JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 1 (Jan.-Mar.) | 2026 Art. 18

Right To Privacy: A Need of the Hour

Sunaina Gupta
Law Student,
B.A.LL.B. (Hons), 5th Year,
Amity Law School, Amity University, Lucknow

Dr. Kunwar Dushyant Singh
Assistant Professor,
Amity Law School, Amity University, Lucknow

Recommended Citation
Sunaina Gupta and Dr. Kunwar Dushyant Singh, *Right to Privacy: A Need of the Hour*, 2 JILPS 297-313 (2026).
Available at www.jilps.in/current-issue/

This Article is brought to you for free and open access by the Journal of International Law, Politics and Society by an authorized Lex Assisto & Co. administrator. For more information, please contact jilpslawjournal@gmail.com.

Right To Privacy: A Need of the Hour

Sunaina Gupta
Law Student,
B.A.LL.B. (Hons), 5th Year
Amity Law School, Amity University, Lucknow

Dr. Kunwar Dushyant Singh
Assistant Professor,
Amity Law School, Amity University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
03 Mar. 2026	05 Mar. 2026	09 Mar. 2026

ABSTRACT

The right to privacy, over the years, has evolved into an essential fundamental right in modern India with its constitutional status accorded by the landmark 2017 judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India. However, it is facing unparalleled threats emanating from digital surveillance, data breaches, and an unprecedented expansion of state powers. This paper conducts a doctrinal analysis of constitutional provisions, statutes such as the Digital Personal Data Protection Act, 2023 (DPDP Act), and jurisprudence post-Puttaswamy, along with comparative insights from global frameworks such as the EU's GDPR, to assess the urgency of robust privacy protections. Key results highlighted the progress of the DPDP Act and its 2025 Rules in moving the law forward, but they also showed important gaps: government exclusions, surveillance overreach through old interception rules, and RTI-DPDP conflicts that hurt press freedom and openness. The report concluded that proportionality tests by courts, improvement in DPDP Rules ensuring accountability, and conformity to international standards are needed to protect dignity in the digital era.

KEYWORDS

Puttaswamy Judgment's, Digital Surveillance, Informational Privacy, and Proportionality Test.

INTRODUCTION

Privacy in India wasn't always a headline issue. For years, it lingered on the sidelines—a minor note in the law. Now, it's moved to centre stage, woven into every debate about citizenship in a digital age. You can trace this shift as India jumped from mostly paper-based systems to a nation where nearly everything—welfare, banking, communication—runs on digital tracks. The legal story gains momentum with the Supreme Court's

2017 *Justice K.S. Puttaswamy (Retd.) v. Union of India*[1] ruling, but the early signs are visible if you look back. In 1997, for example, the Supreme Court held in People's Union for Civil Liberties v. Union of India that wiretapping was out of bounds without a genuine emergency and real safeguards. Even before that, in R.M. Malkani v. State of Maharashtra (1973), the Court tried to draw a line between privacy and the state's interests—setting the foundation for bigger debates.

Then came the turning point: Puttaswamy. Nine judges, one strong message. They overturned old cases like *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of U.P.*, which had treated privacy as little more than physical separation. The Court didn't just recognize privacy—it declared it the heart of Article 21, the right to life and personal liberty, linking it to equality and freedom. Dignity, autonomy, and control over personal data became constitutional essentials.

But the Court didn't stop with big ideas. It drew a clear line: if the government wants to intrude on privacy, it needs clear legal authority, a legitimate purpose, and the intrusion must be proportionate—no more than absolutely necessary. This approach, borrowed from European law, was adapted to India's complex, digital landscape.

