachud observed that dignity is the animating spirit of the Fundamental Rights Chapter and that privacy is an essential condition for its realisation. In this view, privacy is not merely a standalone right but a vital means through which individuals preserve their autonomy, identity, and freedom from unwarranted intrusions. By linking privacy to dignity, the judgment elevated it from a narrow legal protection to a foundational constitutional value. The decision also introduced and developed the concept of informational self-determination, the right of individuals to exercise control over the collection, use, and dissemination of information relating to themselves. This principle recognises that in an increasingly digital society, personal data is closely tied to individual autonomy and liberty. By affirming an individual's authority over their personal information, the court provided the conceptual and constitutional foundation upon which modern Indian data protection law has been built.

THE AADHAAR CONTROVERSY AND PRIVACY

The Aadhaar biometric identification programme, established under the Aadhaar Act 2016, is the largest biometric database in the world, covering more than 1.3 billion individuals across

India. It was conceived as a mechanism for the targeted delivery of government subsidies, welfare schemes, and public benefits by linking identity verification to biometric information. From its inception, however, the programme generated significant privacy concerns. These concerns included the mandatory collection of sensitive biometric data, the potential aggregation of personal information across multiple governmental databases, the possibility of facilitating mass surveillance, and the risk of excluding individuals who are unable to authenticate their identity through biometric verification.

In K.S. Puttaswamy v Union of India, a five-judge constitution bench upheld the constitutional validity of Aadhaar by a majority of four to one. Justice Chandrachud, in a forceful and influential dissent, concluded that the Aadhar Act had been enacted as a money bill in a manner inconsistent with constitutional requirements. He further argued that the institutional architecture of Aadhaar created the conditions for pervasive state surveillance and that mandatory linking of Aadhaar with private services was constitutionally impermissible. Several scholars have subsequently contended that the majority judgment did not adequately account for the structural dangers posed by the repurposing of welfare databases for surveillance.

The broader information technology ecosystem that has developed around Aadhaar, including the Aadhaar-enabled payment system, DigiLocker, the health ID framework, and the CoWIN vaccination platform, has significantly expanded the data footprint associated with the Aadhaar identifier beyond its original objective of subsidy delivery. As a result, information initially collected for one purpose has increasingly become capable of being used in a variety of other contexts. The principle of purpose limitation, which is a foundational element of privacy and data protection law across jurisdictions, has not been consistently observed within the Aadhaar ecosystem. This continuing expansion of data use creates ongoing privacy concerns that, according to many commentators, are not fully addressed by the Digital Personal Data Protection Act 2023.

STATE SURVEILLANCE AND CONSTITUTIONAL LIMITS

The Legal Framework for Surveillance: State surveillance in India is governed by a complex patchwork of legislative provisions that confer broad powers upon governmental authorities. Section 69 of the Information Technology Act 2000 authorises the central and state governments to intercept, monitor, and decrypt information transmitted through any computer

resource when such actions are considered necessary in the interests of national security, public order, or other specified grounds. The procedural framework governing the exercise of these powers is contained in the IT (Interception) Rules 2009. More recently, the Telecommunications Act 2023 has consolidated and replaced several earlier provisions of the Telegraph Act relating to interception and monitoring on similar grounds. However, a significant concern remains that the Interception Rules do not require prior judicial approval before surveillance measures are undertaken. Instead, the system relies primarily on executive authorisation, a model that provides weaker safeguards than those generally required under international human rights standards.

The requirements for lawful surveillance have been elaborated by the European Court of Human Rights in landmark decisions such as Malone v. United Kingdom and Klass v. Germany, where the court emphasised that surveillance regimes must be governed by legal rules that are sufficiently clear, accessible, and foreseeable. In addition, such regimes must provide for independent oversight mechanisms and effective remedies against abuse. Measured against these standards, Indian surveillance law continues to face substantial criticism. Although the procedural safeguards formulated by the Supreme Court in PUCL for telephone interception have, through judicial interceptions, been extended to certain forms of digital surveillance, the underlying statutory framework remains limited in scope and continues to fall short of internationally recognised benchmarks for the protection of privacy and civil liberties.

The Pegasus Revelations and their Legal Significance: In July 2021, a global investigative consortium disclosed allegations that Pegasus spyware, developed by NSO Group, had been used to target the mobile devices of journalists, activists, lawyers, politicians, and other public figures across several countries, including India. These revelations triggered widespread concerns regarding privacy, surveillance, and democratic accountability. In response, the Supreme Court of India constituted a Technical Committee to examine the allegations and investigate the possible use of spyware. This episode brought renewed attention to the constitutional limits of state surveillance and the adequacy of existing legal safeguards.

Several scholars have argued that spyware capable of gaining unrestricted access to a device and extracting virtually all of its data represents an unprecedented level of intrusion into personal privacy. According to this view, such invasive surveillance techniques are so extensive in their reach that no legitimate state objective can proportionally justify their use within a constitutional framework committed to individual rights and liberties. Academic

research has further highlighted the broader consequences of mass surveillance, demonstrating that the mere possibility of constant monitoring can create a chilling effect on the exercise of fundamental rights, discouraging individuals from freely expressing opinions, communicating confidentially, associating with others, or engaging in legitimate political and social activity.

