IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Right to Privacy in the Digital Era in India

Samreen Alvi[1]

Nadeem Alam[2]

[1]Research Scholar, Department of Political Science, Aligarh Muslim University, Aligarh, India

[2]Research Scholar, Department of Political Science, Aligarh Muslim University, Aligarh, India

Abstract

For more than sixty years it was unclear whether the Constitution of India protected privacy at all. That uncertainty ended on 24 August 2017, when a nine-judge bench of the Supreme Court in *Justice K. S. Puttaswamy (Retd.) v. Union of India* unanimously held that privacy is a fundamental right flowing from Articles 14, 19 and 21, and that any interference by the State must satisfy the tests of legality, legitimate aim, proportionality and adequate procedural safeguards. Parliament responded only in 2023, and the Rules giving effect to that statute were notified on 13 November 2025, under which the main duties of data fiduciaries become binding only by 13 May 2027. The research problem is the distance between what the Constitution now promises and what the statutory framework delivers.

The study traces the evolution of privacy in Indian constitutional jurisprudence, examines the statutory framework now governing personal data and State surveillance, measures digital expansion and privacy-related harm from official data, and sets the Indian framework against the General Data Protection Regulation. The central question is whether the Digital Personal Data Protection Act, 2023 satisfies the proportionality standard laid down in Puttaswamy. The hypothesis is that constitutional recognition of privacy in India has outpaced its statutory realisation, and that the present framework disciplines private data fiduciaries far more effectively than it disciplines the State.

The design is doctrinal and descriptive-analytical, and uses secondary data only, drawn from peer-reviewed journal articles, academic books, reported judgments, and official reports of TRAI, the National Crime Records Bureau, UIDAI, the Reserve Bank of India, CERT-In, MeitY, the World Bank, UNCTAD and the ITU. Thematic analysis, doctrinal analysis and descriptive statistics have been applied, and every figure has been traced to a named official publication.

Six findings emerge. Broadband subscribers rose from 131.49 million in November 2015 to 1,065.88 million by March 2026. Cybercrime cases registered by the National Crime Records Bureau rose from 52,974 in 2021 to 86,420 in 2023, an increase of about 63 per cent in two years. A wide urban-rural gap persists, with tele-density of 151.47 per cent in urban India against 60.46 per cent in rural India in March 2026, which limits the usefulness of a consent-based law. The Indian statute is narrower than the General Data Protection Regulation, providing no right to data portability, no separate category of sensitive personal data and no safeguard against automated decision-making. Broad State exemptions under Section 17, an executive-appointed Data Protection Board and the amendment of the Right to Information Act, 2005 by Section 44(3) weaken accountability. Most significantly, no surveillance reform has

followed Puttaswamy: interception under Section 69 of the Information Technology Act, 2000 and Section 5(2) of the Indian Telegraph Act, 1885 still requires no prior judicial authorisation.

The paper concludes that the constitutional promise of 2017 remains only partly realised. It recommends an independent regulator, prior judicial authorisation for interception, restoration of the public-interest override in the Right to Information Act, a safeguard against automated decisions, and digital literacy in regional languages so that consent becomes meaningful.

Keywords: right to privacy; Puttaswamy; Digital Personal Data Protection Act 2023; surveillance; data protection; proportionality; digital India

1. Introduction

1.1 Background of the topic

India is today one of the most heavily datafied societies in the world. According to the Telecom Regulatory Authority of India, the country had 1,065.88 million broadband subscribers and 1,092.79 million internet subscribers as on 31 March 2026.[1] The Unique Identification Authority of India has reported more than 14,800 crore cumulative Aadhaar authentication transactions, of which 2,707 crore were carried out in the financial year 2024–25 alone.[2] The Reserve Bank of India recorded 185.8 billion Unified Payments Interface transactions in the same financial year, amounting to 83.4 per cent of the total volume of payments processed in the country.[3] Every one of these transactions leaves behind a permanent data trail. A welfare application, a hospital visit, a mobile recharge, a train ticket and a school admission are today all mediated by databases that record who did what, when and where.

This transformation has made privacy a question of everyday governance rather than an abstract philosophical concern. Privacy has long been understood in liberal thought as the right of a person "to be let alone",[4] but the framers of the Indian Constitution did not include an express privacy clause. The task of locating privacy within the constitutional text therefore fell to the courts. In *M. P. Sharma v. Satish Chandra*, an eight-judge bench declined to read a right to privacy into the Constitution,[5] and in *Kharak Singh v. State of Uttar Pradesh* the majority took a similar view, although Subba Rao J. in dissent argued that personal liberty under Article 21 must include the right to be free from official intrusion.[6] Over the next five decades the courts moved cautiously towards recognition, until a nine-judge bench settled the question in 2017.

1.2 Statement of the research problem

The decision in *Puttaswamy* declared privacy to be a fundamental right and required that every State intrusion pass a demanding four-part test.[7] The legislative response, however, arrived only in August 2023 in the form of the Digital Personal Data Protection Act, and the Rules giving effect to that Act were notified as late as 13 November 2025, with the substantive duties of data fiduciaries becoming operative in stages up to 13 May 2027.[8] The Act is built around notice and consent and is directed mainly at private entities. The State, by contrast, enjoys wide exemptions under Section 17, appoints the members of the Data Protection Board of India, and has not amended any of the older interception laws. Scholars have

[1] Telecom Regulatory Authority of India. (2026). The Indian telecom services performance indicators, January–March 2026. TRAI.

[2] Unique Identification Authority of India. (2025). Aadhaar authentication surges past 2,707 crore in 2024-25 [Press release]. Ministry of Electronics and Information Technology, Government of India.

[3] Reserve Bank of India. (2025). Annual report 2024–25. Reserve Bank of India.

[4] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.

[5] M. P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[6] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

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

[8] Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025). Gazette of India.

therefore argued that the statute is friendlier to government and business than to the citizen,[9] and that the independence of the regulator remains doubtful.[10] The research problem, stated simply, is that India now has a strong constitutional right on paper but a comparatively weak statutory machinery to protect it in practice, particularly against the State.

