

Data Protection and Privacy in India: Towards a Comprehensive Legislative Framework in the Digital Age

Sandeep Kumar Pandey¹

ABSTRACT

India stands at a defining crossroads in the governance of digital rights. With over 391 million internet subscribers and an ambitious Digital India programme driving rapid expansion of online services, the question of how personal data is collected, stored, processed, and protected has moved from academic debate to urgent national necessity. Yet India's legal architecture for data protection remains fragmented, reactive, and ill-equipped for the scale and sophistication of threats that citizens now face.

KEYWORDS

Data Protection, Information Privacy, Comparative Digital Governance, Fundamental Rights

PRIVACY AND THE CONSTITUTIONAL FOUNDATION

The concept of data privacy does not find explicit mention in the Indian Constitution. Nevertheless, the judiciary has, over time, woven privacy into the fabric of Article 21², which guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. The Supreme Court's evolving interpretation of 'life' has extended it to encompass all those aspects that make a person's existence meaningful, complete, and dignified, a reading that logically encompasses the right to control one's personal information.³

The question before a nine-member Constitution Bench headed by the Chief Justice of India is whether privacy a fundamental right⁴. Regardless of the outcome, the moment is ideal for India to undertake a systematic reconstruction of its privacy laws. A constitutional right without an enforceable statutory framework is, in practice, a hollow guarantee. Recognition alone cannot

¹ Student at Hari Sahay Law College, Gorakhpur, Uttar Pradesh.

² INDIA CONST. art. 21.

³ Maneka Gandhi v. Union of India, AIR 1978 SC 597.

⁴ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

protect a citizen whose data is harvested, monetized, or breached without her knowledge or consent.

THE AGE OF DATA AND THE SCALE OF RISK

We live in what commentators rightly call the ‘age of data.’ Private companies ranging from social media platforms to email services and messaging applications, store enormous volumes of personal information, much of it held on servers located outside India's territorial jurisdiction. Both Facebook and WhatsApp count more than 200 million active users in India, making India one of the largest data-generating nations in the world⁵. India has, in fact, surpassed the United States in total Facebook users and yet it remains without a dedicated data protection statute.⁶

This asymmetry carries serious consequences. Data-colonizing corporations use collected information in myriad ways: targeted advertising, behavioural profiling, credit scoring, and increasingly, influence over political opinion. Individuals exercise limited control over how their data is used; in many cases, they do not even possess undisputed ownership of their own personal information. Meanwhile, company databases remain under constant risk of cyberattacks, and misuse of personal data by third parties for fraud, phishing, identity theft, and financial scams has grown proportionately with internet penetration.

THE INADEQUACY OF EXISTING LEGISLATION

India's primary instrument for cyber governance is the Information Technology Act, 2000⁷ (“the Act”) enacted at a time when the scale of today's data economy was barely imaginable. Originally aimed at providing legal infrastructure for e-commerce and accordingly legal sanctity to electronic records and digital signatures, the Act was not designed as a privacy statute. Chapter IX of the Act provides for penalties and adjudication of offences, and an Adjudicating Officer empowered with civil court powers may award compensation not exceeding one crore rupees, a figure that bears no rational relationship to the scale of harm a major data breach can inflict.

⁵ Gowhar Farooq, *Politics of Fake News: How WhatsApp Became a Potent Propaganda Tool in India*, 9 MEDIA WATCH 115 (2018).

⁶ Aditya Deshbandhu & Sejal Sahni, *Repurposing a WhatsApp group: How a fantasy cricket group transformed into a site of care and support during India's second wave of Covid-19*, 11 MOBILE MEDIA & COMM. 271, 273 (2022).

⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

The Information Technology (Amendment) Act, 2008 took the first tentative steps toward data protection, introducing Section 43A, which imposes liability on companies for failure to maintain reasonable security practices, and Section 72A, which penalizes disclosure of information in breach of a lawful contract.⁸ Section 67C mandates preservation and retention of information by intermediaries, with imprisonment of up to three years for wilful contravention. These provisions, while useful, remain scattered, narrow in scope, and wholly insufficient against the systemic data risks of 2024.

The Privacy (Protection) Bill, 2013 sought to address this gap by focusing specifically on the protection of personal and sensitive personal data, requiring consent of the data provider and establishing rules for collection, storage, processing, transfer, and disclosure, which was never enacted.⁹

THE EUROPEAN STANDARD AND INDIA'S OBLIGATION

The contrast with the European Union is instructive. The General Data Protection Regulation (GDPR), implemented in May 2018, aims at harmonizing data privacy laws across Europe and imposes penalties of up to four percent of a company's worldwide annual turnover for serious breaches, a deterrent proportionate to the power of the entities being regulated.¹⁰ GDPR requires companies to ensure that even their vendors are fully compliant as a condition of doing business. It establishes purpose limitation, data minimization, the right to erasure, and mandatory breach notification as enforceable obligations.

To recognise privacy as a fundamental right in India without enacting comparable enforceable regulations would be, as observers have rightly noted, akin to raking water up a hill. Rights require remedies; remedies require institutions.

WHAT MUST BE DONE

A credible Indian data protection framework must rest on several pillars. Security of personal data must be mandatory, with immediate breach notification to affected individuals and a regulatory authority. Data subjects must have the right to access, correct, and erase their personal information. Violations by both government and private entities must attract

⁸ Information Technology (Amendment) Act, 2008, §§ 43A, 72A, No. 10, Acts of Parliament, 2009 (India).

⁹ The Privacy (Protection) Bill, 2013, Bill No. 115 of 2013, 2013 (India).

¹⁰ Regulation 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

meaningful penalties such as imprisonment and substantial fines which are sufficient to deter non-compliance rather than treat it as a cost of business. Mass surveillance and individual profiling without legal cause must be explicitly prohibited.

At the same time, the framework must be calibrated to legitimate national security interests. The Darknet and encrypted online channels are increasingly exploited for illegal trade, trafficking, and money laundering.¹¹ Regulations that unduly restrict the operational capacity of intelligence and law enforcement agencies would compromise national security. The solution lies in narrowly defined, judicially supervised exceptions and not a blanket government exemption that swallows the right.

India also urgently needs an independent regulatory body, structured along the lines of Data Protection Commissioner offices in Canada and Ireland with genuine autonomy from executive direction, technical expertise, and adequate enforcement powers.¹²

CONCLUSION

The digital future India is building must be one in which citizens are not merely users but rights-holders. Data generated by over a billion people cannot remain the unregulated property of corporations and state agencies. A comprehensive, rights-centered data protection law is not a luxury for a later stage of development, it is a prerequisite for a democratic digital society. The time to legislate is now.

¹¹ United Nations Office on Drugs and Crime, *Darknet and Cybercrime Investigations*, Regional Office for Southeast Asia and the Pacific, <https://www.unodc.org/roseap/uploads/archive/documents/darknet/index.html> (last visited July 11, 2026).

¹² Privacy Act, R.S.C. 1985, c. P-21 (Can.), <https://laws-lois.justice.gc.ca/eng/acts/p-21/fulltext.html>.