Mass Surveillance and the NATGRID: The National Intelligence Grid (NATGRID) has been developed as an integrated intelligence platform intended to enhance counter terrorism and national security capabilities. To achieve this objective, it is designed to connect and analyse information drawn from twenty-one categories of government and private sector databases, including travel records, banking transactions, immigration data, income tax information, and other sources. By bringing together these diverse streams of information, NATGRID seeks to create a comprehensive profiling and intelligence gathering capability for security agencies. While proponents view such integration as an important tool for preventing and investigating security threats, the scale and scope of data aggregation have generated significant concerns regarding privacy and civil liberties.

A particularly serious concern relates to the lack of transparency surrounding the programme. The legal and regulatory framework governing NATGRID's collection, processing, sharing, storage and retention of personal data has not been made publicly available in sufficient detail. As a result, there is limited public knowledge regarding the safeguards that apply to the system, the extent of oversight mechanisms, and the remedies available in cases of misuse or abuse. This opacity has raised important questions about accountability and the compatibility of such large-scale data integration with constitutional privacy protections.

These concerns are reinforced by a substantial body of academic literature in the field of surveillance studies, which has consistently documented the phenomenon known as the "chilling effect". Research suggests that individuals who believe their activities, communications, or associations may be subject to monitoring are often less willing to exercise their fundamental rights freely. Such surveillance environments can discourage open expression, inhibit political participation, restrict freedom of association, and alter individual behaviour in subtle but significant ways. Consequently, the privacy implications of programmes such as NATGRID extend beyond data collection itself and raise broader constitutional questions about the impact of surveillance on democratic freedoms and individual autonomy.

THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Legislative History and Structure: The road to a data protection law in India has been long and contested. The Justice Srikrishna Committee's 2018 report proposed a comprehensive data protection framework drawing on the GDPR model. The Personal Data Protection Bill 2019 was introduced in Parliament and referred to a Joint Parliamentary Committee. The bill was eventually withdrawn, and the Digital Personal Protection Act 2024 was enacted in its place. The DPDPA establishes rights for data principals, obligations for data fiduciaries, and the Data Protection Board as the enforcement authority.

Key Provisions and Their Assessment: The DPDPA requires data fiduciaries to obtain consent that is free, specific, informed, unconditional, and unambiguous before undertaking the processing of personal data. In addition, data principals are granted a range of statutory rights, including the right to obtain information regarding the processing of their personal data, the right to seek correction and erasure of inaccurate or outdated information, and the right to avail themselves of grievance redressal mechanisms. These protections represent a substantial improvement over the earlier framework established under the IT (SPDI) Rules 2011, which operated within a more limited scope and relied upon a comparatively weaker standard of consent.

At the same time, the DPDPA incorporates a broadly framed exemption for state instrumentalities acting in the interest of national security, public order, and related governmental objectives. This exemption has attracted significant criticism from scholars and privacy advocates, who contend that it sits uneasily with the constitutional framework articulated in Puttaswamy. According to this criticism, the judgment requires all restrictions on privacy rights to satisfy the test of proportionality, regardless of the identity of the actor imposing the restrictions. Concerns have also been raised regarding the institutional design of the Data Protection Board. Because the board functions as an executive body rather than an independent regulatory authority, questions have emerged about its ability to provide robust and impartial oversight, particularly in matters involving the processing of personal data by government agencies.

The DPDPA also introduces specific safeguards relating to the protection of children's personal data. Under the Act, data fiduciaries must obtain verifiable parental consent before processing

the personal data of individuals below the age of eighteen years and are prohibited from undertaking forms of data processing that are likely to cause harm to children. These provisions reflect an effort to provide enhanced protection to minors in an increasingly digital environment. At the same time, parliamentary debates surrounding the legislation revealed substantial concern regarding the need to strike an appropriate balance between effective child protection and the practical challenges of implementation. Although the statutory framework has now been enacted, the mechanisms through which parental consent will be verified and enforced remain to be specified and operationalised through subordinate legislation.

Comparison with the GDPR and Global Standards: A comparative analysis of contemporary data protection frameworks suggests that the DPDPA does not fully match the standards established by the General Data Protection Regulation (GDPR). Widely regarded as one of the most comprehensive data protection regimes in the world, the GDPR provides a robust framework of rights, obligations, and enforcement mechanisms designed to ensure a high level of protection for personal data. One of its most significant features is its stringent penalty structure. The GDPR authorises fines of up to four per cent of a company's global annual turnover or EUR 20 million, whichever is higher, creating a powerful deterrent against non-compliance. By contrast, the DPDPA prescribes a maximum penalty of Rs 250 crore, which, while substantial in absolute terms, may be less effective as a deterrent for large multinational corporations with extensive global operations.

Additional insights can be gained by comparing the DPDPA with other international privacy frameworks, including the California Consumer Privacy Act 2018 and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). These laws offer alternative regulatory approaches to the protection of personal data and the enforcement of privacy rights. In particular, the California statute provides a private right of action in certain cases involving data breaches, enabling affected individuals to directly seek remedies through legal proceedings. This mechanism is generally regarded as a stronger and more proactive enforcement tool than the complaint-driven framework adopted under the DPDPA, which relies primarily on regulatory intervention following the filing of grievances. As a result, comparative experience suggests that while the DPDPA represents an important step in India's data protection journey, its enforcement architecture remains comparatively less robust than that of several leading international privacy regimes.