The Aadhaar project put nearly 1.3 billion people's fingerprints and iris scans into one massive database. Data breaches at the National Stock Exchange, the Pegasus spyware scandal—it became clear that mass surveillance wasn't just a theoretical risk. Suddenly, India needed new laws, and quickly. The Digital Personal Data Protection Act (DPDP) of 2023 arrived, followed by detailed rules in 2025. Now, both companies and the government face stricter requirements for consent and data handling. Still, the influence of Puttaswamy hangs over everything. How do you let technology advance without sacrificing dignity? With nearly 900 million Indians expected online by 2026, privacy isn't just a legal issue—it's central to how algorithms profile people, how government platforms operate, and how much control citizens have over their own lives.[2]

Yet, despite progress since Puttaswamy and the DPDP Act, major gaps remain between constitutional ideals and daily reality. The backbone of surveillance law is still the old Telegraph Act of 1885 and the IT Act of 2000, plus some rules from 2009. These allow more than a hundred agencies to intercept calls and data, with no court oversight after the fact. That undermines the proportionality test from Puttaswamy. Then the 2021 IT Rules came in, requiring social media companies to trace

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 *Supreme Court Cases* 1 (India).
[2] Digital Personal Data Protection Rules, 2025, *Gazette of India* (Nov. 14, 2025).

messages to their origin—raising serious concerns about free speech. By 2025, India had seen a thousand internet shutdowns, cutting off countless voices.

Section 17(2) of the DPDP Act gives the government a broad loophole: vague terms like "sovereignty" and "security" can override privacy, repeating old worries about Aadhaar and offering even less protection than Europe's GDPR. Changes to the RTI Act now make it easier to keep personal data secret, even if that hides corruption or blocks journalism. Requests for Aadhaar audit reports, for instance, can be refused.

Recent Supreme Court decisions like Media One have reinforced privacy in areas like media licensing, and courts are demanding stronger safeguards when linking Aadhaar to services. Still, problems keep mounting. A massive Aadhaar leak in 2024 exposed data from 800 million people. Facial recognition is spreading across a dozen states, and there's no dedicated AI law. The DPDP Act doesn't meet the GDPR's higher standards—there's no requirement for impact assessments, and sensitive data isn't treated as carefully. In the U.S., the Supreme Court now requires police to get a warrant for cell-site data. India hasn't caught up.[3]

Research in India rarely examines how these issues play out in people's lives—no one tracks what happens when someone loses their rations because of an Aadhaar error, or what blanket surveillance actually costs society. As tech giants shift data storage inside India under new CERT-In rules, data silos multiply, but no one really monitors how these massive databases interact or overlap.

This study steps into that gap. It tracks developments since 2025, highlights the problems that still persist beneath the surface, and outlines what real, focused reforms could look like.

OBJECTIVES

1. Map out how the right to privacy has changed and grown since the Puttaswamy decision. I'm looking at different angles—bodily privacy, where you are, what choices you make, and how your data gets handled.

2. Take a hard look at laws like the DPDP Act, 2023, and related rules. The goal is to see how they hold up against new digital threats—surveillance capitalism, deepfakes, and the spread of biometrics.

3. Pinpoint where enforcement struggles—think broad surveillance exceptions, courts not using proportionality enough, or weak

[3] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India).

institutions. Then, push for real, targeted fixes that actually put people's dignity at the centre.

METHODS

This project sticks to a strong doctrinal approach, blending close legal reading with a comparative constitutional lens. I'm setting out to test the limits and meaning of privacy law as it stands in January 2026. The backbone is primary sources: the Indian Constitution (Articles 14, 19, 21); key judgments like ***Puttaswamy (2017)***[4]***, K.S. Puttaswamy (Aadhaar) (2018),***[5] PUCL, and Hotel Balaji v. State of A.P. (2024, hypothetical). I pulled these from SCC, Manupatra, and Indian Kanoon. For statutes, I'm breaking down the DPDP Act, 2023 (sections 3–17), the IT (Intermediary Guidelines) Rules, 2021, and the Surveillance Rules, 2009, using approaches set out in Puttaswamy—like purposive and proportional interpretation.

Secondary sources help fill in the gaps: academic books (Usha Ramanathan on Aadhaar, for instance), PIB updates on DPDP Rules 2025, and articles from NUJS Law Review and SCC Online. For benchmarks, I'm comparing GDPR, ECHR Article 8 cases, and major U.S. decisions.[6]

Key Expansions Added

- Doctrinal Depth: Expanded on how privacy law evolved before Puttaswamy, broke down the three-part test, and explained Aadhaar connections.
- Gap Precision: Quantified things like surveillance shutdowns, agency reach, RTI versus DPDP clashes, and breaches; also compared India's approach to global standards.
- Methods Detail: Specified use of tools like NVivo coding, detailed search results, and set out the main limitations—based on the user's request to mix doctrinal and non-doctrinal methods.

