



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.361>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

CHANGING LANDSCAPE OF DIGITAL PRIVACY AND DATA PROTECTION IN INDIA

Shubham Kumar Singh¹

I. ABSTRACT

Digital technology now mediates communication, work, education, commerce, payments and public services, and almost every such activity generates personal data. Individually these fragments appear ordinary, but their aggregation permits detailed profiling, which has turned digital privacy from a question of unauthorised access into one of lawful collection, purpose limitation, retention, automated inference and State access. This article asks whether the Indian statutory framework delivers the standard of informational privacy that the Constitution requires, when most of its substantive obligations remain unenforced and its regulator remains unconstituted. The study is doctrinal, analysing the Constitution, the Digital Personal Data Protection Act, 2023 and the Rules of 2025, the Information Technology Act, 2000, the Telecommunications Act, 2023 and the decisions of the Supreme Court and the High Courts against the General Data Protection Regulation and the European Union Artificial Intelligence Act. The Act builds a coherent architecture of notice, consent, data principal rights, fiduciary duties and graded penalties, but four features weaken it: staged commencement defers the operative obligations to May 2027, so the compensation regime under the Information Technology Act governs until then; the exclusion of publicly available personal data leaves the training of artificial intelligence systems largely outside the Act; the exemption power for State instrumentalities and the power to call for information face constitutional challenge; and the Data Protection Board has no appointed members. The article recommends that Parliament narrow the exemption power, confer a right against solely automated decision-making, and insulate appointments to the Board from executive control.

II. KEYWORDS

¹ B.A.LL.B /2023-2028/7th Semester Student (India). Email: shubhamsinghrajput373@gmail.com

Informational Privacy; Data Protection; DPDP Act 2023; Right to Privacy; Artificial Intelligence.

III. INTRODUCTION

Digital technology now mediates ordinary life. Indians order food, attend classes, transfer money and apply for government services through digital platforms, and every such activity generates information: a phone records location, a payment creates a financial record, a search query discloses what a person wants to know. The important question is not only how much data organisations collect, but what happens to it afterwards.

Privacy was once understood in terms of physical space, personal correspondence and freedom from unwanted interference. The digital environment has widened it to include a person's ability to control information relating to her and to understand how it is collected, processed, stored and shared. This creates a difficult legal problem, because the technology is useful precisely because information can be collected and processed. Banks need information to prevent fraud and government agencies to deliver services, yet unrestricted use of the same information erodes autonomy.

The Supreme Court addressed the constitutional importance of privacy in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge Constitution Bench held that privacy is a constitutionally protected right and linked it with dignity, liberty and autonomy.²

India's framework has developed in response. The Digital Personal Data Protection Act, 2023 provides a dedicated statutory framework for digital personal data,³ and the Digital Personal Data Protection Rules, 2025 followed on 13 November 2025.⁴ Both commence in stages. Sections 1(2), 2, 18 to 26, 35, 38 to 43, 44(1) and 44(3), with rules 1, 2 and 17 to 21, took effect on publication; rule 4 and section 6(9) take effect on 13

² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

⁴ The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Nov. 13, 2025, Gazette of India, Extraordinary, Part II, s. 3(i).

November 2026; and the remaining provisions, which carry the operative obligations, take effect on 13 May 2027.⁵

The research problem arises from the distance between this constitutional promise and its statutory delivery. The provisions that create enforceable duties, confer rights and authorise penalties do not operate until May 2027; the Data Protection Board has no appointed Chairperson or Members; and the provisions governing State access to personal data are before the Supreme Court. This article asks whether the framework, as it stands, secures informational privacy to the standard Article 21 requires, and identifies how Parliament and the Central Government should repair it.

A. Research Questions

The article answers six questions:

1. What does the right to informational privacy under Article 21 protect, and what must a restriction upon it satisfy?
2. Do the provisions on notice, consent, rights and fiduciary obligations give effect to that standard?
3. Do the exemption for notified State instrumentalities and the power to call for information satisfy legality, legitimate aim and proportionality?
4. Does the exclusion of publicly available personal data place the training of artificial intelligence systems outside the Act, and what follows for Data Principals?
5. Can the enforcement architecture make the statutory rights effective, and does the Data Protection Board possess the independence its adjudicatory function requires?
6. What reforms does a comparison with the European instruments suggest?

B. Research Methodology

This article adopts the doctrinal method. It states, interprets and systematises the primary legal materials that govern digital privacy in India and evaluates them

⁵ Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Nov. 13, 2025, Gazette of India, Extraordinary, Part II, s. 3(i).

against the constitutional standard and two comparators, analytically and critically rather than empirically.

The primary Indian sources are the Constitution; the Act of 2023 with the notification issued under it; the Rules of 2025; the Information Technology Act, 2000 with the Rules of 2011, the Interception Rules of 2009 and the directions of the Indian Computer Emergency Response Team; the Telecommunications Act, 2023 with the Interception Rules of 2024; the Payment and Settlement Systems Act, 2007; and the decisions of the Supreme Court and the High Courts. The comparative sources are Regulation (EU) 2016/679, Regulation (EU) 2024/1689 as amended, and Google Spain. The secondary sources are the Shah and Srikrishna Committee Reports, the India AI Governance Guidelines, official notifications and scholarly writing.

Statutory text has been verified against the India Code and the Gazette of India, and pending litigation against the records of the Supreme Court. The study covers Indian law as it stood on 10 October 2026, and citations follow the style of the Indian Law Institute.

IV. RESEARCH AND ANALYSIS

The analysis proceeds under six themes: the constitutional foundation of informational privacy; the statutory framework; State access to personal data and its effect on expression; emerging technologies; sectoral concerns; and enforcement and institutional design.

A. Constitutional Foundation of Informational Privacy

1. Digital Privacy, Data Protection and Personal Data

Digital privacy may be understood as the protection of a person's personal information and digital activities from inappropriate or unauthorised collection, access, use, disclosure or misuse. It is connected with data protection without being identical to it: privacy concerns the individual's interest in controlling personal information, while data protection supplies the mechanisms regulating collection, processing, storage and sharing.

The Act supplies the vocabulary, defining personal data as any data about an individual who is identifiable by or in relation to such data, and allocating three roles: the Data Principal, to whom the data relates; the Data Fiduciary, who determines the purpose and means of processing; and the Data Processor, who processes on a fiduciary's behalf.⁶

Those definitions turn on identifiability, not on sensitivity, and the Act creates no separate category of sensitive personal data. That omission distinguishes the Indian framework both from rule 3 of the Rules of 2011, which treats financial, health and biometric information as sensitive, and from Article 9 of the General Data Protection Regulation.⁷ The value of personal data lies less in single items than in the capacity to combine them, and that capacity to construct detailed profiles is the principal reason data protection now matters.

The scholarship has moved along the same path. The classical formulation treated privacy as a right to be let alone, conceived against intrusion into the domestic sphere.⁸ Later writing treats it as a cluster of related interests,⁹ or as the appropriate flow of information within the norms of the context in which it was disclosed, so that a disclosure made to a physician for treatment is not thereby available to an insurer.¹⁰

Indian writing has urged a similar move away from consent as the sole organising idea, towards accountability for the use made of personal data.¹¹ Both official committees that preceded the Act proceeded on that basis: the Shah Committee recommended national privacy principles,¹² and the Srikrishna Committee proposed the fiduciary model from which the Act takes the term Data Fiduciary.¹³

⁶ Supra note 3, s. 2(t), (j), (i) and (k).

⁷ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Apr. 11, 2011, r. 3.