RIGHT TO PRIVACY IN RELATION TO OTHER FUNDAMENTAL RIGHTS

The constitutional right to privacy does not operate in isolation; rather, it is closely connected with and often overlaps with other fundamental rights guaranteed under the Constitution. One of the most significant areas of interaction is the relationship between privacy and freedom of expression under Article 19(1)(a). The Supreme Court's decision in *Shreya Singhal* struck down section 66A of the Information Technology Act on the ground that it imposed an unconstitutional restriction on free speech and expression. However, the subsequent Intermediary Rules 2021 have reintroduced extensive content regulation obligations for digital platforms and intermediaries. In this context, state measures that regulate online speech may simultaneously affect both expressive freedom and individual privacy, making it necessary for courts to undertake a careful proportionality analysis in accordance with the framework established in *Puttaswamy*. Such analysis is essential to ensure that restrictions imposed in the digital sphere do not unnecessarily undermine either constitutional value.

Privacy also shares a complex relationship with the right to information. In *CPIO, Supreme Court v Subhash Chandra Agarwal*, the Supreme Court addressed the interaction between transparency and privacy by holding that the exemption relating to personal information under the Right to Information Act must be interpreted in light of the constitutional right to privacy. The Court emphasised that disclosure of personal information should not be permitted where it would result in a disproportionate invasion of privacy and where no legitimate public interest justifies such disclosure. The decision reflects an effort to balance two competing constitutional objectives: the promotion of transparency and accountability in public administration on the one hand, and the protection of individual privacy and dignity on the other.

The relationship between privacy and the right to equality under Article 14 presents another important constitutional dimension. In particular, it raises questions regarding differential or discriminatory surveillance practices and whether surveillance programmes that disproportionately target specific groups based on religion, ethnicity, political affiliation, or other protected characteristics amount not only to violations of privacy but also to forms of unconstitutional discrimination. The recognition in *Puttaswamy* that privacy is intrinsically linked to human dignity provides a strong constitutional foundation for advancing such arguments. Nevertheless, the precise contours of this relationship have not yet been fully explored or authoritatively articulated within Indian constitutional jurisprudence, leaving an important area of privacy law open for future judicial development.

COMPARATIVE AND INTERNATIONAL PERSPECTIVES

India's *Puttaswamy* judgment drew heavily upon comparative constitutional jurisprudence from across the world, and the continuing evolution of Indian privacy law has similarly benefited from sustained engagement with international legal developments. The European approach to privacy, founded upon Article 8 of the European Convention on Human Rights and reinforced through the comprehensive framework of the GDPR, treats privacy as a fundamental right that requires not only constitutional recognition but also positive legislative protection and effective independent regulatory oversight. This model places significant emphasis on accountability, transparency, and enforceable safeguards against both public and private infringements of privacy. In addition, the Council of Europe's Convention 108, widely recognised as the first binding international treaty dedicated specifically to data protection, provides an important normative framework for the governance of personal data. Although influential globally, India has not yet formally acceded to this treaty framework.

Within the Indian context, the Justice AP Shah Committee made a particularly significant contribution through its 2012 report, which recommended the enactment of a comprehensive privacy framework grounded in nine foundational privacy principles: notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness, and accountability. These principles were intended to provide a coherent framework for balancing the legitimate use of personal data with the protection of individual rights and freedoms. Even today, they continue to serve as an important normative benchmark against which the provisions of the DPDPA can be assessed and evaluated. Many of the contemporary debates surrounding consent, data minimisation, transparency, and accountability can be traced back to the framework originally proposed by the Committee.

The experience of the United States offers a contrasting perspective on privacy regulation and provides valuable lessons for policymakers. Rather than adopting a single comprehensive data protection statute, the United States has historically relied upon a sector-specific approach, consisting of a patchwork of federal and state laws governing different categories of data and different industries. While this model has allowed for regulatory flexibility in certain contexts, it has also revealed the limitations of non-comprehensive data protection regimes. Fragmented legal protections can lead to inconsistencies, regulatory gaps, and uneven enforcement standards, making it more difficult to ensure uniform protection of privacy rights. As India continues to develop its own privacy framework, the American experience serves as a

cautionary example of the challenges that may arise in the absence of a fully integrated and coherent data protection architecture.

LEGISLATIVE GAPS AND REFORM PROPOSALS

Independent Regulatory Authority: The most significant structural weakness in India's current privacy framework is the absence of a truly independent data protection authority capable of exercising effective oversight over both private and governmental data processing activities. Although the DPDPA 2023 establishes the Data Protection Board as the primary enforcement mechanism under the legislation, the Board functions as an executive body whose members are appointed by, and ultimately accountable to, the Central Government. This institutional design has generated considerable concern regarding its ability to act independently, particularly in matters involving government agencies and the state, which lead to data processing activities.

The lack of institutional independence becomes especially significant in the context of surveillance, national security measures, and large-scale government databases, where effective oversight requires a regulator that is insulated from executive influence. A body that remains structurally dependent upon the government may face inherent limitations when called upon to scrutinise the legality, necessity, or proportionality of governmental actions affecting privacy rights. As a result, many commentators argue that the existing framework falls short of the level of independence required for meaningful privacy protection and regulatory accountability.

Addressing this deficiency would require the creation of a statutory data protection authority endowed with strong institutional safeguards. Such an authority should enjoy security of tenure for its members, operational and financial independence from the executive, and a clear legal mandate to monitor compliance with privacy and data protection obligations. Equally important, it should possess the authority to initiate investigations on its own motion, particularly in relation to government surveillance programmes and large-scale public sector data processing activities, without requiring a prior complaint. Only through the establishment of an independent and empowered regulatory institution can India ensure effective oversight, strengthen public confidence in its privacy framework, and fully realise the constitutional vision of privacy articulated in *Puttaswamy*.