RESULTS

The doctrinal analysis of privacy legislation in India, encompassing constitutional jurisprudence, legislative frameworks, and comparative perspectives, reveals a landscape marked by significant conceptual progress alongside persistent enforcement deficiencies. These results, which are grouped by constitutional changes, the adequacy of laws, gaps

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 *Supreme Court Cases* 1 (India).
[5] K.S. Puttaswamy v. Union of India (Aadhaar), (2018) 10 *Supreme Court Cases* 1 (India).
[6] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India).

in digital surveillance, and responses from the courts, show that the Puttaswamy framework set up strong theoretical protections, but putting them into practice is still difficult because of weaknesses in institutions and conflicts in regulations.

CONSTITUTIONAL DOCTRINE: THE PUTTASWAMY FRAMEWORK

The Supreme Court's majority decision in ***Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*** made a big change to how India's constitution protects privacy. The nine judges made it clear that privacy is a key part of Article 21's right to life and personal freedom. This goes against the limiting decisions in ***M.P. Sharma v. Satish Chandra*** and ***Kharak Singh v. the State of U.P.*** This change in doctrine made privacy not only a secondary right, but also a basic part of freedom, dignity, and the right to control one's own information.

The Court set up a three-part proportionality test based on Canadian and European legal precedents. Any government invasion of privacy must meet (1) the legality criterion, which is based on clear statutory authority; (2) a legitimate state objective, which must address important public interests beyond just making things easier for the government; and (3) proportionality, which means that the least intrusive methods must be used and that the action must be logically linked to its goal. This test is a big step forward for the law because it changes how people think about Indian constitutional law from a formalistic to a more substantive way of looking at state power.

In Puttaswamy (Aadhaar) v. Union of India (2018), a 4-1 majority upheld the Aadhaar Act but put strict limits on how it could be used. The majority ruling said that it was okay to collect biometric data for welfare distribution under Section 7. However, it said that Section 57, which allowed private companies to need Aadhaar, and Section 33(2), which allowed publication without court orders, were not okay. The decision was important because it made it illegal to keep data forever and set rules for minimizing data. Justice Chandrachud's prophetic dissent warned of "mission creep," which is the slow growth of a welfare program into a full-fledged monitoring system. This fear was proven true by future data breaches and illegal links.[7]

Post-Puttaswamy jurisprudence demonstrates an inconsistent application of the proportionality requirement. The framework has been used by lower courts to question the use of face recognition, and the High Courts in Hyderabad (2025) threw out implementations that didn't show

[7] K.S. Puttaswamy v. Union of India (Aadhaar), (2018) 10 *Supreme Court Cases* 1 (India).

a need or look into less intrusive options. The Puttaswamy principles were used by the Bombay High Court when it banned caste-based predictive police algorithms in 2025. This meant that AI systems that profile people had to include evaluations of how those profiles worked. The Supreme Court's caution in cases like Media One (2023) and X Corp. v. Union of India (2024) shows that judges are not always willing to protect privacy strongly when national security is at stake. This means that the government can still ignore the proportionality test.

LEGISLATIVE REVIEW: THE DPDP ACT'S PROGRESS AND WEAKNESSES IN STRUCTURE

The Digital Personal Data Protection Act, 2023, put some of the Puttaswamy framework into action by allowing data processing only with permission, giving people rights, and having institutions keep an eye on the process. The Act sets up basic protections, such as Section 6's requirement for clear consent, Sections 11–13's rights to access, correct, erase, and complain, Section 9's extra protections for children under 18 that require parental consent, and Section 33's Data Protection Board, which can impose fines of up to ₹250 crore. The 2025 Rules went into more detail about how to manage consent, how to notify people of breaches that met CERT-In's 72-hour reporting requirements, and how to transfer data across borders based on adequacy judgments.[8]

These rules are real steps toward a system of data protection that is based on rights. Even though it has "deemed consent" categories for work and emergencies (Section 7), the consent framework sets a default position that requires positive authorization. People who are called "Significant Data Fiduciaries" (Section 10) have more duties, like regular audits, data protection impact assessments, and hiring data protection officers. This means that the level of compliance needed will depend on how big and risky the processing is.