⁸ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193 (1890).

⁹ Helen Nissenbaum, "Privacy as Contextual Integrity" 79 *Washington Law Review* 119 (2004).

¹⁰ Daniel J. Solove, *Understanding Privacy* (Harvard University Press, Cambridge, 2008).

¹¹ Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins India, Noida, 2018).

¹² Group of Experts on Privacy under the Chairmanship of Justice A.P. Shah, *Report of the Group of Experts on Privacy* (Planning Commission, Government of India, 2012).

¹³ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, 2018).

2. The Constitutional Right to Privacy and the Standard of Review

The Constitution contains no provision titled “Right to Privacy”. The Supreme Court has nevertheless developed privacy protection through the interpretation of fundamental rights, and particularly of Article 21.

The decisive development came in *Puttaswamy*. The nine-judge Bench overruled the earlier line of authority that had denied privacy the status of a fundamental right, and held that privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and of the freedoms guaranteed by Part III.¹⁴

The Court also held that privacy is not absolute. The plurality required a restriction to satisfy legality, in the sense of a law authorising the interference, a legitimate State aim, and proportionality between object and means.¹⁵ The Aadhaar judgment then applied a four-fold test, adding to legitimate goal, suitability and necessity the further requirement of procedural guarantees against abuse.¹⁶ This standard, and not a general appeal to public purpose, governs every provision examined below that authorises the State to collect, demand or process personal data.

3. Major Threats to Digital Privacy

- Unauthorised Collection, Tracking and Profiling: Users accept privacy notices without reading them, which opens a gap between formal and meaningful consent. Applications then track behaviour, social media aggregates posts, connections and browsing into profiles far more detailed than anything consciously supplied, and location tracking adds where a person lives and works. A single breach may expose such information in bulk, and stolen credentials support impersonation and fraud, which the Information Technology Act, 2000 punishes.¹⁷

¹⁴ Supra note 2.

¹⁵ Supra note 2.

¹⁶ *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.

¹⁷ The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C and 66D.

- Biometric Surveillance: Facial recognition and fingerprint systems assist identification, but large-scale collection raises questions of necessity, accuracy and proportionality, as the Aadhaar judgment demonstrates.¹⁸

B. The Digital Personal Data Protection Framework

1. Scope, Grounds for Processing and the Architecture of the Act: The Act of 2023 is India's first dedicated data protection statute, and its stated purpose is to provide for the processing of digital personal data in a manner recognising both the right to protect personal data and the need to process it for lawful purposes.¹⁹
2. Scope and Applicability: Section 3 confines the Act to digital personal data, whether collected in digital form or digitised thereafter, and extends it extraterritorially where processing outside India connects with the offering of goods or services to Data Principals within India.²⁰ Two exclusions matter: processing by an individual for a personal or domestic purpose, and personal data made publicly available by the Data Principal, or made public by another person under a legal obligation in India.²¹ The second carries consequences well beyond its apparent modesty.
3. Grounds for Processing: Section 4 permits processing only for a lawful purpose, meaning any purpose no law expressly forbids, and only on consent or a legitimate use.²² Section 5 requires notice with or before every request for consent, and section 6 places on the Data Fiduciary the burden of proving that it gave notice and obtained valid consent.²³ Section 7 lists nine legitimate uses that dispense with consent, several of which serve the State: the delivery of subsidies, benefits, services, certificates, licences and permits, the performance of State functions under law, and compliance with judgments and orders, alongside medical emergencies, public health

¹⁸ Supra note 16.

¹⁹ Supra note 3, long title.

²⁰ Supra note 3, s. 3(a) and (b).

²¹ Supra note 3, s. 3(c)(i) and (ii).

²² Supra note 3, s. 4.

²³ Supra note 3, s. 6(10).

threats, disasters and employment purposes.²⁴ The Act contains no ground equivalent to the legitimate interests of the controller under Article 6(1)(f) of the European Regulation, so processing must rest on consent or on one of the nine enumerated uses. Section 6 also creates the Consent Manager, through whom a Data Principal may give, manage, review or withdraw consent, and who must register with the Board,²⁵ rule 4 requiring incorporation in India and a minimum net worth.²⁶

4. **Significant Data Fiduciaries:** Section 10 empowers the Central Government to notify any Data Fiduciary or class of fiduciaries as significant, having regard to the volume and sensitivity of the data processed, the risk to Data Principals and the effect on sovereignty, electoral democracy and the security of the State. Such a fiduciary must appoint an India-based Data Protection Officer answerable to its governing body and an independent auditor, and must undertake periodic impact assessments and audits.²⁷ Rule 13 requires these every twelve months, obliges the fiduciary to satisfy itself that its algorithmic software poses no risk, and requires specified data to remain within India.²⁸
5. **Exemptions:** Section 17 withdraws the framework in four ways. Section 17(1) exempts six classes of processing from most of the Act, among them the enforcement of legal claims, judicial and regulatory functions, and the prevention, investigation and prosecution of offences.²⁹ Section 17(2) disapplies the Act altogether, first for processing by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity, the security of the State, friendly relations with foreign States and public order, and secondly for research, archiving and statistical purposes where the data is not used to take any decision specific

²⁴ Supra note 3, s. 7(a) to (i).

²⁵ Supra note 3, s. 6(7), (8) and (9).

²⁶ Supra note 4, r. 4 and First Schedule.

²⁷ Supra note 3, s. 10(1) and (2).

²⁸ Supra note 4, r. 13.

²⁹ Supra note 3, s. 17(1)(a) to (f).

to a Data Principal.³⁰ Section 17(3) permits exemption of notified classes of fiduciaries, including start-ups, and section 17(5) permits the Central Government, within five years, to declare that any provision shall not apply to specified fiduciaries for a specified period.³¹ Section 17(2)(a) deserves particular criticism, because it permits the executive to remove an entire class of processing from the statute by notification. The Act prescribes no criteria beyond the broad heads it recites, requires no reasons, fixes no sunset, provides no independent scrutiny, and leaves the notified instrumentality under no substantive obligation at all, not even the duty to maintain reasonable security safeguards. Article 23 of the European Regulation, by contrast, permits restriction only by a legislative measure that respects the essence of the rights concerned and specifies the purpose, the categories of data and the safeguards.³² A power to exempt that supplies no procedural guarantee against abuse is vulnerable on the four-fold test, and it is now under challenge.

6. Penalties: Section 33 empowers the Board, after an inquiry and a hearing, to impose the penalty the Schedule specifies,³³ which grades penalties by the obligation breached, from rupees 250 crore for failure to take reasonable security safeguards down to rupees 10,000 for breach of the duties of a Data Principal.³⁴ The ceilings are high in absolute terms, but they are fixed sums rather than a proportion of turnover, so their deterrent effect on the largest processors will fall as those undertakings grow. Article 83(5) of the European Regulation, permitting a fine of up to four per cent of worldwide annual turnover, scales with the undertaking.³⁵

³⁰ Supra note 3, s. 17(2)(a) and (b).

³¹ Supra note 3, s. 17(3) and (5).

³² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), O.J. L 119/1, art. 23.

³³ Supra note 3, s. 33.

³⁴ Supra note 3, Schedule.

³⁵ Supra note 32, art. 83(5).