Surveillance Reform: India's surveillance framework requires substantial reform if it is to comply fully with the constitutional standards articulated in *Puttaswamy*, particularly the requirement that all restrictions on privacy satisfy the test of proportionality. The existing legal regime continues to vest broad surveillance powers in the executive while providing limited mechanisms for independent oversight and accountability. To align surveillance practices with constitutional principles and international human rights standards, a number of specific reforms have been proposed by scholars, policymakers, and civil liberties advocates.

Among the most significant proposals is the requirement of mandatory prior judicial authorisation before targeted surveillance measures can be undertaken. Judicial scrutiny at the pre-authorisation stage would provide an important safeguard against arbitrary or excessive intrusions into privacy. Additional recommendations include the introduction of sunset clauses for interception orders to ensure that surveillance authorisations do not continue indefinitely without review, and the establishment of a system of post-surveillance notification under which individuals are informed, after operational concerns have ceased, that they were subjected to surveillance. Such notification mechanisms are widely regarded as important accountability tools because they enable affected individuals to challenge unlawful surveillance and seek appropriate remedies.

Further reforms include the creation of an independent parliamentary oversight committee tasked with monitoring the activities of intelligence and surveillance agencies. Parliamentary oversight would introduce an additional layer of democratic accountability and help ensure that surveillance powers are exercised consistently with constitutional norms. There have also been increasing calls for a clear and comprehensive legal framework governing the acquisition, deployment, and use of commercial spyware technologies, particularly in light of growing concerns regarding highly intrusive surveillance tools capable of accessing extensive personal information from digital devices.

Leading scholars of Indian privacy law have repeatedly emphasised that constitutional protections cannot be effective in the absence of meaningful oversight of executive surveillance powers. Without independent review, transparent procedures, and enforceable accountability mechanisms, the constitutional guarantee of privacy risks becoming largely theoretical rather than practically enforceable.56 Consequently, reform of India's surveillance laws remains one of the most important challenges in the ongoing effort to translate the constitutional promise of *Puttaswamy* into effective protection for individual rights in the digital age.

Strengthening the DPDPA: The DPDPA would benefit from a series of targeted amendments aimed at strengthening privacy protections and bringing the legislation into closer alignment with the constitutional principles articulated in *Puttaswamy,* as well as emerging international best practices in data protection. One of the most important reforms would be the narrowing of the Act's broad exemption for state instrumentalities. Rather than permitting wide-ranging exemptions based solely on governmental assertions of national security or public order, the law should require an independent assessment of whether the proposed data processing is necessary and proportionate in the specific circumstances. Such a requirement would ensure that state action remains subject to meaningful constitutional scrutiny and does not escape accountability merely because it is undertaken by governmental authorities.

Another significant reform would be the introduction of mandatory data protection impact assessments for high-risk processing activities. These assessments would require data fiduciaries to evaluate, in advance, the potential privacy risks associated with large-scale, sensitive, or technologically complex forms of data processing and to implement appropriate safeguards before such activities are undertaken. By identifying and mitigating risks at an early stage, impact assessments can serve as an important preventive mechanism for protecting individual rights.

The DPDPA could also be strengthened through the creation of a private right of action for data breaches. Such a provision would enable affected individuals to seek remedies directly when their personal data has been compromised, rather than relying exclusively on regulatory intervention. A private enforcement mechanism would enhance accountability, provide stronger incentives for compliance, and supplement the role of regulatory authorities in protecting data principals.

In addition, the legislation should expressly incorporate the principles of data minimisation, purpose limitation, and storage limitation as core statutory obligations. These principles are widely recognised as foundational elements of modern data protection law. Data minimisation requires that only the data necessary for a specified purpose be collected; purpose limitation ensures that personal data is not subsequently used for unrelated objectives; and storage limitation restricts the retention of personal data beyond the period for which it is legitimately required. Explicit incorporation of these principles would provide greater clarity and strengthen the overall architecture of privacy protection under the Act.

Finally, the increasing use of automated decision-making systems and algorithmic processes makes it essential to require algorithmic impact assessments in situations where such systems may significantly affect data principals. These assessments would help identify risks relating to bias, discrimination, opacity, and unfair outcomes, while promoting transparency and accountability in the deployment of automated technologies. As algorithmic systems assume a greater role in decisions affecting access to services, employment, credit, welfare benefits, and other important aspects of life, regulatory safeguards of this nature will become increasingly important for ensuring that technological innovation remains consistent with constitutional values and individual rights.

International Engagement: India should seriously consider acceding to Convention 108 and its 2018 modernising Protocol, as doing so would demonstrate a commitment to internationally recognised standards of data protection and privacy governance. Convention 108, as the world's first binding international treaty dedicated to the protection of personal data, provides a comprehensive framework for ensuring that personal information is processed in a manner that respects individual rights while facilitating legitimate data use. Accession would not only strengthen India's domestic privacy framework but also enhance confidence among international partners regarding the adequacy of India's data protection standards. In practical terms, it could facilitate cross-border data flows and promote greater regulatory cooperation with Convention 108 member states, thereby supporting India's growing participation in the global digital economy.