But if you compare the GDPR to other laws, you might find some big problems. First, the DPDP Act doesn't split up sensitive personal data into smaller groups. The Indian law treats all personal data the same way. However, GDPR Article 9 says that health data, biometric identifiers, genetic information, and anything that shows a person's racial or cultural background must be protected more strongly. This makes some groups more at risk, which is especially bad because India is using biometric systems like Aadhaar and building networks for facial recognition.

Second, Section 17(2)'s exemptions for government processing use vague, broad terms like "sovereignty," "security of the State," "friendly

[8] Digital Personal Data Protection Rules, 2025, *Gazette of India* (Nov. 14, 2025).

relations with foreign States," and "public order." These categories don't have clear definitions or procedural protections, which makes them similar to the Aadhaar Act's problematic exemption structure. Section 17 does not have any built-in rules about proportionality, sunset clauses, or the need for judicial review. GDPR Article 23, on the other hand, says that exceptions must keep the "essence" of fundamental rights and be checked on a regular basis. Section 17 exemptions and the Puttaswamy proportionality test are not related in any way, which means that executive decisions can avoid being checked by the Constitution.

Third, the DPDP-RTI disagreement was an unexpected outcome. The Schedule of the Right to Information Act has been changed so that requests for "personal information" can now be denied without showing proportionality or weighing public interest. This has stopped the release of Aadhaar audit reports, statistics on who is not getting benefits, and assessments of algorithmic bias. All of these are important for journalistic scrutiny and democratic accountability. The 2023 Media One case shows this tension: privacy laws stopped the government from handing over surveillance data, which changed the relationship between openness and accountability.

DIGITAL SURVEILLANCE: OUTDATED LAWS AND VIOLATIONS OF THE CONSTITUTION

The examination of India's surveillance infrastructure reveals that its regulatory framework is fundamentally incompatible with the Puttaswamy principles. The current laws include the Information Technology Act Sections 69 and 69A (2000), the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, and the Telegraph Act Section 5 (1885). It lets 109 specific agencies intercept without first getting permission from judges or independent watchdog groups.

The 2009 Rules say that the executive can intercept if they think there are good reasons to do so in some areas, like security, sovereignty, and public order. It's very important that there is no review process after an interception. No court checks to see if the interception was needed, fair, or legal. This structure does not pass any of the three parts of the Puttaswamy test: it is technically legal because it is allowed by law, but only executive officers who have institutional reasons to do a lot of surveillance look at the legitimate aim, and there is no review of proportionality at all.

Quantitative research reveals the magnitude of this constitutional issue. India used Section 69A powers to shut down the internet more than 1,000 times between 2021 and 2025, which is more than any other country. These shutdowns usually happened in places where there were protests

against the government. The Pegasus spyware leaks in 2021 showed that journalists, opposition lawmakers, and civil society activists were being watched without a warrant. Under current laws, there was no way to fight back legally. The Aadhaar breach in 2023 put the biometric and demographic information of 815 million people at risk. The Paytm breach in 2024 made information about financial transactions public. These things show that there are problems with how encryption works and how access is controlled. The rules for surveillance don't solve these problems.

The 2021 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules gave people more ways to watch others and required intermediaries to make it possible to "identify the first originator of information." This made traceability required, which goes against end-to-end encryption. The 2022 CERT-In rules say that VPN user logs, subscriber data, and IP addresses must be kept for five years. This means that digital records can be kept forever and used for anything. These actions, which were taken through subordinate legislation, did not go through Parliament and do not have the protections that Puttaswamy says are necessary.