Finally, commencement. The notification of 13 November 2025 brought into force sections 1(2), 2, 18 to 26, 35, 38 to 43, 44(1) and 44(3); section 6(9) follows on 13 November 2026; and the provisions creating the substantive duties examined above follow on 13 May 2027.³⁶ Until then the Act states obligations that bind nobody, and section 43A of the Information Technology Act, 2000 with the Rules of 2011 continues to govern sensitive personal data, because section 44(2)(a), which omits section 43A, has itself not been brought into force.³⁷

Commentators read the statute in sharply different ways. One assessment treats it as a workable, deliberately light-touch instrument suited to a developing digital economy;³⁸ another treats it as friendly to business and to government and hostile to the consumer, chiefly because of the exemptions and the dependence of the regulator on the executive.³⁹ The analysis below supports the second reading on those two points, while accepting that the architecture is sound in design.

C. Notice, Consent and Consent Managers

Consent carries most of the weight in the Indian framework, because the Act offers no general ground of legitimate interests. Section 5 requires notice, with or before every request for consent, of the data proposed to be processed and the purpose, of the manner of exercising rights, and of the manner of complaining to the Board, available in English or any language in the Eighth Schedule to the Constitution.⁴⁰ Rule 3 adds that the notice must stand on its own, use clear and plain language, itemise the data and the purpose, and explain how to withdraw consent as easily as it was given.⁴¹ Section 6 requires consent to be free, specific, informed, unconditional and unambiguous, signified by a clear affirmative action and limited to the data necessary for the specified purpose, and confers a right to withdraw at any time with comparable

³⁶ Supra note 5.

³⁷ Supra note 3, s. 44(2)(a).

³⁸ Anirudh Burman, "Understanding India's New Data Protection Law" (Carnegie Endowment for International Peace, Oct. 3, 2023).

³⁹ Graham Greenleaf, "India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile" 185 *Privacy Laws & Business International Report* 3 (2023).

⁴⁰ Supra note 3, s. 5.

⁴¹ Supra note 4, r. 3.

ease, after which the fiduciary and its processors must cease processing within a reasonable time.⁴²

The difficulty is not that the statute sets a low standard but that the standard resists enforcement. In the digital environment consent collapses into a single click, and the question is whether a Data Fiduciary that satisfies the letter of these provisions, by publishing a long and technically accurate notice, has satisfied their object. Consent should not become a device by which a fiduciary transfers responsibility to the user, and the obligations in section 8 exist precisely because consent alone cannot discharge that responsibility.

D. Rights of Data Principals

Chapter III confers four rights: to obtain a summary of the personal data being processed and the identities of those with whom it has been shared; to correction, completion, updating and erasure; to grievance redressal against the Data Fiduciary or Consent Manager, which the Data Principal must exhaust before approaching the Board; and to nominate another individual to exercise these rights on death or incapacity.⁴³ Section 15 imposes corresponding duties, including a duty not to register a frivolous grievance.⁴⁴ Rule 14 requires a fiduciary to publish the means of making a request, maintain a grievance redressal system and respond within ninety days,⁴⁵ a generous period beside the one month Article 12(3) of the European Regulation allows,⁴⁶ and long enough to defeat a correction request where inaccurate information is presently affecting a person's employment or credit.

Two limitations qualify these rights. They become meaningful only through effective procedures, and until the Board is constituted the only forum is the fiduciary's own grievance mechanism. Further, Chapter III does not commence until 13 May 2027, so no Data Principal can presently assert any of them. The Act also omits portability

⁴² Supra note 3, s. 6(1) to (6).

⁴³ Supra note 3, ss. 11 to 14.

⁴⁴ Supra note 3, s. 15.

⁴⁵ Supra note 4, r. 14.

⁴⁶ Supra note 32, art. 12(3).

under Article 20 of the European Regulation and the right against solely automated decisions under Article 22.

E. Obligations of Data Fiduciaries and Significant Data Fiduciaries

An organisation that collects personal data should ask not whether collection is technically possible but whether the data is necessary. Section 8 converts that proposition into enforceable duties.

Section 8 makes the Data Fiduciary responsible for compliance in respect of any processing it undertakes or that a processor undertakes on its behalf, notwithstanding any agreement to the contrary or any failure by the Data Principal to perform her duties. It permits a processor to be engaged only under a valid contract; requires the completeness and accuracy of data used to make a decision affecting the Data Principal; requires technical and organisational measures and reasonable security safeguards against a breach; requires intimation of a breach to the Board and to each affected Data Principal; requires erasure on withdrawal of consent or when the purpose is no longer served; and requires an effective grievance redressal mechanism.⁴⁷

The practices of responsible data governance correspond to these duties rather than standing apart from them. Controlled access and security measures answer to section 8(5) with rule 6, which requires encryption, obfuscation, masking or virtual tokens, access controls, logs and monitoring, backups and retention of logs for one year; and retention answers to section 8(7) with section 8(8), which deems a purpose no longer served where the Data Principal neither approaches the fiduciary nor exercises her rights for the prescribed period.⁴⁸

These obligations matter because individuals hold little bargaining power when they use essential services. A person may have no realistic alternative to supplying information to a bank or a government service, and there the statutory duty, not the bargain, protects her.

⁴⁷ Supra note 3, s. 8(1) to (10).

⁴⁸ Supra note 4, rr. 6 and 7.

F. The Digital Personal Data Protection Rules, 2025 and the Commencement Scheme

The Central Government notified the Digital Personal Data Protection Rules, 2025 by G.S.R. 846(E) dated 13 November 2025. The Rules translate the general obligations of the Act into operative requirements, prescribing the content of the notice, the registration of Consent Managers, the standards applying to State processing, security safeguards, breach intimation, the data of children, the obligations of Significant Data Fiduciaries, the exercise of rights, transfer outside India, the constitution of the Board, appeals, and the power to call for information.⁴⁹

Rule 1 staggers commencement. Rules 1, 2 and 17 to 21 came into force on publication, so the only operative provisions are those establishing the administrative machinery of the Board; rule 4 follows on 13 November 2026, and rules 3, 5 to 16, 22 and 23 on 13 May 2027.⁵⁰ The Ministry of Electronics and Information Technology placed before stakeholders in January 2026 a proposal to advance the obligations of Significant Data Fiduciaries, including the cross-border restrictions in rules 13(4) and 15, but had notified no such change when this article was finalised.⁵¹

The consequence deserves emphasis, because much published commentary treats the framework as operative. For the eighteen months from November 2025 the Act confers no right on any Data Principal, imposes no notice or consent obligation on any fiduciary, authorises no penalty and gives the Board no power to inquire. Data protection in India during that period rests where it rested before 2023, on section 43A of the Information Technology Act, 2000 and the Rules of 2011, supplemented by the directions of the Indian Computer Emergency Response Team and by sectoral regulation.⁵²

⁴⁹ Supra note 4, r. 1.

⁵⁰ Supra note 4, r. 1(2) to (4).

⁵¹ Ministry of Electronics and Information Technology, Government of India, stakeholder consultation on advancing the commencement of the obligations of Significant Data Fiduciaries (Jan. 23, 2026).

⁵² Graham Greenleaf, "Rules Expand India's Data Privacy Law, but Slowly" 199 *Privacy Laws & Business International Report* 19 (2026).

G. Comparative Perspective: The General Data Protection Regulation and the European Union Artificial Intelligence Act

Two European instruments supply the natural comparators, because the Indian framework borrows its vocabulary from the first and must address the subject matter of the second: Regulation (EU) 2016/679,⁵³ and Regulation (EU) 2024/1689, which entered into force on 1 August 2024.⁵⁴

On the grounds for processing, the European instrument offers six lawful bases and permits processing necessary for the legitimate interests of the controller subject to a balancing test.⁵⁵ The Indian Act permits consent or one of nine enumerated uses and offers no balancing test, so it is the more rigid and the narrower, because several of the nine serve the State rather than the private processor. On rights, the European instrument confers access, rectification, erasure, restriction, portability and objection, and a right against decisions based solely on automated processing,⁵⁶ while the Indian Act omits the last four, and the omission of any control over automated decisions is the most significant.