At the international level, India should also play a more active role in ongoing discussions concerning the right to privacy in the digital age within the United Nations system. As digital technologies increasingly shape economic activity, governance, communication, and social interaction, the development of global privacy norms has become a matter of significant international importance. Active engagement in these processes would allow India to contribute constructively to the formulation of international standards governing surveillance, data protection, artificial intelligence, and digital rights.

Such participation is particularly important because global privacy debates have often been shaped by the experiences and priorities of developed economies. As one of the world's largest democracies and a leading digital society, India is uniquely positioned to articulate perspectives that reflect the realities, developmental priorities, and governance challenges of the Global South. By contributing to the evolution of international privacy norms, India can help ensure

that emerging global frameworks are rights-respecting and responsive to the diverse social, economic, and technological contexts of developing countries. In doing so, it can play a meaningful role in shaping a more inclusive and balanced international approach to privacy and data protection in the digital era.

CONCLUSION

The right to privacy in India has travelled a long and remarkable constitutional journey. From the judicial reluctance reflected in *M.P. Sharma* and *Kharak Singh*, through the gradual expansion of privacy protections in *Gobind* and *Rajagopal*, to the landmark affirmation in *Puttaswamy*, Indian constitutional jurisprudence has evolved towards a conception of privacy that is philosophically robust, doctrinally sophisticated, and firmly anchored within the constitutional framework. The recognition by the nine-judge bench that privacy is a fundamental right rooted in the value of human dignity stands as one of the most significant constitutional achievements of the Indian Supreme Court. By locating privacy at the heart of personal liberty, autonomy, and dignity, the Court transformed it from a peripheral concern into a foundational constitutional guarantee.

At the same time, *Puttaswamy* should be understood not as the culmination of the privacy project but as its beginning. The digital age has generated challenges of a scale and complexity that were unimaginable when many of India's existing legal frameworks were conceived. State surveillance capabilities have expanded dramatically through the use of artificial intelligence, predictive technologies, and large-scale data analytics. Private corporations increasingly rely on business models built around the collection, processing, and monetisation of personal information. Biometric identification systems create enduring repositories of highly sensitive personal data, while sophisticated spyware technologies possess the capacity to penetrate virtually every aspect of an individual's private life. Against this backdrop, the legal framework that India has constructed remains fragmented, uneven, and insufficiently protective of the constitutional values that *Puttaswamy* sought to secure.

Meeting these challenges will require both legislative vision and sustained judicial vigilance. Parliament must undertake meaningful reforms to ensure that the DPDPA functions as a genuinely rights-protective instrument rather than merely a framework for data governance. This includes strengthening safeguards against excessive state access to personal data, establishing a truly independent regulatory authority, and enacting comprehensive legislation

governing surveillance activities in accordance with constitutional standards. India must also engage more actively with international data protection norms and emerging global privacy frameworks to ensure that its domestic regime remains responsive to evolving technological realities.

The judiciary, for its part, must continue to apply the proportionality framework articulated in *Puttaswamy* with rigour and consistency whenever governmental action affects privacy interests. Constitutional scrutiny must remain meaningful, particularly in cases involving surveillance, data collection, and restrictions justified on grounds of national security or public order. Ultimately, as *Puttaswamy* so powerfully recognised, privacy is not merely one right among many; it is a necessary precondition for the meaningful exercise of numerous other freedoms guaranteed by the Constitution. In a democratic society committed to the constitutional ideals of justice, liberty, equality, and fraternity, the protection of privacy cannot be treated as an optional policy choice. It is a foundational constitutional imperative, essential to preserving individual dignity, safeguarding autonomy, and ensuring the continued vitality of democratic governance.

MAIN FINDINGS

The following principal findings emerge from the foregoing doctrinal, comparative, and policy analysis of the right to privacy in India -

Privacy is a Fundamental Right of Unambiguous Constitutional Status:

- The nine-judge bench decision in K.S. Puttaswamy v. Union of India (2017) firmly settled that privacy is a fundamental right under the Indian Constitution. It overruled earlier decisions like M.P. Sharma v. Satish Chandra and Kharak Singh v. State of Uttar Pradesh, which had denied privacy an independent constitutional status.
- The Court clarified that privacy is an essential part of dignity and personal liberty, protected under Part III of the Constitution. It is not just a separate right but lies at the heart of Articles 14, 19, and 21.
- In simple terms, the judgment recognises that a person cannot truly live with freedom or dignity if their private life is constantly exposed or controlled. Privacy, therefore, becomes the foundation that allows all other fundamental rights to be meaningfully exercised.

The proportionality framework is the governing standard -

- K.S. Puttaswamy v. Union of India (2017) laid down a clear test for when the State can restrict the right to privacy. Any restriction must pass a four-step proportionality standard.
- First, the State must show a legitimate aim. Second, the measure must be rationally connected to that aim. Third, it must be the least restrictive option available. Finally, the impact on individual rights must not be excessive compared to the goal being achieved.
- This framework is now the main tool used by courts to assess privacy violations, including in later cases like the Aadhaar decision. If a law, executive action, or even certain private conduct fails this test, it is considered unconstitutional.

State surveillance law is constitutionally deficient -

- India's surveillance legal system, which includes Section 69 of the Information Technology Act, 2000, the Interception Rules 2009, and the Telecommunications Act 2023, falls short of the proportionality standards laid down in K.S. Puttaswamy v. Union of India (2017).
- The main concerns are structural: there is no requirement for prior judicial approval, no truly independent oversight body, no mandatory post-surveillance notification, and no strong mechanism for affected individuals to seek an effective remedy. Because of these gaps, the framework does not meet constitutional standards.
- The Pegasus spyware revelations further highlighted these weaknesses, showing that targeted surveillance of journalists, lawyers, and civil society members has taken place without meaningful legal accountability.