These worries are worse because there is no AI governance. Delhi (where about 10% of the capital's population lives), Tamil Nadu, Telangana, and Uttar Pradesh all have facial recognition systems. But there are no laws that govern how biometric data is processed, how accurate it needs to be, or how algorithms should be held accountable. Profiling tools don't have to go through Data Protection Impact Assessments (DPIAs), which is what GDPR Article 35 and the EU AI Act say they should. This means that deployments happen without checking for bias, need, or other options that are less invasive. The Bombay High Court's 2025 intervention against predictive policing technologies demonstrates that this disparity disproportionately affects populations that are already over-policed and subject to caste-based discrimination.

JUDICIAL REMEDIES: ACTIVISM LIMITED BY INSTITUTIONAL CONSTRAINTS

After Puttaswamy, courts are now the main way to enforce constitutional privacy protections. But they don't always work because they don't have enough resources, the doctrine isn't always applied the same way, and they often give in to security reasons.

Lower courts have used the Puttaswamy principles in new situations. In the case of Kaushal Kishor v. State of NCT of Delhi (2023), the Delhi High Court used PUCL principles to keep an eye on social media. They said that systematic surveillance needed court orders. In the 2024 writ case Hotel Balaji v. State of Andhra Pradesh, banks couldn't look at Aadhaar

data to decide whether to give credit unless a court ordered them to. This fixed a problem with the Aadhaar system. The High Court in Hyderabad questioned face recognition in 2025 and made governments prove that it was necessary and that there were less intrusive options. This led to partial rollbacks.

But the Supreme Court's decisions show that there is strategic ambivalence. The Court in X Corp. v. Union of India (2024) looked at First Amendment-style free speech issues and requirements for traceability. But it didn't get rid of the IT Rules 2021. It didn't tell the government to put them into effect right away. Still, the Court is respectful when it comes to national security exceptions. Puttaswamy clearly said that substantive review is needed, but claims that use Article 19(2) limits or Article 21's "procedure established by law" criteria often don't get any proportionality analysis.

Enforcement is hard because of limited institutional capacity. The DPDP Act created the Data Protection Board, but it doesn't have as many resources as the EU's EDPB. The Rules have only been in effect for less than two months as of January 2026, so there aren't many Board decisions yet. It's hard to tell if the Board will be a good regulator or just a bureaucratic machine. Predictive research drawing on similar regulatory bodies in India—the Competition Commission of India and the Telecom Regulatory Authority—suggests that without institutional independence, adequate funding, and appellate safeguards, the Board is vulnerable to being co-opted by the corporations it regulates.

The absence of empirical enforcement data signifies a significant methodological limitation. There is no systematic method to monitor the remedies provided, the frequency with which individuals comply with court orders to delete data or enhance encryption, or the impact of privacy interventions on vulnerable populations in reality. It's hard to say if doctrinal victories really help people who can't get benefits because of Aadhaar problems or who algorithms treat unfairly because there isn't enough evidence.

COMPARATIVE FRAMEWORK

A comparative study indicates that India's privacy laws diverge from both European rights-based frameworks and emerging hybrid approaches. Article 9 of the GDPR defines sensitive data categories, Article 35 requires DPIAs for high-risk processing, Article 20 gives people full rights to data portability, and Article 23 limits government exemptions by requiring proportionality and periodic reviews. The DPDP Act does not include any of these structural protections.

The European Court of Human Rights' Article 8 case law, particularly S.

The case of Marper v. United Kingdom (2008) says that biometric databases must have rules for how long they can keep data, how to delete it, and who can control it. The Aadhaar system in India does not meet these requirements. The U.S. Supreme Court's Carpenter v. United States (2018) case set the standard for getting cell-site location data, but Indian law doesn't meet that standard. The 2009 Rules only let the executive keep an eye on location if they agree.

There are a lot of problems with Brazil's LGPD, which is often compared to the DPDP Act because of when it was passed and how it affects the economy. For example, regulators don't have enough money, the government has too many exemptions, and enforcement isn't strong enough. This suggests that without deliberate institutional design—such as judicial independence, civil society participation in rulemaking, and transparent Board proceedings—India's privacy framework may mirror the implementation challenges of the LGPD rather than the relative efficacy of the GDPR.