On cross-border transfers, the two instruments invert each other. Chapter V of the European instrument prohibits transfer unless an adequacy decision, standard contractual clauses, binding corporate rules or a derogation permits it, so transfer is conditional by default.⁵⁷ Section 16 of the Indian Act permits transfer unless the Central Government notifies a restricted country, so transfer is permissive by default and operates on a blacklist.⁵⁸ The Indian model offers the weaker guarantee, because personal data may lawfully leave India for a jurisdiction with no comparable protection until the Central Government acts. On enforcement, the European instrument requires independent supervisory authorities appointed through a

⁵³ Supra note 32.

⁵⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), O.J. L, 12.7.2024.

⁵⁵ Supra note 32, art. 6(1).

⁵⁶ Supra note 32, arts. 15 to 22.

⁵⁷ Supra note 32, arts. 44 to 49.

⁵⁸ Supra note 3, s. 16(1).

transparent procedure,⁵⁹ while the Indian Act vests appointment, terms of service and removal in the Central Government.

On artificial intelligence, the contrast is one of regulatory choice. The European instrument classifies systems by risk and attaches graded obligations, the prohibitions applying from February 2025, the obligations of providers of general-purpose models from August 2025 and the transparency obligations from August 2026, while Regulation (EU) 2026/1744 deferred the high-risk obligations to December 2027 and August 2028.⁶⁰ India has taken a different route: the India AI Governance Guidelines of 5 November 2025 decline to propose a standalone statute and rely instead on existing law, supplemented by voluntary principles.⁶¹ The standard commentary on the European Regulation⁶² and the comparative literature on Asian data privacy laws⁶³ supply the fuller treatment a dedicated comparative study would require.

H. Surveillance, Expression and the Limits of State Access

1. Statutory Routes for State Access to Personal Data

Government access to personal data presents the hardest question in this field. The State may legitimately require information to prevent crime, protect national security and deliver public services, while extensive surveillance interferes with privacy. The question is not whether surveillance serves a public purpose but whether the particular measure satisfies the four-fold test, which cannot be applied in the abstract, so the five routes by which the State lawfully obtains personal data must be identified first.

2. Interception of Telecommunication Messages

The leading authority is *People's Union for Civil Liberties v. Union of India*, in which the Supreme Court held that telephone tapping infringes Articles 19(1)(a) and 21

⁵⁹ *Supra* note 32, arts. 51 to 54.

⁶⁰ Regulation (EU) 2026/1744, O.J. L, 24.7.2026.

⁶¹ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (Nov. 5, 2025).

⁶² Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, Oxford, 2020).

⁶³ Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, Oxford, 2014).

unless it follows a procedure established by law, and laid down safeguards requiring the order to issue from the Home Secretary, limiting its life and providing for review by a committee, later embodied in rule 419A of the Indian Telegraph Rules, 1951.⁶⁴

The power now rests in section 20 of the Telecommunications Act, 2023, in force from 26 June 2024,⁶⁵ and the Interception Rules of 2024 supply the procedure, superseding rules 419 and 419A so far as telecommunication services are concerned.⁶⁶ Those Rules reproduce the substance of the safeguards the Court required and add to them. An order must issue from the Union Home Secretary or a State Home Secretary, and in unavoidable circumstances from a specially authorised Joint Secretary. An emergent order must be confirmed within seven working days, failing which interception must cease and the messages become inadmissible. An order lasts sixty days and may not be extended beyond one hundred and eighty, and a Review Committee chaired by the Cabinet Secretary, or the Chief Secretary in a State, must meet every two months and may set aside a non-conforming order and direct destruction of the material.⁶⁷

One point of commencement requires care. Section 60 of the Act of 2023, which repeals the Indian Telegraph Act, 1885, was not brought into force on 26 June 2024 and has not been notified since,⁶⁸ so the Act of 1885 remains on the statute book although interception is governed by section 20 and the Rules of 2024.

3. Interception, Monitoring and Decryption of Information

Section 69 of the Information Technology Act, 2000 empowers the Central Government, a State Government or an authorised officer to direct the interception, monitoring or decryption of information in any computer resource on the grounds that provision specifies,⁶⁹ and the Rules of 2009 prescribe the procedure.⁷⁰ This route

⁶⁴ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

⁶⁵ The Telecommunications Act, 2023 (Act 44 of 2023), s. 20.

⁶⁶ Ministry of Communications, Department of Telecommunications, Notification dated June 21, 2024, bringing ss. 1, 2, 10 to 30, 42 to 44, 46, 47, 50 to 58, 61 and 62 of the Telecommunications Act, 2023 into force with effect from June 26, 2024.

⁶⁷ The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Dec. 6, 2024.

⁶⁸ *Supra* note 66.

⁶⁹ *Supra* note 17, s. 69.

⁷⁰ The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

reaches stored data and communications over internet services, which section 20 does not. Section 69A separately permits the blocking of public access to information, and the Supreme Court upheld it in *Shreya Singhal v. Union of India* as narrowly drawn and attended by procedural safeguards.⁷¹

4. Exemption of State Instrumentalities

Section 17(2)(a) permits the Central Government to notify an instrumentality of the State in respect of which the Act shall not apply, in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or the prevention of incitement to a cognizable offence.⁷² Such a notification removes the obligations of notice, consent, purpose limitation, accuracy, security, breach intimation and erasure, and the rights of the Data Principal, entirely. The only countervailing provision is rule 5 with the Second Schedule, which prescribes standards of lawfulness, necessity, accuracy, retention and accountability where the State processes data to deliver a subsidy or service, and those standards do not apply to a notified instrumentality.⁷³

5. Power to Call for Information

Section 36 empowers the Central Government to require the Board, any Data Fiduciary or any intermediary to furnish such information as it may call for, and rule 23 confines the power to the purposes in the Seventh Schedule, namely the use of personal data by the State in the interests of sovereignty, integrity and security, the performance of State functions, and the assessment of whether a fiduciary should be notified as significant.⁷⁴ Rule 23(2) permits the Central Government to forbid disclosure of the request to the Data Principal, where disclosure would prejudice the sovereignty, integrity or security of India.⁷⁵

Applying the four-fold test produces a mixed result. The interception regime under the Act of 2023 satisfies legality, pursues a legitimate aim and supplies procedural

⁷¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁷² Supra note 3, s. 17(2)(a).

⁷³ Supra note 4, r. 5 and Second Schedule.

⁷⁴ Supra note 3, s. 36.

⁷⁵ Supra note 4, r. 23 and Seventh Schedule.

guarantees in the form of a named competent authority, time limits, a review committee and destruction requirements, so the question concerning it is one of compliance rather than design, and section 69 of the Act of 2000 stands on a similar footing.

Section 17(2)(a), by contrast, supplies no procedural guarantee at all, while removing every substantive protection. Section 36 with rule 23 raises a related difficulty, because rule 23(2) can prevent the Data Principal from ever learning that her data was furnished, which removes the factual basis for any remedy. The following safeguards serve as the benchmark against which each route should be measured, and sections 17(2)(a) and 36 fail several of them:

- Clear legal authority;
- Defined purposes;
- Limited collection;
- Restricted retention;
- Access controls;
- Oversight mechanisms;
- Accountability; and
- Remedies for unlawful interference.