1.3 Objectives of the study

Five objectives follow from that problem. The paper traces the evolution of the right to privacy in Indian constitutional jurisprudence from 1954 to the present; examines the statutory and regulatory framework that now governs personal data, interception and internet suspension; measures, from verified official data, the scale of digital expansion and the extent of privacy-related harm; sets the Indian framework against the European Union's General Data Protection Regulation and against global patterns of adoption; and identifies the gaps that remain, together with reforms that would close them.

1.4 Research questions and hypothesis

The study is guided by five questions. How has the right to privacy evolved in Indian constitutional jurisprudence? What is the present scale of digital expansion and privacy-related harm in India? Does the Digital Personal Data Protection Act, 2023 satisfy the proportionality standard laid down in Puttaswamy? How does the Indian framework compare with the General Data Protection Regulation and with global trends? What reforms are required to close the gap between constitutional promise and statutory practice?

The working hypothesis is that constitutional recognition of the right to privacy in India has outpaced its statutory realisation. A subsidiary hypothesis is that the present framework regulates private data fiduciaries far more effectively than it regulates the State, and that the resulting imbalance is the principal weakness of the Indian data protection regime.

1.5 Why the question matters now

Timing gives the study most of its usefulness. The Rules were notified in November 2025 and the substantive obligations bind only from May 2027, so the design of the framework can still be examined before it hardens into settled practice. Once the Data Protection Board starts deciding cases, the questions asked here turn into questions about enforcement. There is also a disciplinary reason for asking them. Privacy marks a boundary between the citizen and the State, and where that boundary falls, and who is permitted to move it, is a question about the distribution of power. Indian political science has largely left this ground to the lawyers, which is why the constitutional literature on Puttaswamy is rich and the empirical literature on what the judgment actually changed is thin.

2. Review of literature

The literature reviewed here was selected using a systematic procedure. Only three categories of material were admitted: peer-reviewed journal articles, academic books published by recognised academic publishers, and institutional reports of governments and international organisations. Newspaper reports, blogs, encyclopaedias and commercial websites were excluded. The selected literature has been organised into five themes, and each theme closes with a short critical evaluation setting out where scholars agree, where they disagree, and what remains unexamined.

[9] Greenleaf, G. (2023). India's 2023 Data Privacy Act: Business/government friendly, consumer hostile. Privacy Laws & Business International Report, 185, 1, 3–12.

[10] Sonkar, A. (2025). The Digital Personal Data Protection Act, 2023: Analysing its implications, challenges, and future prospects. International Cybersecurity Law Review, 6(4), 547–569.

2.1 Theme one: the conceptual foundations of privacy

Modern privacy scholarship begins with Warren and Brandeis, who argued in 1890 that the law must protect an "inviolate personality" against intrusive publicity.[11] Their formulation, however, treats privacy mainly as seclusion, which is inadequate for a world of databases. Solove has offered a more useful framework by abandoning the search for a single definition and instead classifying privacy harms into four groups of activities: information collection, information processing, information dissemination and invasion.[12] Nissenbaum has taken a third approach, arguing that privacy is not secrecy but "contextual integrity": information flows are appropriate or inappropriate depending on the norms of the context in which the information was originally shared.[13]

These three frameworks are complementary rather than competing, and the Supreme Court of India in Puttaswamy drew on all of them when it described privacy as having spatial, decisional and informational dimensions. Their limitation is that they were developed in Western societies with high literacy, strong individual property traditions and functioning regulators. Whether the notion of individual informational self-determination travels well to a country where a large share of users access the internet through a shared device and in a language in which privacy notices are rarely available is a question the conceptual literature does not answer.

2.2 Theme two: datafication and surveillance capitalism

Zuboff has argued that the dominant business model of the digital economy converts human experience into behavioural data, which is then traded in prediction markets, producing a form of power she calls "Big Other".[14] She develops the argument at length in her later book, where surveillance capitalism is presented as a challenge to human autonomy itself.[15]

This body of work is persuasive in explaining why voluntary consent is a weak protection: when the same platform supplies the service and writes the terms, the user's choice is formal rather than real. Its weakness, for Indian purposes, is that it concentrates on private corporations. In India the single largest collector of personal data is the State itself, through identity, welfare, taxation, health and policing databases. A framework built to explain Silicon Valley therefore needs adaptation before it can explain Aadhaar-linked governance, and this adaptation has not been systematically carried out.

2.3 Theme three: comparative and global data protection law

Greenleaf's comparative work remains the standard reference for data privacy law in Asia. His book on Asian data privacy laws examines the interaction between trade pressures and human rights standards across twenty-six jurisdictions,[16] and his annual survey records that 172 countries had national data privacy laws by 2025.[17] The United Nations Conference on Trade and Development, using a stricter counting method, reports that 137 of 194 economies, or 71 per cent, have data protection and privacy legislation in force.[18] On the European side, Lynskey has shown that European data protection law rests on a dual foundation of fundamental rights and internal market harmonisation,[19] while Basu and

[11] Warren & Brandeis, supra, at 205.

[12] Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564.

[13] Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

[14] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), 75–89.

[15] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

[16] Greenleaf, G. (2014). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press.

[17] Greenleaf, G. (2025). Global data privacy laws 2025: 172 countries, twelve new in 2023/24. Privacy Laws & Business International Report, 194, 1.

[18] United Nations Conference on Trade and Development. (n.d.). Data protection and privacy legislation worldwide. Global Cyberlaw Tracker. UNCTAD.

[19] Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.

Guinchard have argued that data protection functions best when it is designed as an "architecture of custody" that restores public trust rather than as a compliance burden.[20]

The disagreement between Greenleaf's count of 172 countries and UNCTAD's count of 137 is not an error but a difference of method: Greenleaf includes sectoral and partial laws, whereas UNCTAD applies a stricter checklist. Both counts nonetheless point in the same direction, namely that data protection legislation has become a global norm and that India was a late adopter rather than an innovator.