The Digital Personal Data Protection Act 2023 is a partial and flawed advance -

- The Digital Personal Data Protection Act, 2023, is India's first comprehensive law aimed at governing how personal data is collected, stored, and used. It marks a clear improvement over the earlier fragmented approach to data protection.
- However, the framework has been criticised for some important gaps. One major concern is the broad exemption given to the State, which allows government agencies to process data with limited independent oversight. Another issue is that the

enforcement body, the Data Protection Board, is not fully independent, which raises doubts about its ability to effectively regulate state action.

- The Act also does not strongly embed core privacy principles like data minimisation, purpose limitation, and storage limitation. In addition, individuals do not have a direct private right to sue for data breaches, and the penalties may not be strong enough to deter large corporations from violating data protection rules.
- Overall, while the law is a step forward, these limitations weaken its ability to fully protect privacy in practice.

Cross-cutting intersections and other rights remain underdeveloped -

- The connection between privacy and other fundamental rights like freedom of expression, the right to information, and equality has been recognised by Indian courts in cases such as Shreya Singhal v. Union of India (2015), CPIO v. Subhash Chandra Agarwal, and the Aadhaar decision in K.S. Puttaswamy v. Union of India (2018 Aadhaar judgment).
- These decisions show that privacy does not exist in isolation; it often interacts with, and sometimes conflicts with, other rights. Courts have tried to balance these interests, but the doctrine is still evolving.
- Some important questions remain unresolved. For instance, how should the Constitution deal with algorithmic profiling that may indirectly discriminate on protected grounds? Similarly, the privacy impact of internet shutdowns and increasing platform-based content regulation has not yet been clearly settled by the courts.
- As a result, while the broad framework exists, Indian constitutional law is still developing clearer rules for these emerging digital-age challenges.

India's privacy framework lags behind international standards -

- A comparative view shows that India's privacy and data protection system is still less developed than stronger global frameworks like the EU's GDPR, the Council of Europe's Convention 108, and domestic laws in countries such as Canada, Australia, and Brazil.
- Unlike the European Union's GDPR regime, India has not yet achieved "adequacy" recognition from the European Commission, which limits the free flow of data between

India and the EU. India is also not a party to Convention 108, which is an important international benchmark for harmonised data protection standards.

- Additionally, gaps in mutual legal assistance mechanisms make it harder to enforce privacy protections across borders. These limitations collectively reduce India's ability to fully integrate into the global digital economy while maintaining strong and enforceable privacy safeguards for individuals.

Digital literacy and public awareness remain critical gaps -

- The effectiveness of legal privacy protections ultimately depends on whether people actually understand and can use them. If individuals are not aware of their rights, even strong laws remain weak in practice.
- In India, studies and surveys show that many internet users have a limited understanding of how their data is collected, how consent works, and where to go if their rights are violated. This creates a significant gap between legal protections and real-world enforcement.
- The consent-based approach under the Digital Personal Data Protection Act, 2023, assumes a level of awareness and digital literacy that may not yet be widespread. As a result, consent alone may not be enough to ensure meaningful privacy protection.
- This suggests that legal reform must go hand in hand with stronger public awareness, digital literacy, and education efforts so that individuals can effectively exercise their privacy rights.

SUGGESTIONS

Based on the foregoing analysis and findings, the following specific suggestions are advanced for the attention of the legislature, the executive, the judiciary, civil society, and the legal academy -

Establish a genuinely independent data protection authority:

- The Data Protection Board created under the Digital Personal Data Protection Act, 2023, is widely viewed as needing stronger institutional independence to function as an effective privacy regulator.
- One proposed reform is to redesign it as a fully independent statutory authority, similar in spirit to bodies like the Election Commission of India or the Comptroller and Auditor

General. This would involve a transparent, multi-stakeholder appointment process, fixed non-renewable terms for members, and strong safeguards ensuring security of tenure and freedom from executive influence.

- Such a body should also have robust enforcement powers. These would include the ability to initiate investigations into government data practices on its own, impose meaningful financial penalties where violations occur, and publish findings without requiring prior approval from the executive.
- Overall, the aim is to ensure that data protection enforcement is not only legally mandated but also institutionally independent and capable of holding both private actors and the State accountable.

Enact a comprehensive Surveillance Reform Act -

- A strong reform proposal would be the enactment of a dedicated Surveillance Accountability Act to bring India's interception regime in line with constitutional privacy standards under K.S. Puttaswamy v. Union of India (2017).
- Such a law could require prior judicial authorisation from a specialised surveillance court before any targeted interception begins, ensuring independent scrutiny at the outset. It could also mandate post-surveillance notification to affected individuals after the operation ends, with limited exceptions only where a judicial authority approves a national security claim.
- Further safeguards would include a clear statutory prohibition on the use of commercial spyware by state agencies unless specifically authorised by law and subject to judicial oversight. Oversight could be strengthened through an independent parliamentary intelligence committee with access to classified materials, ensuring democratic accountability.
- Finally, the framework should recognise a direct right to judicial remedy for unlawful surveillance, including compensation for violations. Together, these measures would significantly strengthen accountability and align surveillance practices with constitutional requirements of necessity, proportionality, and due process.