6. Privacy, the Chilling Effect and Freedom of Expression

Privacy and freedom of expression support each other. A person who believes that every online activity is monitored may hesitate to express an opinion, join a lawful association or participate in public debate, and the resulting self-censorship reduces the freedom Article 19(1)(a) guarantees. The task is to keep legitimate regulation of fraud, harassment and unlawful content from intruding upon constitutional freedoms further than the object requires.

Two decisions mark the limits. In *Shreya Singhal* the Supreme Court struck down section 66A of the Information Technology Act, 2000 for vagueness and overbreadth, holding that it failed to distinguish advocacy from incitement and that the chilling

effect on protected speech was itself a constitutional vice.⁷⁶ In *Anuradha Bhasin v. Union of India* the Court held that the freedoms of speech and of trade through the internet attract constitutional protection, that every order suspending internet services must be published, record reasons, satisfy proportionality and remain subject to periodic review, and that indefinite suspension is impermissible.⁷⁷ Constitutional rights do not lose their force because the medium has changed. The constitutional literature traces the same movement, from a tendency test towards the requirement of a proximate connection with incitement.⁷⁸

The connection to the present framework is direct. The absence of any exemption for processing undertaken for journalistic purposes, and the substitution of section 8(1)(j) of the Right to Information Act, 2005 by section 44(3) of the Act, both bear on the ability of journalists and researchers to publish information that identifies individuals, and both form part of the pending challenge described below.

I. Emerging Technologies

1. Artificial Intelligence and Privacy

Artificial intelligence presents the most demanding privacy problem of the coming years, because these systems process quantities of information beyond human review and infer attributes nobody disclosed. The question for a lawyer is which provisions govern that capability, and the answer in India is that very few do.

The decisive provision is section 3(c)(ii). The Act does not apply to personal data the Data Principal has made publicly available, or that another person has made public under a legal obligation in India.⁷⁹ A developer who collects personal data from public social media profiles, published photographs or public registers in order to train a model therefore processes data to which the Act does not apply. No notice or consent is required, the duties in section 8 do not attach and the rights in sections 11 to 14 do not arise, so a Data Principal cannot ask what data about her entered a training set,

⁷⁶ Supra note 71.

⁷⁷ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

⁷⁸ Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (Oxford University Press, New Delhi, 2016).

⁷⁹ Supra note 3, s. 3(c)(ii).

nor require its correction or erasure. The European instrument contains no equivalent carve-out: public availability does not remove personal data from its scope, and the right to erasure survives publication.⁸⁰ The Indian exclusion is accordingly the single largest gap in the framework as it applies to model development.

The second relevant provision is the research exemption. Section 17(2)(b) disapplies the Act to processing necessary for research, archiving or statistical purposes, provided the data is not used to take any decision specific to a Data Principal and the processing follows the standards rule 16 prescribes.^{81 82} The exemption therefore protects research, not deployment.

The third source is policy rather than law. The India AI Governance Guidelines are voluntary and technology-neutral, declining to recommend a standalone statute and relying on existing law together with principles of accountability, transparency, fairness and human oversight.⁸³

The Guidelines also acknowledge the gaps this reliance leaves, identifying as open questions the scope of the exemption for training on publicly available personal data, whether collection and purpose limitation fit the way these systems operate, and how notice can be given dynamically. An admitted gap addressed by a voluntary principle remains a gap.

Regulation (EU) 2024/1689 shows what a binding instrument looks like. It classifies systems by risk, prohibits certain practices outright, imposes obligations on providers of general-purpose models, requires disclosure where content is generated or manipulated, and requires human oversight of high-risk systems.^{84 85}

Five concerns commonly raised about these systems can each be tied to a provision, or to its absence.

⁸⁰ Supra note 32, arts. 14 and 17.

⁸¹ Supra note 3, s. 17(2)(b).

⁸² Supra note 4, r. 16.

⁸³ Supra note 61.

⁸⁴ Supra note 54, arts. 14 and 50.

⁸⁵ Supra note 60.

Training data: whether personal information forms part of the training corpus is governed by section 3(c)(ii) and, for research, by section 17(2)(b) with rule 16, and where the data was publicly available neither confers any right on the individual.

Profiling: the Act confers no right to object to profiling and none against a decision taken solely by automated means, in contrast to Article 22 of the European instrument.⁸⁶ The nearest Indian provision, section 8(3), addresses the quality of the input rather than the legitimacy of the inference.⁸⁷

Transparency: section 5 requires notice of the data processed and the purpose, but no explanation of the logic of processing, which Article 13(2)(f) of the European instrument requires.⁸⁸

Accuracy: section 8(3) imposes the accuracy duty and section 12 confers the right to correction, but both reach the data held by the fiduciary rather than the trained parameters of a model, and neither commences before 13 May 2027.⁸⁹

Human oversight: Indian law requires none, while Article 14 of the European instrument requires high-risk systems to be designed so that natural persons can oversee them effectively.⁹⁰

Privacy and accountability must therefore enter the design of these systems from the outset. Parliament should qualify section 3(c)(ii) so that publicly available personal data loses the protection of the Act only where it is processed for a purpose compatible with that for which it was made public, and should confer a right against decisions taken solely by automated means.

2. Facial Recognition and Biometric Data

Biometric information differs from a password, which can be changed once compromised; a face or a fingerprint cannot be replaced. Facial recognition assists law enforcement and authentication, but large-scale deployment creates the possibility of

⁸⁶ Supra note 32, art. 22.

⁸⁷ Supra note 3, s. 8(3).

⁸⁸ Supra note 32, art. 13(2)(f).

⁸⁹ Supra note 3, s. 12.

⁹⁰ Supra note 54, art. 14.

continuous identification, so the legal question should focus on purpose, necessity, accuracy, security, retention and oversight. Rule 3 of the Rules of 2011 classifies biometric information as sensitive personal data, so a body corporate holding it must presently maintain reasonable security practices and is liable in compensation under section 43A.^{91 92}

The Act of 2023 creates no special category, so from May 2027 biometric data will attract the same obligations as a postal address, in contrast to Article 9 of the European Regulation, which prohibits processing biometric data for unique identification subject to enumerated conditions.⁹³ The Aadhaar judgment supplies the constitutional test, and it is that test, rather than any statutory classification, that presently constrains large-scale biometric identification by the State.⁹⁴

J. The Right to Erasure and Digital Memory

Information published years ago continues to appear in search results after the circumstances that produced it have changed, which raises the question whether it should remain accessible indefinitely.

The statutory position is narrow. Section 12 confers a right to correction, completion, updating and erasure of personal data for which the Data Principal previously gave consent, and erasure may be refused where retention is necessary for the specified purpose or for compliance with law;⁹⁵ section 8(7) imposes an independent duty of erasure.⁹⁶ Three limitations confine these provisions. They bind only a Data Fiduciary, so they do not reach a search engine indexing a lawfully published page; they do not apply to personal data excluded by section 3(c)(ii); and they do not commence until 13 May 2027.

The High Courts have developed the remedy under Article 21 in the absence of statute. In *Jorawar Singh Mundy v. Union of India* the Delhi High Court granted

⁹¹ Supra note 7, r. 3.

⁹² Supra note 17, s. 43A.

⁹³ Supra note 32, art. 9(1).

⁹⁴ Supra note 16.

⁹⁵ Supra note 3, s. 12.