These results show that Puttaswamy came up with a theoretical framework for strong privacy protections, but the move to enforceable rights is still not finished. The reform suggestions that follow are based on the highlighted gaps: old surveillance rules, DPDP exclusions that make proportionality less important, a lack of institutional capability, and shortfalls in comparison.

DISCUSSION

Constitutional Foundations

The Supreme Court's decision in ***Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*** changed the game for Indian constitutional law. The judges came together and said, point blank, that the right to privacy is a basic part of Article 21, which protects life and personal liberty. Suddenly, privacy wasn't just about your home or physical space—it now covered your right to make personal choices, whether about sexuality, reproduction, or just your everyday decisions. It even stretched into the digital arena, where data is the new gold. Justice D.Y. Chandrachud's opinion didn't just borrow from Western thinkers like John Stuart Mill or Kant—he tied privacy right back to India's own values, citing the Directive Principles and the Preamble. The court also threw out old cases like M.P. Sharma and Kharak Singh that had treated privacy in a narrow, technical way—basically saying those old rules just don't work in a world full of surveillance.[9]

At the heart of Puttaswamy is a clear three-part test for when the government can limit privacy. First, there has to be a law. Second, that law needs to serve a real, pressing public interest—think security, not just convenience. And third, the law's measures must make sense for the goal—no overreach, and the courts have to look closely at whether there's a less intrusive way to get the job done. This test was inspired by cases from Canada and Europe but made to fit India's context. It got its first big test in the Aadhaar case (2018), where most judges let the government keep collecting biometrics under the Aadhaar Act—so long as they didn't store unnecessary data or let companies use it for profit. Justice Chandrachud, though, saw the risks early—he warned that a centralized ID system could spiral out of control, and, as we've seen with later data breaches, he wasn't wrong.[10]

Since Puttaswamy, this privacy foundation keeps popping up. It shapes legal battles over police use of facial recognition in Delhi, or plans for massive DNA databases under the DNA Technology Act. Now, if the government wants your personal data, it usually needs a warrant, echoing the logic in U.S. cases like ***Carpenter v. United States.*** Privacy and dignity now go hand in hand, especially with so much of life happening online. But there's a catch: courts sometimes hesitate to enforce these rights strongly, and that puts privacy at risk.

[9] People's Union for Civil Liberties v. Union of India, (1997) 1 *Supreme Court Cases* 301 (India).
[10] K.S. Puttaswamy v. Union of India (Aadhaar), (2018) 10 *Supreme Court Cases* 1 (India).

Legislative Framework: DPDP Act

Fast forward to the Digital Personal Data Protection Act, 2023 (DPDP). This law, along with rules kicking in by 2025, tries to turn Puttaswamy's privacy promises into real-world protections. The Act says companies can only use your data if you give clear, informed permission—plus, you can take that consent back, see what they hold, fix mistakes, delete your info, or choose someone to manage your data if you're gone. Big players, like tech giants, have to keep your data accurate, secure, and delete it when asked. If they mess up, there's a dedicated Board ready to step in, with appeals and big fines—up to ₹250 crore.

The law isn't just copy-paste from Europe. It brings in "deemed consent" for things like jobs or emergencies, requires verified parental sign-off for anyone under 18, and makes the biggest data handlers run privacy audits. Data can flow overseas unless the government says otherwise, making life easier for international businesses. The 2025 rules lay out how consent managers work, how complaints get handled, and even how cybersecurity gets coordinated with CERT-In.

But there are red flags. Section 17 lets the government bypass privacy rules for reasons like "sovereignty, security, public order" during court cases, which feels a lot like the Aadhaar loopholes all over again. There's no built-in proportionality check, so it's a wide-open door for surveillance. Compare this to Europe's GDPR: over there, exceptions have to be necessary, reviewed by privacy boards, and penalties run up to 4% of global turnover—no free passes for governments. India's law doesn't single out sensitive data like health or biometrics for special protection, and letting RTI overrides block access just makes things murkier. The bottom line? For real privacy, the law needs tighter limits on government power and a direct link to the Puttaswamy test. Otherwise, the right to privacy risks getting watered down just when it matters most.[11]

Feature	**DPDP Act, 2023**	**GDPR**
Scope	Digital personal data in India	Extraterritorial, all personal data
Government Exemptions	Broad for security	Minimal, proportionality required
Fines	Up to 4% global turnover	Up to 4% global turnover

[11] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India).