Amend the DPDPA to narrow the State Exemption -

- A key reform suggestion for the Digital Personal Data Protection Act, 2023, is to significantly narrow the current broad exemption granted to the State under section 17.

- Instead of a wide and largely discretionary exemption, state agencies should only be exempted in clearly defined and limited categories involving national security or law enforcement needs. Even in those cases, processing should be allowed only with independent judicial or quasi-judicial approval and subject to regular periodic review.
- For all other government data processing, the State should be held to the same standards as private entities. This means full compliance with core privacy principles such as informed consent, purpose limitation, data minimisation, and strict retention limits.
- Such a restructuring would better balance legitimate state interests with the constitutional requirement of proportionality under K.S. Puttaswamy v. Union of India (2017), while ensuring that government data practices remain transparent and accountable.

Introduce Data Protection Impact Assessments -

- Large-scale data processing, whether by the government or private companies, especially involving sensitive categories like biometric, health, financial, or children's data, should be subject to mandatory Data Protection Impact Assessments (DPIAs) before they begin.
- These assessments would require organisations to clearly evaluate whether the processing is proportionate, identify possible privacy risks, and explain what safeguards they will use to reduce harm.
- In high-risk cases, the independent data protection regulator under the Digital Personal Data Protection Act, 2023, should not only review but also formally approve these assessments before the processing is allowed to proceed.
- This approach strengthens preventive oversight and aligns with the proportionality principles laid down in K.S. Puttaswamy v. Union of India (2017), ensuring that privacy risks are addressed before harm occurs rather than after violations take place.

Accede to Convention 108 and engage with the Budapest Convention -

- India could strengthen its global data protection standing by acceding to the Council of Europe's Convention 108+, along with its 2018 modernising protocol. This would place India within a binding international framework for personal data protection and could also support future adequacy recognition by the European Commission.

- Alongside this, India may also consider joining the Second Additional Protocol to the Budapest Convention on Cybercrime. This would strengthen cross-border cooperation by improving mutual legal assistance mechanisms for accessing electronic evidence and addressing cyber-enabled privacy violations more effectively.
- Taken together, these steps would help align India more closely with international standards and improve cooperation in the governance of data and cybersecurity in a global digital environment.

Constitutionalise the Aadhaar Ecosystem's Purpose Limitation -

- The use of the Aadhaar system should be strictly confined to the purposes expressly permitted under the Aadhaar framework, so that it is not extended into unrelated areas without clear legal backing.
- In particular, the Government should ensure that the Aadhaar identifier is not used beyond what is authorised under the existing Aadhaar law, and that purpose limitation operates as a binding legal principle across all Aadhaar-linked systems.
- Any attempt to expand Aadhaar into new domains should require a clear and affirmative act of Parliament, supported by a mandatory Data Protection Impact Assessment and a process of public consultation before approval.
- This approach would reinforce safeguards around the Aadhaar ecosystem and align its operation with constitutional privacy requirements recognised in K.S. Puttaswamy v. Union of India (2017), particularly the need for necessity, proportionality, and strict limits on state use of personal data.

Strengthen Judicial Remedies for Privacy Violations -

- The right to privacy, as recognised as a fundamental right under K.S. Puttaswamy v. Union of India (2017), must be backed by strong and practical remedies to be meaningful in real life.
- Courts, especially the Supreme Court and High Courts, should develop a clear and consistent approach to granting interim relief in privacy matters. This should include the power to temporarily halt or suspend large data processing programmes when there is a serious constitutional question, until a full hearing is completed.
- At the legislative level, Parliament should also introduce a private right of action for individuals affected by data breaches. This should allow people to seek compensation

for measurable harm without having to prove exact financial loss, since privacy violations often cause non-pecuniary harm such as distress, vulnerability, or loss of control over personal information.

- Together, these measures would make privacy enforcement more accessible and effective, ensuring that constitutional guarantees are supported by real and enforceable remedies.

Mandate Digital Literacy and Privacy Education -

- The right to privacy, recognised as a fundamental right in K.S. Puttaswamy v. Union of India (2017), is meaningful only if it is supported by effective and practical remedies.
- Courts, particularly the Supreme Court and High Courts, should evolve a consistent approach to interim relief in privacy disputes. This includes the power to temporarily suspend large-scale data processing programmes where serious constitutional concerns arise, until a full judicial review is completed.
- At the legislative level, Parliament should introduce a private right of action for data breaches, enabling individuals to claim compensation for harm without needing to prove precise financial loss. This is important because privacy violations often result in non-material harms such as distress, loss of control, or increased vulnerability.
- Taken together, these reforms would make privacy protection more real and enforceable, ensuring that constitutional guarantees translate into effective remedies in practice.

Develop a coherent framework for Algorithmic Accountability -

- As artificial intelligence and machine learning systems become central to decision-making in both the public and private sectors, whether in credit scoring, insurance pricing, hiring, or even law enforcement, there is a growing need for clear legal safeguards.
- Parliament should introduce algorithmic accountability rules requiring greater transparency around automated decision-making systems. Individuals should have the right to know when a decision affecting them has been made by an algorithm and to seek meaningful human review in cases with significant consequences.
- In addition, automated decisions based on sensitive personal data should not be permitted without explicit consent. High-risk systems used at scale should also be

subject to mandatory independent algorithmic audits to assess fairness, accuracy, and potential bias.

- These safeguards would ensure that technological innovation does not come at the cost of accountability, fairness, and constitutional rights.