⁹⁶ Supra note 3, s. 8(7).

interim relief to an acquitted petitioner, directing that the judgment be removed from search results pending final adjudication.⁹⁷ In *Vysakh K.G. v. Union of India* the Kerala High Court declined to recognise a free-standing right to the erasure of judgments without a statutory basis, holding their publication to be protected speech, while accepting that in a fit case the court may permit de-indexing.⁹⁸

In *Laksh Vir Singh Yadav v. Union of India* the Delhi High Court held that informational privacy requires protection under Article 21 even without specific legislation, and that search engines have no legal basis for maintaining unlimited name-based access to records of persons acquitted or discharged or to private disputes. It directed search engines to de-index name-based results linking to judgments, orders and news reports in cases of acquittal, discharge, quashing, settlement or private dispute, and directed legal databases to restrict name-based search while retaining access by case number, citation, court and date. It ordered no deletion, so the judgments remain available through the courts' own records.⁹⁹

The European position arrived earlier and by a different route. In *Google Spain* the Court of Justice of the European Union held that the operator of a search engine processes personal data as a controller, and may be required to remove links to lawfully published pages from the results displayed for a search on a person's name where the information is inadequate, irrelevant or excessive, subject to a balance against the public interest in access.¹⁰⁰ Article 17 of the European Regulation subsequently codified a right to erasure, with exceptions for freedom of expression, legal obligations, archiving and research.¹⁰¹ The difference is structural: the European right binds the search engine directly and is statutory, while the Indian remedy binds it only by order of a writ court, and the statutory right in section 12 is not yet in force.

⁹⁷ *Jorawar Singh Mundy v. Union of India*, 2021 SCC OnLine Del 2306.

⁹⁸ *Vysakh K.G. v. Union of India*, 2022 SCC OnLine Ker 7337.

⁹⁹ *Laksh Vir Singh Yadav v. Union of India*, W.P.(C) No. 1021 of 2016 and connected matters, decided on May 29, 2026 (Del.).

¹⁰⁰ *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (CJEU, Grand Chamber, May 13, 2014).

¹⁰¹ *Supra* note 32, art. 17.

The competing interests remain genuine, because journalists, researchers and the public have legitimate interests in continued access and open justice requires that judgments remain available. The balance the Delhi High Court struck, restricting name-based retrieval while preserving the record, offers a workable reconciliation that Parliament should place on a statutory footing.

K. Sectoral Concerns

1. Children and Digital Privacy

Children use social media, educational applications, games and video platforms heavily, and may not understand the long-term consequences of sharing information that remains available for years.

The Act addresses this directly. Section 9 requires verifiable consent from a parent or lawful guardian before a Data Fiduciary processes the personal data of a child, forbids processing likely to cause any detrimental effect on a child's well-being, and forbids tracking, behavioural monitoring and targeted advertising directed at children.¹⁰²

Rule 10 prescribes how verifiable consent is obtained, requiring the fiduciary to satisfy itself that the person consenting is an identifiable adult, using reliable identity and age details it holds, details voluntarily furnished, or a virtual token issued by an authorised entity; rule 11 governs consent by the guardian of a person with disability, and rule 12 exempts specified classes, including healthcare professionals and educational institutions, from parts of section 9.¹⁰³ Breach of section 9 attracts a penalty of up to rupees 200 crore.¹⁰⁴

2. Corporate Data Collection and the Digital Economy

Businesses collect personal information to provide services, prevent fraud and understand customers. The difficulty arises when collection becomes excessive, or when information supplied for one purpose is combined with behavioural data to build a profile the consumer never anticipated. The Act confines processing to a lawful

¹⁰² Supra note 3, s. 9(1) to (3).

¹⁰³ Supra note 4, rr. 10 to 12.

¹⁰⁴ Supra note 3, Schedule, entry 3.

purpose and limits consent to the data necessary for that purpose,¹⁰⁵ and requires erasure once the purpose is no longer served.¹⁰⁶

3. Financial and Health Data: The Loss of the Sensitive Category

Financial and health information are the two categories whose protection the Act reduces rather than enhances, and both presently depend on instruments the Act will displace.

Financial information attracts regulation from two directions. Rule 3(ii) of the Rules of 2011 treats bank account, credit card and other payment instrument details as sensitive personal data,¹⁰⁷ and section 43A of the Information Technology Act, 2000 renders a body corporate that fails to maintain reasonable security practices liable to pay compensation.¹⁰⁸ Separately, the Reserve Bank of India, exercising its power under the Payment and Settlement Systems Act, 2007, has directed all system providers to store payment system data only in India.¹⁰⁹ That direction survives the Act, because section 16(2) preserves any law affording a higher degree of protection or a greater restriction on transfer.¹¹⁰

Health information likewise receives no special treatment under the Act. The protection presently available rests on rule 3(i) of the Rules of 2011, which treats physical, physiological and mental health condition, medical records and history as sensitive personal data, read with section 43A.¹¹¹

When those provisions give way in May 2027, health and financial data will be governed by the same provisions as any other personal data. Article 9 of the European Regulation, by contrast, prohibits the processing of data concerning health subject to

¹⁰⁵ Supra note 3, ss. 4 and 6(2).

¹⁰⁶ Supra note 3, s. 8(7).

¹⁰⁷ Supra note 7, r. 3(ii).

¹⁰⁸ Supra note 17, s. 43A.

¹⁰⁹ Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153, DPSS.CO.OD No. 2785/06.08.005/2017-2018 (Apr. 6, 2018).

¹¹⁰ Supra note 3, s. 16(2).

¹¹¹ Supra note 7, r. 3(i).

enumerated conditions.¹¹² The levelling down of these categories is a deliberate design choice, and one Parliament should reconsider.

4. Cross-Border Data Transfers

Digital services do not operate within national borders. A person in India may use an application incorporated in one country whose data is stored in another, which raises questions about the applicable law, the location of storage, who may obtain access, and how an individual obtains a remedy.

The Act answers these questions only in part. Section 3(b) extends the Act to processing outside India where that processing connects with the offering of goods or services to Data Principals within India, so the question of applicable law has a statutory answer.¹¹³ Section 16 permits the Central Government to restrict transfer to a notified country, and preserves any other law affording a higher degree of protection.¹¹⁴

Rule 15 adds that a fiduciary may transfer personal data outside India subject to the requirements the Central Government may specify in respect of making such data available to a foreign State.¹¹⁵ Neither section 16 nor rule 15 is in force: both commence on 13 May 2027, and the Central Government has notified no restricted country.¹¹⁶

The comparison with Chapter V of the European Regulation explains why this matters. There, the lawfulness of a transfer turns on the protection available in the destination; here, transfer is lawful unless the Central Government forbids it, and the destination's law is irrelevant.¹¹⁷

The remaining questions have no satisfactory statutory answer. The Act does not require a fiduciary to disclose where personal data is stored, so the Data Principal cannot discover the location from the notice under section 5. Investigation of a breach occurring abroad depends on the cooperation of the foreign processor, because the

¹¹² Supra note 32, art. 9.

¹¹³ Supra note 3, s. 3(b).

¹¹⁴ Supra note 3, s. 16.

¹¹⁵ Supra note 4, r. 15.

¹¹⁶ Supra note 51.

¹¹⁷ Supra note 32, arts. 44 to 49.

Board has no process running outside India, and an order of the Board binds an entity with no Indian presence only so far as it chooses to comply. A framework asserting extraterritorial application without a corresponding enforcement mechanism secures less than it promises.

L. Enforcement and Institutional Design

1. Data Breaches, Security Safeguards and Incident Reporting

Privacy protection cannot be separated from cybersecurity, because a privacy framework may regulate why information is collected while technical safeguards protect it afterwards.