2.4 Theme four: Indian scholarship after Puttaswamy

Indian scholarship divides sharply. Writing before the judgment, Arun described India's statutory safeguards against mass surveillance as "paper-thin" and warned that executive authorisation without judicial oversight offered little protection.[21] Bhandari and Sane examined the Srikrishna Committee Report and the 2018 Bill and concluded that the proposed law protected citizens from private companies far better than from the State.[22] The Committee itself had recommended a framework built on a fiduciary relationship between the data principal and the data fiduciary.[23]

After the Act was passed, Malhotra and Malhotra offered a broadly favourable assessment, describing the statute as a citizen-centric instrument that places the interests of "digital nagriks" first and simplifies compliance for a developing economy.[24] Greenleaf reached the opposite conclusion, arguing that the extent of the government exemptions makes the Act read in places like a blueprint for surveillance and that the Data Protection Board of India lacks credible independence.[25] Sonkar occupies a middle position, welcoming the accountability principles while criticising the breadth of State exemptions and the limited autonomy of the regulator.[26] More recently, Jha and Lakra have questioned the treatment of publicly available data under the Act on constitutional grounds.[27]

The disagreement between Malhotra and Malhotra on the one hand and Greenleaf and Sonkar on the other is the central fault line in the current Indian literature. It is essentially a disagreement about the standard of comparison. If the Act is compared with the position before 2023, when only Section 43A of the Information Technology Act and the 2011 Rules applied, it is clearly an improvement. If it is compared with the standard set by Puttaswamy itself, the assessment is far less favourable. This paper adopts the second standard, because a constitutional court has already fixed it.

2.5 Theme five: the digital divide and the gendered experience of privacy

The International Telecommunication Union estimates that about 68 per cent of the world's population used the internet in 2024 and continues to record a persistent gender gap in internet use.[28] The World Bank's development indicators place India's internet-using population at 55.9 per cent in 2022.[29] Kovacs has argued that dominant conceptions of privacy have historically been gendered, and that datafication

[20] Basu, S., & Guinchard, A. (2020). Restoring trust into the NHS: Promoting data protection as an "architecture of custody" for the sharing of data in direct care. International Journal of Law and Information Technology, 28(3), 243–272.

[21] Arun, C. (2014). Paper-thin safeguards and mass surveillance in India. National Law School of India Review, 26(2), 105–114.

[22] Bhandari, V., & Sane, R. (2018). Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. Socio-Legal Review, 14(2), 143–169.

[23] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. Ministry of Electronics and Information Technology, Government of India.

[24] Malhotra, C., & Malhotra, U. (2024). Putting interests of digital nagriks first: Digital Personal Data Protection (DPDP) Act 2023 of India. Indian Journal of Public Administration. Advance online publication.

[25] Greenleaf, supra, at 3–5.

[26] Sonkar, supra, at 552–560.

[27] Jha, N., & Lakra, R. (2026). Reevaluating publicly available data under the DPDPA Act 2023: A constitutional challenge. Indian Law Review. Advance online publication.

[28] International Telecommunication Union. (2024). Facts and figures 2024: Measuring digital development. ITU.

[29] World Bank. (2024). World development indicators: Individuals using the Internet (% of population), India [Data set]. World Bank.

reproduces this inequality by treating the body itself as a source of data.[30] This theme is the least developed in the Indian legal literature, even though it has direct statutory consequences: a consent-based law assumes an autonomous individual who can read a notice and refuse a service, which is not the situation of a large number of Indian women who use shared devices.

2.6 Research gap

Four gaps emerge from this review. No empirical study of how the Digital Personal Data Protection framework actually works yet exists, which is unsurprising given that the Rules were notified in November 2025 and the core obligations bind only from May 2027. The amendment of Section 8(1)(j) of the Right to Information Act, 2005 by Section 44(3) of the new Act has drawn political controversy and almost no peer-reviewed analysis. The surveillance reform vacuum has not been re-examined since the Telecommunications Act, 2023 came into force; the scholarship on interception is largely pre-2017 and does not account for the statutes now in place. And doctrinal writing on privacy in India seldom draws on official quantitative data, so the scale of the problem tends to be asserted instead of shown. This study takes up the third and fourth of these directly, and offers preliminary analysis on the first two.

3. Research methodology

3.1 Research design

The study adopts a doctrinal and descriptive-analytical research design. The doctrinal component examines constitutional provisions, reported judgments, statutes and delegated legislation in order to establish what the law is and what standard it sets. The descriptive-analytical component uses official statistics to establish the factual context in which that law must operate. The two components are then read together, so that legal analysis is grounded in evidence and statistical evidence is given legal meaning. The design is qualitative in its dominant orientation, with quantitative data used in a supporting and illustrative role.

3.2 Nature and type of data

The study uses secondary data only. No survey, interview or field observation was conducted, and no primary data of any kind were collected. Three categories of secondary material were used: peer-reviewed journal articles and academic books; reported judgments of the Supreme Court of India; and official reports and statistical releases of government bodies and international organisations.

3.3 Sources of data

The legal sources are the Constitution of India, the Information Technology Act, 2000 and the Rules of 2011 and 2021 made under it, the Indian Telegraph Act, 1885, the Aadhaar Act, 2016, the Right to Information Act, 2005, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Telecommunications Act, 2023, and Regulation (EU) 2016/679. The judicial sources are the eight reported decisions listed in Table 1.

The statistical sources are named individually so that every figure can be traced. Subscriber and tele-density data are taken from the performance indicator reports and monthly subscription releases of the Telecom Regulatory Authority of India. Crime data are taken from the Crime in India volumes of the National Crime Records Bureau. Aadhaar authentication and e-KYC data are taken from official releases of the Unique Identification Authority of India. Digital payment data are taken from the Annual Report of the Reserve Bank of India. Cyber-security incident data are taken from the annual report of the Indian Computer Emergency Response Team. Comparative legislative data are taken from the Global Cyberlaw

[30] Kovacs, A. (2022). Searching for a room of one's own in cyberspace: Datafication and the global feminisation of privacy [Working paper]. Social Science Research Network.

Tracker of the United Nations Conference on Trade and Development. International connectivity data are taken from the International Telecommunication Union and the World Bank's World Development Indicators. Data on internet suspensions are taken from the annual reports of the #KeepItOn coalition.