Reform RTI-Privacy Balance through clear statutory criteria -

- The balance between the right to information and the right to privacy should be clarified through clear statutory standards in both the Right to Information Act, 2005 and the Digital Personal Data Protection Act, 2023.
- These laws should explicitly set out how privacy interests are to be weighed against public interest in disclosure. A key distinction should be drawn between information relating to the performance of public duties, where transparency will usually take priority and genuinely personal information about public officials, where privacy concerns may justifiably override disclosure.
- By setting out these criteria in advance, information commissioners and appellate authorities would have a clearer, more principled framework for decision-making, reducing inconsistency and strengthening both transparency and privacy protections in a balanced way.

REFERENCES

1. KS Puttaswamy (Retd) v Union of India [2017] 10 SCC 1 ('Puttaswamy I').

2. Constitution of India 1950, art 21.

3. Puttaswamy I (n 1) [310]-[312] (Chandrachud J).

4. Puttaswamy I (n 1) [125] (Khehar CJ).

5. Puttaswamy I (n 1) [180] (Nariman J).

6. KS Puttaswamy (Retd) v Union of India [2018] 1 SCC 809 ('Puttaswamy II' - Aadhaar judgment).

7. Pegasus Project Investigation - The Wire, 'How Pegasus Spyware Works' (18 July 2021)

8. Digital Personal Data Protection Act 2023 (India), s 4.

9. Constitution of India 1950, art 19(1)(a).

10. MP Sharma v Satish Chandra [1954] SCR 1077.

11. Kharak Singh v State of Uttar Pradesh [1963] 1 SCR 332.

12. Gobind v State of Madhya Pradesh [1975] 2 SCC 148.

13. R Rajagopal v State of Tamil Nadu [1994] 6 SCC 632.

14. People's Union for Civil Liberties v Union of India [1997] 1 SCC 301.

15. PUCL v Union of India [1997] 1 SCC 301 [28].

16. Puttaswamy I (n 1) [497]-[502] (Chandrachud J) - proportionality analysis.

17. Modern Dental College and Research Centre v State of Madhya Pradesh [2016] 7 SCC 353 [65].

18. Puttaswamy I (n 1) [649]-[651] (Chandrachud J) - informational self-determination.

19. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (India), s 2(1).

20. Usha Ramanathan, 'A Jurisprudence of Identity' (2010) 615 Seminar 12.

21. Reetika Khera (ed), The Aadhaar Effect: Why the World's Largest Identity Project Matters (Oxford University Press 2019) ch 5.

22. Aadhaar-Enabled Payment System - Reserve Bank of India, Circular No RBI/2019-20/206 dated 3 March 2020.

23. Information Technology Act 2000 (India), s 69 - power to intercept.

24. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of

Information) Rules 2009 (India).

25. Telecommunication Act 2023 (India), s 20.

26. Telegraph Act 1885 (India), s 5(2) (as amended).

27. Malone v United Kingdom (1984) 7 EHRR 14.

28. Klass v Germany (1978) 2 EHRR 214.

29. Vrinda Bhandari and Rishab Bailey, 'India's Surveillance State' (2020) 13(1) Indian Journal of Law and Technology 1.

30. Nikhil Pahwa and Pranesh Prakash, 'Profiling and Scoring in India' (2022) Internet Freedom Foundation

31. National Intelligence Grid (NATGRID) Project - Ministry of Home Affairs, Annual Report 2022-23, 78.

32. Surveillance Studies Network, Report of the Surveillance Society (Information Commissioner's Office, UK 2006) 4.

33. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology 2018) 13.

34. Personal Data Protection Bill 2019 (India), Draft cl 3.

35. Personal Data Protection Bill 2019 (India), Draft cl 91 - Data Protection Authority.

36. Digital Personal Data Protection Act 2023 (India), s 18 - Data Protection Board.

37. Digital Personal Data Protection Act 2023 (India), s 6.

38. Digital Personal Data Protection Act 2023 (India), s 8.

39. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India), r 3.

40. Digital Personal Data Protection Act 2023 (India), s 17.

41. Justice BN Srikrishna, 'Reflections on India's Data Protection Journey' (2023) 1(1) Indian Data Protection Review 5.

42. Digital Personal Data Protection Act 2023 (India), s 9 - processing of children's data.

43. Lok Sabha Debates, 'Discussion on Digital Personal Data Protection Bill 2023' (3 August 2023) 17th Lok Sabha.

44. General Data Protection Regulation (EU) 2016/679, art 5.

45. General Data Protection Regulation (EU) 2016/679, art 83(5).

46. California Consumer Privacy Act 2018 (USA), Cal Civ Code s 1798.100.

47. Personal Information Protection and Electronic Documents Act 2000 (Canada), s 5.

48. Shreya Singhal v Union of India [2015] 5 SCC 1.

49. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), r 4(2).

50. Central Public Information Officer, Supreme Court of India v Subhash Chandra Agarwal [2019] 10 SCC 1.

51. Right to Information Act 2005 (India), s 8(1)(j).

52. European Convention on Human Rights 1950, art 8.

53. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) CETS No 108, opened for signature 28 January 1981, entered into force 1 October 1985.

54. Justice AP Shah Committee, Report of the Group of Experts on Privacy (Planning Commission of India 2012) 21.

55. Law Commission of India, Personal Data Protection (Law Commission Report No 272, 2018).

56. Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India 2018) 88.