Two distinct reporting regimes govern this subject, and only one presently binds anyone. The Indian Computer Emergency Response Team issued directions on 28 April 2022 under section 70B(6) of the Information Technology Act, 2000 requiring a service provider, intermediary, data centre, body corporate or Government organisation to report the listed cybersecurity incidents within six hours of noticing them.¹¹⁸ Failure to comply is punishable under section 70B(7). The six-hour clock is among the shortest in the world, and it is the clock an Indian organisation must presently observe.¹¹⁹

The second regime takes effect on 13 May 2027. Section 8(5) requires a Data Fiduciary to protect personal data in its possession or control by taking reasonable security safeguards against a breach,¹²⁰ and rule 6 specifies those safeguards, namely encryption, obfuscation, masking or virtual tokens, access controls, logs and monitoring, backups, retention of logs for one year, and contractual security provisions binding processors.¹²¹ Section 8(6) requires intimation of a breach to the Board and to each affected Data Principal.¹²²

¹¹⁸ Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In, Apr. 28, 2022.

¹¹⁹ Supra note 17, s. 70B(6).

¹²⁰ Supra note 3, s. 8(5).

¹²¹ Supra note 4, r. 6.

¹²² Supra note 3, s. 8(6).

Rule 7 prescribes that form and sets two timelines. The fiduciary must intimate each affected Data Principal without delay, in concise and plain language, describing the nature, extent and timing of the breach, its likely consequences and the mitigation measures taken. It must also intimate the Board without delay, and furnish within seventy-two hours of becoming aware, or such longer period as the Board allows, the broad facts and causes, the remedial measures and a report of the intimations given.¹²³

The penalties are severe: up to rupees 250 crore for failure to take reasonable security safeguards, the highest ceiling in the Schedule, and up to rupees 200 crore for failure to intimate a breach.¹²⁴ These figures apply only from 13 May 2027. Until then the compensation framework remains section 43A read with the Rules of 2011, under which an affected person claims compensation before the adjudicating officer rather than relying on a regulator.^{125 126}

The two regimes are cumulative rather than alternative, and they do not align. Their triggers differ, because a cybersecurity incident need not involve personal data at all, while a personal data breach need not involve any cybersecurity incident; their recipients differ, one reporting to the Response Team and the other to the Board and to each affected individual; and their clocks differ, one running for six hours from notice and the other requiring a report within seventy-two. After May 2027 a single incident may require three notifications on two timetables, with a fourth where a sectoral regulator imposes its own. Parliament or the Central Government should harmonise them, because inconsistent duties waste the response capacity that the first hours of an incident most require.

2. The Data Protection Board of India

Section 18 establishes the Data Protection Board of India as a body corporate, and sections 19 to 26 govern its composition and working. The Board consists of a Chairperson and such number of Members as the Central Government may notify, appointed by it in the prescribed manner, each a person of ability, integrity and

¹²³ Supra note 4, r. 7.

¹²⁴ Supra note 3, Schedule.

¹²⁵ Supra note 17, s. 43A.

¹²⁶ Supra note 7.

standing with special knowledge in the enumerated fields, of whom at least one must be an expert in law.¹²⁷ Rules 17 to 21, with the Fourth, Fifth and Sixth Schedules, prescribe the terms of appointment, the salary and the procedure of the Board.¹²⁸

The Board's powers lie in sections 27 and 28. On receiving intimation of a breach it may direct urgent remedial measures, inquire and impose a penalty; it may act on a complaint by a Data Principal, on a reference by the Central Government, on a direction of a court, and on complaints concerning Consent Managers. It must give a hearing and record reasons, and its directions bind.¹²⁹ Section 29 provides an appeal to the Telecom Disputes Settlement and Appellate Tribunal within sixty days, and section 30 makes the Tribunal's orders executable as a decree of a civil court.^{130 131}

The Board's present status requires accurate statement, because published accounts conflict. Sections 18 to 26 came into force on 13 November 2025, so the Board exists in law.¹³² The Ministry of Electronics and Information Technology issued a notice dated 6 May 2026 inviting applications for one Chairperson and four Members, followed by a recruitment advertisement in Employment News on 6 June 2026 which a written answer in the Lok Sabha on 12 August 2026 confirmed.¹³³ No appointment notification has been published. Some secondary sources report that appointments were formalised on 6 June 2026; that is the date of the advertisement, and no Gazette notification supports the report. Sections 27, 28, 33 and 34, which confer the powers to inquire and to penalise, commence on 13 May 2027, so the Board can presently neither receive a complaint nor pass an order.

The Board's independence raises a distinct concern. The Central Government determines the number of Members, appoints them, prescribes their salary and terms by rule, and may refer matters to the Board and seek reconsideration of its directions.

¹²⁷ Supra note 3, ss. 18 and 19.

¹²⁸ Supra note 4, rr. 17 to 21.

¹²⁹ Supra note 3, ss. 27 and 28.

¹³⁰ Supra note 3, ss. 29 and 30.

¹³¹ Supra note 4, r. 22.

¹³² Supra note 5.

¹³³ Ministry of Electronics and Information Technology, Government of India, Invitation of applications for the posts of Chairperson and Members of the Data Protection Board of India, F. No. 2(1)/2026-Pers.I (May 6, 2026).

The same Government is the largest processor of personal data in the country, the beneficiary of the exemption in section 17(2)(a) and the holder of the power to call for information under section 36.

Article 52 of the European Regulation requires a supervisory authority to act with complete independence, and Articles 53 and 54 require a transparent appointment procedure and a fixed term with defined grounds of dismissal.¹³⁴ The Indian design does not meet that standard, and the independence of the Board forms one ground of the challenge described below. A law may confer rights, but only an institution capable of acting against the State can make those rights effective.

3. Judicial Developments

The decisions that shape this field have been analysed where they arise. This section turns to the litigation that will determine the framework's constitutional fate.

- The Pending Challenge to the Framework: The most consequential litigation in this field is pending. On 16 February 2026 the Supreme Court issued notice on a batch of writ petitions challenging the Act and the Rules.¹³⁵ Four matters are challenged. The first is section 44(3), which substitutes section 8(1)(j) of the Right to Information Act, 2005 so that information relating to personal information is exempt from disclosure, removing the public-interest override and the test of relationship to public activity.¹³⁶ ¹³⁷ The second is section 36 with rule 23. The third is the absence of any exemption for processing for public-interest purposes, including journalism. The fourth is the institutional independence of the Board.

The grounds pleaded are that the scheme is manifestly arbitrary and unreasonable and violates Articles 14, 19(1)(a) and 21.¹³⁸ The Court declined to stay the operation of

¹³⁴ Supra note 32, arts. 52 to 54.

¹³⁵ *Venkatesh Nayak v. Union of India*, W.P.(C) No. 177 of 2026; *The Reporters Collective Trust v. Union of India*, W.P.(C) No. 211 of 2026; *National Campaign for Peoples' Right to Information v. Union of India*, W.P.(C) No. 212 of 2026 (SC).

¹³⁶ Supra note 3, s. 44(3).

¹³⁷ The Right to Information Act, 2005 (Act 22 of 2005), s. 8(1)(j).

¹³⁸ The Constitution of India, arts. 14, 19 and 21.

the framework and referred the questions concerning the amendment of the Right to Information Act, 2005 to a larger bench. Section 44(3) commenced on 13 November 2025, so the challenge to it concerns an operative provision, while the challenge to section 36 concerns a provision commencing on 13 May 2027.