3.4 Analytical tools and methods

Four analytical methods were used. Thematic analysis was applied to the literature: each source was read, coded and grouped under the five themes presented in Section 2. Doctrinal analysis was applied to the statutory framework using the four-part proportionality test of legality, legitimate aim, proportionality and procedural safeguards as the evaluative standard, since this is the standard the Supreme Court itself has prescribed. Comparative legal analysis was used to place the Indian statute alongside the General Data Protection Regulation on a set of common parameters. Descriptive statistical analysis, confined to absolute values, percentages, ratios and percentage change, was used to interpret the quantitative data; no inferential statistics were attempted because the data are aggregate administrative records rather than sample observations. The tables were prepared manually and the figures were generated using the Matplotlib library in Python.

A triangulation rule was followed throughout. No numerical value has been used unless it could be traced to a named official publication, and wherever possible each value was checked against a second independent source. Values that could not be verified in this manner were excluded rather than estimated, which is why some series in this paper begin later than the reader might expect.

3.5 Limitations of the study

The study has six limitations, which are stated plainly. First, it relies entirely on secondary data and therefore cannot capture how ordinary citizens actually experience privacy. Second, the crime statistics are affected by the Principal Offence Rule followed by the National Crime Records Bureau, under which only the most serious offence in a case is counted, so privacy-related offences are likely to be understated. Third, the counts of internet suspensions compiled by civil society organisations differ from figures given by government in Parliament, and this paper presents the former while acknowledging the divergence. Fourth, the Digital Personal Data Protection framework is not yet fully in force, so no enforcement data exist and the assessment of the statute is necessarily prospective. Fifth, the reporting intervals of the Telecom Regulatory Authority are not uniform, so the trend shown in Figure 1 uses verified reporting dates that are not evenly spaced in time. Sixth, the judgment in Puttaswamy consists of six separate opinions, and the four-part proportionality test is drawn principally from the plurality opinion and the concurring opinion of Kaul J. rather than from a single formal majority; this paper follows the standard scholarly reading but notes the qualification.

4. Results and discussion

4.1 The evolution of privacy jurisprudence in India

Indian privacy jurisprudence did not develop steadily. Table 1 sets out the eight decisions that mark its course, and the pattern in them is one of long hesitation followed by abrupt settlement. Between 1954 and 1963 the Court refused to recognise a general right; between 1975 and 1997 it recognised the right in specific settings such as police surveillance, publication and telephone tapping; and in 2017 it placed the right on a firm constitutional footing.

Table 1: Evolution of the Right to Privacy in Indian Constitutional Jurisprudence, 1954–2020

Case	Citation	Bench	Principal holding relevant to privacy
M. P. Sharma v. Satish Chandra (1954)	AIR 1954 SC 300	8 judges	Declined to read a right to privacy into the Constitution in the context of search and seizure. Overruled on this point in 2017.
Kharak Singh v. State of U.P. (1963)	AIR 1963 SC 1295	6 judges	Struck down domiciliary night visits but the majority denied a general right to privacy. Subba Rao J. dissented. Partly overruled in 2017.
Gobind v. State of M.P. (1975)	(1975) 2 SCC 148	3 judges	Accepted a limited right to privacy, subject to a compelling State interest.
R. Rajagopal v. State of T.N. (1994)	(1994) 6 SCC 632	2 judges	Recognised the right to be let alone in the context of publication and the press.
PUCL v. Union of India (1997)	(1997) 1 SCC 301	2 judges	Read privacy into Article 21 and laid down procedural safeguards for telephone tapping.
Justice K. S. Puttaswamy v. Union of India (2017)	(2017) 10 SCC 1	9 judges	Held unanimously that privacy is a fundamental right under Articles 14, 19 and 21, with spatial, decisional and informational dimensions, and prescribed a proportionality standard.
Justice K. S. Puttaswamy v. Union of India (2018)	(2019) 1 SCC 1	5 judges	Upheld the core of the Aadhaar scheme under Section 7 but struck down Section 57, which had allowed private parties to demand Aadhaar.
Anuradha Bhasin v. Union of India (2020)	(2020) 3 SCC 637	3 judges	Held that internet access for speech and trade is constitutionally protected, and that suspension orders must be published, proportionate and open to review.

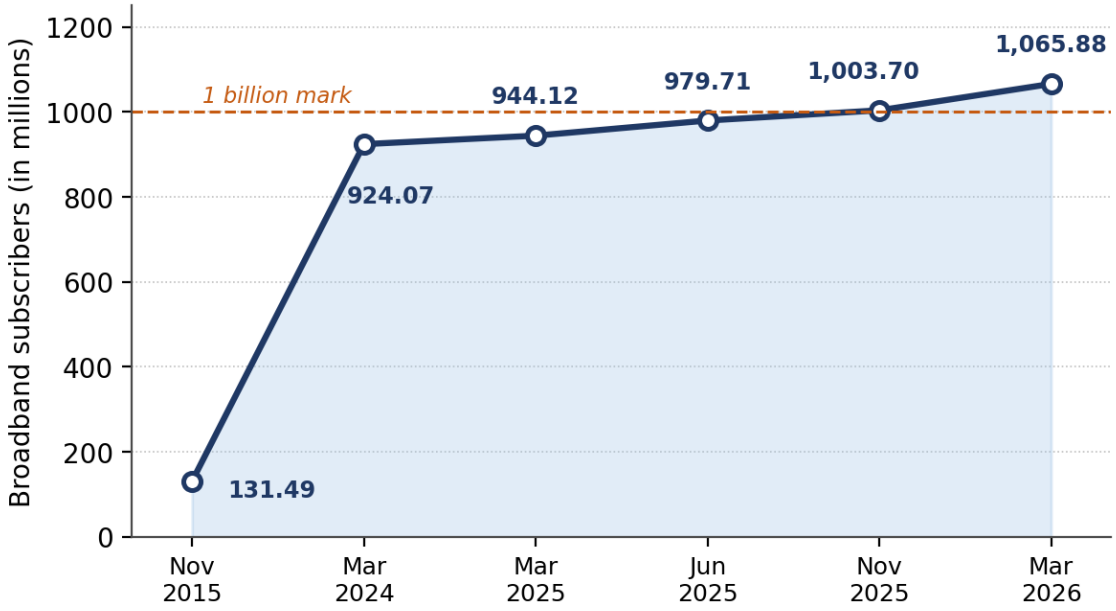
Source: Compiled by the authors from reported judgments of the Supreme Court of India as cited above.