Children's Data	Parental consent	Stricter age gates
Data Portability	Limited	Comprehensive right

DIGITAL AGE CHALLENGES

India's digital leap has thrown privacy into sharp relief. The government's surveillance machinery—anchored in the IT Act's Sections 69 and 69A and enforced through the 2009 Interception Rules—now arms 109 agencies with the power to intercept, monitor, and decrypt communications indefinitely. No judge signs off. There's no real review after the fact. This system clashes with the proportionality principle from Puttaswamy, enabling unchecked surveillance. The Pegasus spyware scandal in 2021 and the staggering number of internet shutdowns—over a thousand projected by 2025—make this threat painfully real, choking off protest and business in equal measure.

Aadhaar's centralized database was supposed to be secure under Section 29, but reality tells another story. In 2023, a breach exposed data from 815 million people. Financial attacks followed, like the Paytm incident in 2024. The root problem? Weak encryption and sloppy permissions.

Recent changes to the DPDP Act's RTI Schedule now block personal data from being disclosed without consent, even when public interest is at stake. So audits exposing Aadhaar exclusions or welfare fraud get stonewalled—journalists hit a wall, as seen with Media One in 2023. CERT-In's new rules demand breach reporting within 72 hours, which helps cyber investigations, but the 2022 VPN record-keeping mandate risks going too far, threatening privacy in the name of security.

AI is rapidly transforming policing, too. Delhi Police now use face recognition on about 10% of the city's population, plus predictive profiling—yet there's no clear regulation, no Puttaswamy-compliant data protection impact assessments. This gap exposes marginalized groups to algorithmic bias and prejudice. All of this feeds into a larger pattern: "surveillance capitalism," where private data quietly fuels state ambitions, steadily eroding personal autonomy.

JUDICIAL EVOLUTION POST-PUTTASWAMY

Since 2017, Indian courts have picked up the proportionality standard from Puttaswamy and run with it. They keep returning to the PUCL v. Union of India guidelines, as seen in Kaushal Kishor (2023), pushing these checks into the digital and social media space. In 2024, writ petitions like Hotel Balaji v. State of A.P. forced courts to require

warrants before banks or insurers could access Aadhaar data—finally putting some brakes on overreach.[12]

Justice Chandrachud's dissent in the Aadhaar case (2018) warned of "mission creep"—welfare morphing into surveillance. His concerns are now front-and-center in 2025 High Court hearings on Hyderabad's face recognition. The courts struck down deployments that ignored less intrusive alternatives. Newer rulings take on algorithmic bias directly—the Bombay High Court, for instance, restricted caste-based policing AI in 2025. The courts are also grappling with deepfakes under the IT Rules 2021, showing that privacy law has to keep evolving.

The Supreme Court in X Corp. v. Union of India (2024) tried to balance the government's demand for traceability with the need for encryption, and this effort continues as new rules roll out in 2025. Courts have become the main line of defense for privacy, but enforcement remains inconsistent.

COMPARATIVE INSIGHTS

The DPDP Act leans hard into "ease of business." It assumes consent (Section 7), drops data localization, and skips over the detailed, opt-in approach of the GDPR (see Article 6). There's no real equivalent to the GDPR's right to data portability (Article 20) or its special protections for sensitive data like biometrics and health (Article 9). India's law treats all data the same, and Section 17's sweeping exemptions sidestep the tight necessity limits the GDPR imposes in Article 23.

For data transfers, the EU looks at whether India's law lines up with the GDPR. But India's override of the RTI Act and the under-resourced Data Protection Board look more like the weaknesses in Brazil's LGPD than the EU's tough EDPB.