This litigation tests two conclusions reached above: that section 36 with rule 23 supplies no procedural guarantee to the individual whose data is furnished, and that an adjudicatory body appointed and remunerated by its principal respondent cannot discharge the function the Act assigns to it.

V. RECOMMENDATIONS

The recommendations that follow proceed from the defects the analysis has identified.

1. **Strengthen Literacy, Design and Transparency:** Individuals should be educated about data collection, tracking and privacy settings; organisations should adopt privacy by design, collect no more than the stated purpose requires, and maintain encryption, access controls and regular audits; and privacy notices should be written in clear language. Children's data warrants additional protection alongside age-appropriate digital education.
2. **Ensure Proportionate Surveillance:** Parliament should narrow section 17(2)(a) so that a notification under it states reasons, is laid before Parliament, carries a sunset and preserves at least the duties of security and accuracy; and the non-disclosure power in rule 23(2) should be confined to a defined period, after which the Data Principal is informed.¹³⁹
3. **Strengthen Institutional Capacity:** The Central Government should complete the appointments to the Data Protection Board without further delay, and Parliament should insulate those appointments by prescribing a selection committee with judicial and independent membership, a fixed term and defined grounds of removal. Individuals require practical mechanisms of complaint and redress.

¹³⁹ Supra note 3, s. 17(2)(a).

4. Develop Responsible AI Practices: Parliament should qualify section 3(c)(ii) so that publicly available personal data loses the protection of the Act only where it is processed for a purpose compatible with that for which it was made public, and should confer a right against decisions taken solely by automated means.¹⁴⁰
5. Harmonise Breach Reporting: The six-hour duty under the directions of 2022 and the duties under section 8(6) with rule 7 should be harmonised, so that a single incident produces one timetable and one set of reports rather than parallel obligations to different authorities.
6. Restore Protection for Special Categories: Parliament should reinstate a category of sensitive personal data covering health, biometric and financial information, so that the repeal of the Rules of 2011 in May 2027 does not reduce the protection those categories presently receive.

VI. CONCLUSION

Personal information is no longer confined to documents kept inside homes and offices. It moves constantly through phones, applications, payment systems, government databases and social media, which has made public services more accessible while making it easier to monitor, profile and influence individuals.

The recognition of privacy as a fundamental right in Puttaswamy provides the constitutional foundation, and the four-fold proportionality standard supplies the measure against which every restriction must be judged.¹⁴¹

The Act of 2023 and the Rules of 2025 are significant steps in building a statutory framework, and this article has described their architecture of notice, consent, rights, obligations and graded penalties.^{142 143} It has also identified where that architecture falls short. Staged commencement leaves the operative obligations inert until 13 May 2027. The exclusion of publicly available personal data places the training of artificial

¹⁴⁰ Supra note 3, s. 3(c)(ii).

¹⁴¹ Supra note 2.

¹⁴² Supra note 3.

¹⁴³ Supra note 4.

intelligence systems largely outside the Act. The exemption power for notified State instrumentalities and the power to call for information supply no procedural guarantee to the individual and now face constitutional challenge. The Data Protection Board exists in law without appointed Members, and its design does not secure the independence its adjudicatory function requires.

Two propositions follow. Privacy protection cannot be left to individuals, because it is not enough to tell users to read the privacy policy while organisations analyse information at scale; responsibility must rest with those who design, operate and regulate digital systems. Equally, privacy is not an absolute barrier to technology or to legitimate governmental activity, and the task is to pursue genuine public interests within a framework of legality, necessity, proportionality and accountability.

The goal is not to stop the flow of information, on which modern society depends, but to ensure that it is collected and used responsibly. Protecting privacy in the digital world means protecting choice, dignity and autonomy, not data alone.

VII. BIBLIOGRAPHY

A. Constitutional and Legislative Sources

1. The Constitution of India, 1950.
2. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
3. The Information Technology Act, 2000 (Act 21 of 2000).
4. The Indian Telegraph Act, 1885 (Act 13 of 1885).
5. The Payment and Settlement Systems Act, 2007 (Act 51 of 2007).
6. The Right to Information Act, 2005 (Act 22 of 2005).
7. The Telecommunications Act, 2023 (Act 44 of 2023).

B. Subordinate Legislation and Official Notifications

1. Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022).

2. Ministry of Communications, Department of Telecommunications, Notification dated June 21, 2024, bringing specified provisions of the Telecommunications Act, 2023 into force with effect from June 26, 2024.
3. Ministry of Electronics and Information Technology, Government of India, Notification G.S.R. 843(E), Nov. 13, 2025, Gazette of India, Extraordinary, Part II, s. 3(i) (commencement of the Digital Personal Data Protection Act, 2023).
4. Ministry of Electronics and Information Technology, Government of India, Invitation of applications for the posts of Chairperson and Members of the Data Protection Board of India, F. No. 2(1)/2026-Pers.I (May 6, 2026).
5. Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153, DPSS.CO.OD No. 2785/06.08.005/2017-2018 (Apr. 6, 2018).
6. The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Nov. 13, 2025, Gazette of India, Extraordinary, Part II, s. 3(i).
7. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
8. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
9. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Apr. 11, 2011.
10. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, G.S.R. 754(E), Dec. 6, 2024.

C. Judicial Decisions

1. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
2. *Jorawar Singh Mundy v. Union of India*, 2021 SCC OnLine Del 2306.
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
4. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
5. *Laksh Vir Singh Yadav v. Union of India*, W.P.(C) No. 1021 of 2016 and connected matters, decided on May 29, 2026 (Del.).

6. *National Campaign for Peoples' Right to Information v. Union of India*, W.P.(C) No. 212 of 2026 (SC) (pending).
7. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
8. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
9. *The Reporters Collective Trust v. Union of India*, W.P.(C) No. 211 of 2026 (SC) (pending).
10. *Venkatesh Nayak v. Union of India*, W.P.(C) No. 177 of 2026 (SC) (pending).
11. *Vysakh K.G. v. Union of India*, 2022 SCC OnLine Ker 7337.

D. Foreign and Comparative Materials

1. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (CJEU, Grand Chamber, May 13, 2014).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), O.J. L 119/1.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), O.J. L, 12.7.2024.
4. Regulation (EU) 2026/1744 amending Regulation (EU) 2024/1689 (Digital Omnibus on Artificial Intelligence), O.J. L, 24.7.2026.

E. Committee Reports and Government Policy Documents

1. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, New Delhi, 2018).
2. Group of Experts on Privacy under the Chairmanship of Justice A.P. Shah, *Report of the Group of Experts on Privacy* (Planning Commission, Government of India, New Delhi, 2012).

3. Ministry of Electronics and Information Technology, Government of India, *India AI Governance Guidelines* (New Delhi, Nov. 5, 2025).

F. Books

1. Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, Oxford, 2020).
2. Daniel J. Solove, *Understanding Privacy* (Harvard University Press, Cambridge, 2008).
3. Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (Oxford University Press, New Delhi, 2016).
4. Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, Oxford, 2014).
5. Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins India, Noida, 2018).

G. Journal Articles and Research Papers

1. Anirudh Burman, "Understanding India's New Data Protection Law" (Carnegie Endowment for International Peace, Oct. 3, 2023).
2. Graham Greenleaf, "India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile" 185 *Privacy Laws & Business International Report* 3 (2023).
3. Graham Greenleaf, "Rules Expand India's Data Privacy Law, but Slowly" 199 *Privacy Laws & Business International Report* 19 (2026).
4. Helen Nissenbaum, "Privacy as Contextual Integrity" 79 *Washington Law Review* 119 (2004).
5. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193 (1890).