4.2 The scale of digital expansion

The factual ground beneath the judgment shifted while the judgment was being written. Figure 1 shows broadband subscribers rising from 131.49 million in November 2015 to 1,065.88 million in March 2026. TRAI records that the base grew more than sixfold in the decade to November 2025, when it crossed the one billion mark at 100.37 crore.[31] In plain terms, a country that had fewer than fourteen crore broadband connections a decade ago now has more than a hundred crore. Every additional connection represents a new stream of personal data.

[31] Telecom Regulatory Authority of India. (2025). Telecom subscription data as on 31st October 2025 (Press Release No. 141/2025). TRAI; and TRAI performance indicator reports for the quarters ending March 2025, June 2025 and March 2026.

Figure 1: Growth of Broadband Subscribers in India, November 2015 to March 2026 (in millions)



Note: The horizontal axis plots verified reporting dates; spacing is not proportional to time.

Source: Created by Authors, Telecom Regulatory Authority of India. (2025, 2026). Telecom subscription data and performance indicator reports. TRAI.

Table 2 places this expansion alongside other indicators of data generation. Read together, the figures show that identity verification, payments and connectivity have all reached a scale at which even a small proportional failure rate translates into a very large absolute number of affected persons.

Table 2: Selected Indicators of India's Digital Expansion

Indicator	Value	Source and reference period
Internet subscribers	1,092.79 million	TRAI, Performance Indicator Report, quarter ending March 2026
Broadband subscribers	1,065.88 million	TRAI, Performance Indicator Report, quarter ending March 2026
Overall tele-density	93.26 per cent	TRAI, Telecom Subscription Data, 31 March 2026
Aadhaar authentications (year)	2,707 crore	UIDAI, financial year 2024–25
Aadhaar authentications (cumulative)	Over 14,800 crore	UIDAI, as on 31 March 2025
e-KYC transactions (cumulative)	2,356 crore	UIDAI, as on 31 March 2025
UPI transactions	185.8 billion	Reserve Bank of India, financial year 2024–25
Cyber-security incidents handled	13,91,457	CERT-In, Annual Report 2022

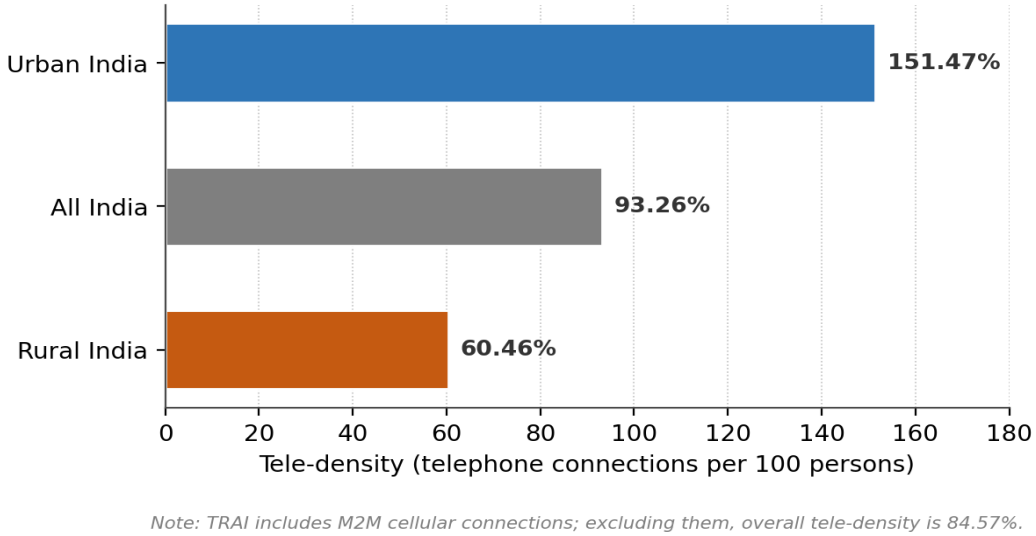
Source: Compiled by the authors from TRAI (2025, 2026), UIDAI (2025), Reserve Bank of India (2025) and CERT-In (2023).

4.3 The digital divide and the limits of consent

That growth has not been evenly shared. Figure 2 shows urban tele-density at 151.47 per cent on 31 March 2026 against rural tele-density of 60.46 per cent.[32] The urban figure exceeds one hundred because many urban users hold more than one connection; the rural figure means that fewer than three out of five rural residents have a telephone connection at all. The gap has in fact widened rather than narrowed as the network has grown.

[32] Telecom Regulatory Authority of India. (2026). Telecom subscription data as on 31st March 2026 (Press Release No. 53/2026). TRAI.

Figure 2: Urban and Rural Tele-density in India as on 31 March 2026 (connections per 100 persons)



Source: Created by Authors Telecom Regulatory Authority of India. (2026). Telecom subscription data as on 31st March 2026 (Press Release No. 53/2026). TRAI.