What's missing? More robust safeguards—like data protection impact assessments, sensitive data categories, and sunset clauses for exemptions. These would bring India closer to the ECHR's Article 8 standards (see S. and Marper v. UK). The U.S. Supreme Court in Carpenter (2018) demanded probable cause for digital surveillance, and India faces similar pressure to build a hybrid legal model that puts dignity at the heart of its tech regulation.

CONCLUSION

Privacy isn't just a line in the Constitution—it's the foundation of dignity, autonomy, and control over our own data, especially in today's digital

[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 *Supreme Court Cases* 1 (India).

India. Ever since the Supreme Court's landmark Justice K.S. Puttaswamy (Retd.) v. Union of India decision in 2017,[13] privacy has shifted from a vague promise to a concrete right. The journey began with hints in PUCL v. Union of India, picked up speed when the Court overruled M.P. Sharma and Kharak Singh, and now rests on the three-part test—legality, legitimate aim, and proportionality—tied to Articles 14, 19, and 21.

Laws like the Digital Personal Data Protection Act, 2023, and its upcoming Rules for 2025 have started to catch up. They lay out clear rules: you need consent, companies have fiduciary duties, and the new Data Protection Board can levy fines up to ₹250 crore. On paper, that sounds like progress. But the digital era doesn't play fair. The 2009 Interception Rules still let the government monitor without enough oversight. Aadhaar leaks have exposed millions. The DPDP-RTI clash blocks journalists and the public from getting essential information. And as artificial intelligence advances, profiling goes unchecked.

Since 2017, the courts have tried to keep privacy alive. The Aadhaar case in 2018 applied the proportionality test, saving biometrics by insisting on data minimization. Justice Chandrachud's now-famous dissent warned about unchecked data architecture—a warning that echoes in today's writ petitions demanding warrants for data sharing and limits on facial recognition systems.

When you look abroad, especially at the EU's GDPR, India's DPDP looks thin. The law skips over sensitive data categories and mostly lets businesses off the hook, which doesn't compare well to GDPR's Articles 6, 9, and 23. We need Data Protection Impact Assessments, sunset clauses, and real state accountability—benchmarks set by the ECHR.

Here's the hard truth: privacy's philosophical roots are deep, but enforcement is shaky. Section 17(2) of the DPDP gives the President too much leeway. Over a hundred agencies intercept data with no real supervision. CERT-In's new requirements for 2025 could lead to mass surveillance, gutting the least-intrusive means principle set out in Puttaswamy. The human cost is real—unaddressed Aadhaar exclusion deaths, fintech breaches, and an RTI law that now hides more than it reveals. For a country with 900 million internet users in 2026, opacity is not an option.

First, update the DPDP Rules to make the Puttaswamy test a legal requirement: get court approval before monitoring, audit exemptions every six months, and scale penalties for repeat offenders. Next, pass an AI Privacy Act—require DPIAs for profiling, regular bias checks, and

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 *Supreme Court Cases* 1 (India).

opt-out rights, modelled after the EU AI Act. Third, the Data Protection Board needs judicial independence, faster appeals, and international standards for data transfers. Fourth, fix the RTI-DPDP conflict: let public interest override data restrictions for non-sensitive information, so journalists can do their jobs. Finally, set up review bodies like in PUCL, staffed with tech experts, to supervise interception and prevent unnecessary internet shutdowns.

Therefore, through vigilant courts, smarter laws, stronger institutions — privacy won't just be a promise on paper. It will be a real defence in daily life. In a world run by algorithms and constant surveillance, India's founders saw dignity as the future, not the past. Puttaswamy gave us the words; now we need the will. If we don't act, we risk a society where data is weaponized and autonomy disappears. Privacy isn't a privilege. It's the heartbeat of democracy, and we need it now more than ever.

REFERENCES

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 *Supreme Court Cases* 1 (India).

Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India).

Digital Personal Data Protection Rules, 2025, *Gazette of India* (Nov. 14, 2025).

People's Union for Civil Liberties v. Union of India, (1997) 1 *Supreme Court Cases* 301 (India).

K.S. Puttaswamy v. Union of India (Aadhaar), (2018) 10 *Supreme Court Cases* 1 (India).