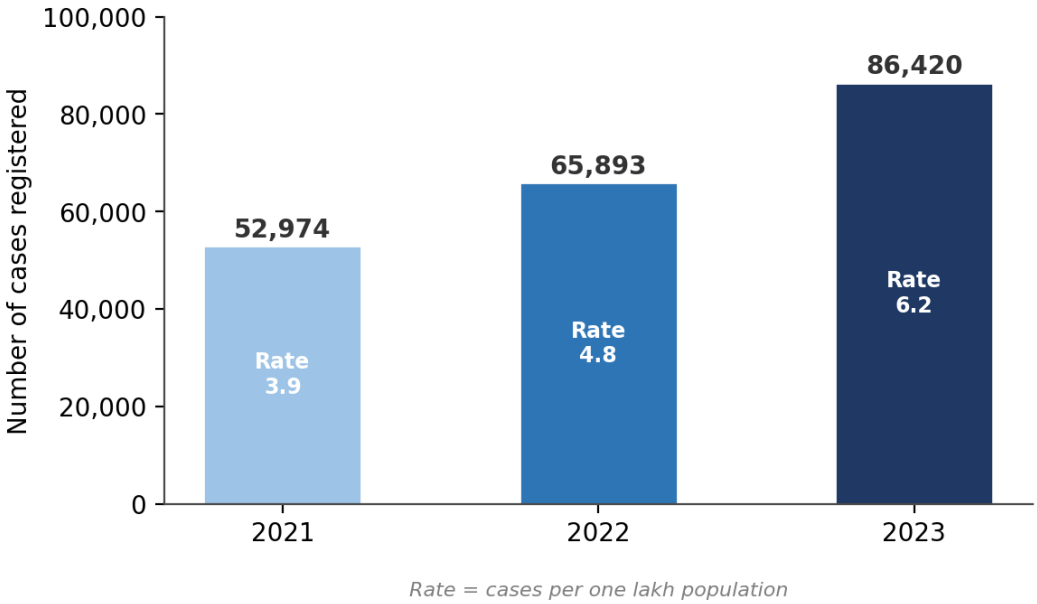
This gap has a direct legal consequence. The Digital Personal Data Protection Act is built on notice and consent. Consent is meaningful only where the person can read the notice, understand it, and realistically decline the service. For a rural user with a shared handset, limited literacy in the language of the notice, and no substitute for a government service, none of these conditions is reliably satisfied. This is precisely the difficulty that the surveillance capitalism literature identifies in a Western setting, and it is sharper in India because the alternative to consenting is often the loss of a welfare entitlement rather than the loss of a social media account.

4.4 The growth of privacy-related harm

Harm has grown alongside connectivity. Cybercrime cases registered by the National Crime Records Bureau rose from 52,974 in 2021 to 65,893 in 2022 and 86,420 in 2023, as Figure 3 shows. The rate per lakh of population rose from 3.9 to 6.2 over the same period. Fraud was the dominant motive, accounting for 68.9 per cent of cases (59,526) in 2023.[33]

[33] National Crime Records Bureau. (2023). Crime in India 2022 (Vol. 2). Ministry of Home Affairs, Government of India; and National Crime Records Bureau. (2025). Crime in India 2023 (Vol. 2). Ministry of Home Affairs, Government of India.

Figure 3: Cybercrime Cases Registered in India, 2021 to 2023



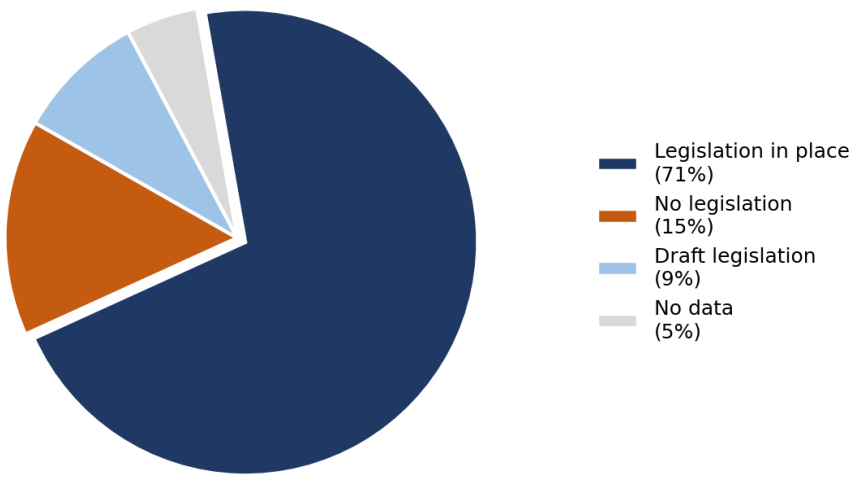
Source: Created by Authors National Crime Records Bureau. (2023, 2025). Crime in India 2022 and Crime in India 2023. Ministry of Home Affairs, Government of India.

Interpreted simply, registered cybercrime increased by about 63 per cent in two years, which is faster than the growth in the number of internet users over the same period. Two cautions are necessary. Registered crime measures reporting as much as offending, so part of the rise may reflect greater public awareness and easier reporting. Equally, because the National Crime Records Bureau counts only the most serious offence in each case, offences specifically relating to breach of privacy and data theft are likely to be undercounted. The direction of the trend is nevertheless clear, and it is consistent with the incident data of the Indian Computer Emergency Response Team, which handled 13,91,457 cyber-security incidents in 2022.

4.5 India in global comparison

India was a late adopter, not an innovator. Figure 4 shows that 71 per cent of the 194 economies tracked by the United Nations Conference on Trade and Development have data protection legislation in force, 15 per cent have none, and 9 per cent have a bill in draft. India moved from the second group to the first in 2023, nearly three decades after the European Union adopted its first data protection directive.

Figure 4: Global Status of Data Protection and Privacy Legislation across 194 Economies



Source: Created by Authors, United Nations Conference on Trade and Development. (n.d.). Data protection and privacy legislation worldwide. Global Cyberlaw Tracker. UNCTAD.

Membership of the group, however, says nothing about the strength of the law. Table 3 compares the Indian statute with the General Data Protection Regulation on seven parameters. Four differences stand out: the absence of a right to data portability, the absence of an independent right to erasure, the absence of a separate category of sensitive personal data, and the absence of any safeguard against decisions taken purely by automated means. The last of these is particularly significant for a country now deploying algorithmic systems in welfare targeting, credit scoring and policing.

Table 3: Comparison of the Digital Personal Data Protection Act, 2023 with the General Data Protection Regulation

Parameter	GDPR (Regulation (EU) 2016/679)	DPDP Act, 2023 (India)
Legal basis for processing	Six lawful bases including consent, contract and legitimate interests	Consent and specified 'legitimate uses'
Sensitive personal data	Special categories given heightened protection	No separate category recognised
Right to data portability	Expressly provided	Not provided
Right to erasure	Independent right, subject to exceptions	Erasure available but not as an equivalent standalone right
Automated decision-making	Specific safeguard against decisions based solely on automated processing	No equivalent safeguard
Regulator	Independent supervisory authorities with guaranteed independence	Data Protection Board of India, with members appointed by the Central Government
Cross-border transfer	Adequacy decisions and safeguards model	Negative-list model under Section 16

Source: Compiled by the authors from Regulation (EU) 2016/679; the Digital Personal Data Protection Act, 2023; Lynskey (2015); Greenleaf (2023); and Sonkar (2025).

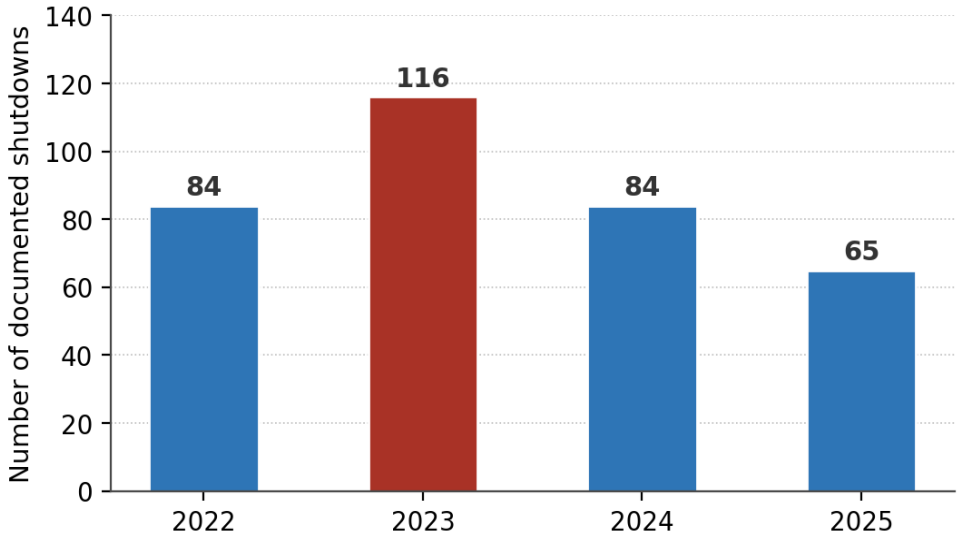
Put concretely, the Indian citizen may ask what data an organisation holds and may ask for it to be corrected, but cannot easily carry that data to a competing service, cannot compel its deletion as a matter of right, and cannot demand an explanation when a machine refuses an application. These are not technical omissions. Each of them is a point at which the individual loses the ability to contest a decision taken about her, which is precisely the interest that the proportionality standard was designed to protect.

4.6 Surveillance, internet suspension and the missing reform

The branch of law most directly concerned with State intrusion has not been touched. Interception under Section 69 of the Information Technology Act, 2000 and under Section 5(2) of the Indian Telegraph Act, 1885 continues to rest on executive authorisation, without any requirement of prior judicial approval. The Digital Personal Data Protection Act did not amend either provision. Figure 5 shows the number of documented internet suspensions in India, which stood at 84 in 2022, rose to 116 in 2023, fell back to 84 in 2024 and to 65 in 2025. Even after this decline India remained the country with the highest recorded number of shutdowns among democracies.[34]

[34] Access Now. (2025). Emboldened offenders, endangered communities: Internet shutdowns in 2024. Access Now.

Figure 5: Documented Internet Shutdowns in India, 2022 to 2025



Source: Created by Authors, Access Now. (2023, 2024, 2025, 2026). #KeepItOn annual reports on internet shutdowns. Access Now. Note: Figures compiled by a civil society coalition and may differ from figures placed before Parliament.

These findings should be read against *Anuradha Bhasin*, in which the Supreme Court held that suspension orders must be published, must be proportionate and must be open to judicial review.[35] The persistence of high shutdown numbers six years later, and India's continued position at the top of the democratic world on this measure, suggests that the difficulty is not the absence of a legal standard but the absence of an institution willing and able to enforce it. This is the point at which the present study departs from the more optimistic assessments in the literature. Malhotra and Malhotra are right that the Act simplifies compliance and states citizen-facing principles clearly; but simplification is not the same as accountability, and the evidence assembled here supports the more critical readings offered by Greenleaf and Sonkar, and confirms the concern raised earlier by Arun and by Bhandari and Sane that Indian data protection law protects the citizen from the company far better than from the State.

4.7 The implementation gap

Timing matters as much as content here. Table 4 sets out the phased schedule under which the Rules of 2025 come into effect. Only the provisions establishing the Data Protection Board took effect immediately. The registration of consent managers begins in November 2026, and the core obligations of data fiduciaries, including breach notification, protection of children's data and the duties of significant data fiduciaries, become binding only in May 2027.

Table 4: Phased Implementation of the Digital Personal Data Protection Rules, 2025

Effective date	Provisions brought into force	Practical meaning
13 November 2025	Rules 1 and 2 and Rules 17 to 21	Definitions take effect and the Data Protection Board of India is constituted.
13 November 2026	Rule 4	Consent managers must be registered with the Board and must be companies incorporated in India.
13 May 2027	Rules 3, 5 to 16, 22 and 23	Notice and consent duties, security safeguards, breach notification, children's data protection, obligations of significant data fiduciaries and rights of data principals become enforceable.

Source: Created by Authors, Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025). Gazette of India.

[35] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

The practical meaning of this schedule is that for a period of almost four years after the Act received assent, Indian citizens continued to rely on a constitutional right without a working statutory remedy. During the same four years, broadband connections crossed one billion and registered cybercrime rose by more than sixty per cent. The volume of personal data therefore grew fastest during the very period in which the protective machinery was least available. This is the clearest possible illustration of the hypothesis with which the study began: recognition has run well ahead of realisation.

5. Conclusion

This study asked whether India's legal framework for privacy has kept pace with the right declared in 2017. On the evidence assembled here, it has not. Broadband connections grew more than sixfold in the decade to November 2025 and stood at 1,065.88 million by March 2026, while registered cybercrime rose by about 63 per cent between 2021 and 2023. The urban-rural divide widened over the same period, to 151.47 per cent tele-density in urban India against 60.46 per cent in rural India, which weakens the assumption of informed consent on which the whole statute rests. On portability, erasure, sensitive data and automated decisions the Indian law gives less than the General Data Protection Regulation gives. The State keeps its exemptions, appoints the regulator and has narrowed the Right to Information Act. And the interception laws that most directly enable State intrusion remain exactly as they were. The hypothesis holds: recognition has outpaced realisation.

References

Journal articles, books and working papers

1. Arun, C. (2014). Paper-thin safeguards and mass surveillance in India. *National Law School of India Review, 26*(2), 105–114.
2. Basu, S., & Guinchard, A. (2020). Restoring trust into the NHS: Promoting data protection as an "architecture of custody" for the sharing of data in direct care. *International Journal of Law and Information Technology*, *28*(3), 243–272. https://doi.org/10.1093/ijlit/eaaa014
3. Bhandari, V., & Sane, R. (2018). Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. *Socio-Legal Review, 14*(2), 143–169. https://doi.org/10.55496/uuiz9934
4. Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199679669.001.0001
5. Greenleaf, G. (2023). India's 2023 Data Privacy Act: Business/government friendly, consumer hostile. *Privacy Laws & Business International Report, 185*, 1, 3–12. https://doi.org/10.2139/ssrn.4666389
6. Greenleaf, G. (2025). Global data privacy laws 2025: 172 countries, twelve new in 2023/24. *Privacy Laws & Business International Report, 194*, 1.
7. Jha, N., & Lakra, R. (2026). Reevaluating publicly available data under the DPDPA Act 2023: A constitutional challenge. *Indian Law Review*. Advance online publication. https://doi.org/10.1080/24730580.2026.2619382
8. Kovacs, A. (2022). *Searching for a room of one's own in cyberspace: Datafication and the global feminisation of privacy* [Working paper]. Social Science Research Network.
9. Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.
10. Malhotra, C., & Malhotra, U. (2024). Putting interests of digital nagriks first: Digital Personal Data Protection (DPDP) Act 2023 of India. *Indian Journal of Public Administration*. Advance online publication. https://doi.org/10.1177/00195561241271575

11. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

12. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

13. Sonkar, A. (2025). The Digital Personal Data Protection Act, 2023: Analysing its implications, challenges, and future prospects. *International Cybersecurity Law Review, 6*(4), 547–569. https://doi.org/10.1365/s43439-025-00164-2

14. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

15. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

16. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Institutional reports and data sets

1. Access Now. (2024). *Shrinking democracy, growing violence: Internet shutdowns in 2023*. Access Now.

2. Access Now. (2025). *Emboldened offenders, endangered communities: Internet shutdowns in 2024*. Access Now.

3. Access Now. (2026). *#KeepItOn: Internet shutdowns in 2025*. Access Now.

4. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology, Government of India.

5. Indian Computer Emergency Response Team. (2023). *Annual report 2022*. Ministry of Electronics and Information Technology, Government of India.

6. International Telecommunication Union. (2024). *Facts and figures 2024: Measuring digital development*. ITU.

7. Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025* (G.S.R. 846(E), 13 November 2025). Gazette of India.

8. National Crime Records Bureau. (2023). *Crime in India 2022* (Vol. 2). Ministry of Home Affairs, Government of India.

9. National Crime Records Bureau. (2025). *Crime in India 2023* (Vol. 2). Ministry of Home Affairs, Government of India.

10. Reserve Bank of India. (2025). *Annual report 2024–25*. Reserve Bank of India.

11. Telecom Regulatory Authority of India. (2025). *Telecom subscription data as on 31st October 2025* (Press Release No. 141/2025). TRAI.

12. Telecom Regulatory Authority of India. (2026). *Telecom subscription data as on 31st March 2026* (Press Release No. 53/2026). TRAI.

13. Telecom Regulatory Authority of India. (2025). *The Indian telecom services performance indicators, January–March 2025*. TRAI.

14. Telecom Regulatory Authority of India. (2026). *The Indian telecom services performance indicators, January–March 2026*. TRAI.

15. Unique Identification Authority of India. (2025). *Aadhaar authentication surges past 2,707 crore in 2024-25* [Press release]. Ministry of Electronics and Information Technology, Government of India.

16. Unique Identification Authority of India. (2025). *Annual report 2024–25*. UIDAI.

17. United Nations Conference on Trade and Development. (n.d.). *Data protection and privacy legislation worldwide*. Global Cyberlaw Tracker. UNCTAD.

18. World Bank. (2024). *World development indicators: Individuals using the Internet (% of population), India* [Data set]. World Bank.

Cases cited

1. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
2. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
3. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
4. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1.
5. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
6. *M. P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
7. *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
8. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

Statutes and regulations

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016 (India).
2. Digital Personal Data Protection Act, No. 22 of 2023 (India).
3. Indian Telegraph Act, No. 13 of 1885 (India).
4. Information Technology Act, No. 21 of 2000 (India).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
6. Right to Information Act, No. 22 of 2005 (India).
7. Telecommunications Act, No. 44 of 2023 (India).

Note on source verification

Every source and every figure used in this paper has been checked against its publisher, repository or issuing authority. The judicial citations were checked against the reported series, and the statutory dates against the Gazette of India and the notifications of the Ministry of Electronics and Information Technology. Subscriber and tele-density figures come from the performance indicator reports and press releases of the Telecom Regulatory Authority of India, crime figures from the Crime in India volumes of the National Crime Records Bureau, and Aadhaar figures from releases of the Unique Identification Authority of India. Payment figures are taken from the Annual Report of the Reserve Bank of India, incident figures from the annual report of the Indian Computer Emergency Response Team, and comparative legislative figures from the Global Cyberlaw Tracker of the United Nations Conference on Trade and Development. Bibliographic details for the journal articles and books were checked against the publishers' own records and, where available, against the digital object identifier.

Three cautions are recorded for transparency. First, tele-density as reported by the Telecom Regulatory Authority includes machine-to-machine cellular connections; excluding them, overall tele-density in March 2026 was 84.57 per cent rather than 93.26 per cent, although the urban-rural gap remains. Second, the internet shutdown figures in Figure 5 are compiled by a civil society coalition and differ in method from figures placed before Parliament; they should be read as monitoring data rather than as official

statistics. Third, Kovacs (2022) is a working paper and not a peer-reviewed article, and has been cited as such.

Two items remain to be confirmed against the printed original before final submission, because they were available only as advance online publications at the time of writing and had not yet been assigned volume, issue and page numbers: Jha and Lakra (2026) in the Indian Law Review, and Malhotra and Malhotra (2024) in the Indian Journal of Public Administration.