INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ONLINE SURVEILLANCE, DATA PROTECTION, AND PRIVACY IN INDIA: A CONSTITUTIONAL AND LEGAL PERSPECTIVE

AUTHOR - PRIYANSHU CHATURVEDI, STUDENT AT UNIVERSITY OF ALLAHABAD

BEST CITATION - PRIYANSHU CHATURVEDI, ONLINE SURVEILLANCE, DATA PROTECTION, AND PRIVACY IN INDIA: A CONSTITUTIONAL AND LEGAL PERSPECTIVE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (1) OF 2026, PG. 455-459, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

Recognizing the right to privacy as a fundamental right in the Indian Constitution has changed how we think about personal freedom and state power. These days, everything's digital. The government and private companies collect, handle, and store our personal data all the time. That brings up big questions about surveillance, autonomy, and dignity—questions that go right to the heart of the Constitution.

This paper digs into how the idea of privacy has grown in India, starting from its roots in the Constitution and shaping up through the courts, especially after the huge Justice K.S. Puttaswamy v. Union of India decision back in 2017. It looks at the new problems cropping up as digital governance expands—things like mass surveillance, biometric ID systems, and data-driven policies. There's always a tug-of-war between state interests like national security or public order and the rights of individuals to privacy and autonomy. The paper looks at how courts and lawmakers have tried to strike that balance, and it brings in international privacy law to show where India stands.

Honestly, with digital tech moving so fast, if we don't have strong laws, real oversight, and tough data protection, the whole promise of privacy could fade away. The study wraps up with practical legal steps India can take to strengthen privacy protections and keep that constitutional promise alive

Introduction

Privacy sits right at the heart of modern constitutional democracies. It shapes how people relate to the state and sets the boundaries for how much the government can intrude into someone's personal life. In India, you won't find the word "privacy" spelled out as a fundamental right in the Constitution. But thanks to the way courts have read and expanded Article 21—the guarantee of life and personal liberty—privacy has become a constitutional right in practice.

Technology has changed everything. Now we have digital governance, biometric IDs, artificial intelligence, and massive data collection. People aren't just citizens on paper anymore; they've got digital profiles that decide how they access welfare, services, and even their rights. This shift has created a new kind of power imbalance between the state and the individual. Protecting privacy isn't just about personal freedom anymore—it's become essential for democracy itself.

This paper looks at how the right to privacy has evolved in India, both through the Constitution and in courtrooms. It digs into digital surveillance and data collection, and asks: Are India's current laws strong enough to keep up? Can constitutional principles really protect dignity and autonomy in the era of digital governance?

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Literature Review / Law

Constitutional Provisions

Article 21 is the bedrock for privacy in India. It guarantees the right to life and personal liberty, and judges have repeatedly stretched its meaning to cover everything a person needs to live with dignity. Articles 14 and 19 also matter—they're about equality and freedom, and they back up privacy, even if not directly.

Judicial Development

Early on, Indian courts didn't even recognize privacy as a right. In M.P. Sharma (1954) and Kharak Singh (1963), the Supreme Court flat-out said there was no constitutional right to privacy. Still, they admitted there were some protections for personal liberty.

Things started to shift with cases like Gobind v. State of Madhya Pradesh (1975), where the Court acknowledged privacy as an implicit constitutional value. The real turning point came with Justice K.S. Puttaswamy v. Union of India (2017). A nine-judge bench unanimously declared privacy a fundamental right under Article 21, making it a core part of the Constitution's protections.

Statutory Framework

India's data protection laws have grown bit by bit, with sector-specific rules leading up to the Digital Personal Data Protection Act, 2023. This law sets out how personal data should be handled and aims to protect people's information. Still, there are big concerns—especially about how the law is carried out, the wide exemptions, and the broad surveillance powers the state still holds.

Analysis / Discussion

The Constitutional Value of Privacy

Recognizing privacy as a fundamental right shifts it from just a legal policy to a constitutional duty. It's no longer about protecting physical spaces—it's about giving people control over their own information, choices, and identity.

The Supreme Court, especially in the Puttaswamy judgment, made it clear: privacy is tied to dignity, autonomy, and liberty. It's not some special privilege—it belongs to everyone, no matter who they are. In a constitutional democracy, that's a moral foundation.

Institutional Challenges, Algorithmic Governance, and Structural Risks to Privacy

Institutional Deficit in Privacy Protection

India's Supreme Court has recognized privacy as a fundamental right, which sounds like a big win. But on the ground, the systems needed to protect that right just aren't there yet. It's not enough to declare privacy a right in theory—you need real ways to enforce it, actual institutions that know what they're doing, and clear lines of accountability. Without these, privacy risks turning into more of a promise than something people actually experience.

Right now, the job of protecting privacy mostly falls to executive agencies. The problem? These agencies often work behind closed doors, without much independent oversight or real transparency. They're the ones in charge of greenlighting surveillance, collecting data, and sharing information, but Parliament hardly gets a say. So, power piles up on the government's side, and ordinary people don't have many options to push back. It messes with the whole idea of checks and balances.

Courts are supposed to help, but they usually step in only after the damage is done. The legal system offers relief once a violation happens, but it doesn't do much to stop problems before they start. And in the digital world, once your data is out there, you can't really put the genie back in the bottle. The harm is permanent, which makes prevention way more important than patching things up afterward.

There's another gap, too—India doesn't have a dedicated body to handle privacy issues the way it does for the environment or consumer rights. That means there's no specialized place for people to go when their privacy is threatened. Without this kind of structure, the

promise of privacy in the Constitution ends up hollow.

Algorithmic Governance and Automated Decision-Making

Government is changing fast, and a big part of that shift comes from algorithms and automated systems. These days, governments use algorithms everywhere — handing out welfare, checking IDs, running risk assessments, policing, even making administrative decisions. All of this leans on crunching personal data.

But bringing algorithms into the heart of government isn't as simple as it sounds. Privacy takes a hit, and there are real constitutional worries, too. The problem is, most of these systems run in the shadows — they're "black boxes." If you're on the receiving end, you don't get to see how or why the system made a call about your rights or your benefits. That kind of secrecy chips away at the ideas of transparency, accountability, and fair process.

Then there's the issue of automated profiling. These systems build digital versions of people, but let's be real — they get it wrong, a lot. Bad data, biases baked into the code, mistakes in the inputs — all of that can mean someone gets shut out, treated unfairly, or flat-out denied their rights. When a computer starts to replace human judgment, people stop being citizens with rights and just become data points in a system.

It goes deeper, too. At the heart of the constitution is the idea that every person has dignity. Reducing people to their data strips that away. Suddenly, citizens start to look more like objects to be managed than individuals with agency and rights. That's not what Article 21 — with its focus on dignity, autonomy, and personal freedom — is supposed to protect.

And there's another problem: surveillance. Algorithms don't just watch what you've done; they try to guess what you might do next. So the government moves from judging actions to predicting behavior, operating more on suspicion than on actual evidence. That flips the script on the whole relationship between the state and its people. The presumption of innocence and the rule of law start to look shaky when a computer decides you're risky before you've done anything at all.

Surveillance Capitalism and Private Data Power

Privacy threats these days aren't just about big government watching you. Now, private companies—especially tech giants—hold more personal data than most governments ever have. They scoop it up, sift through it, and turn it into profit. People call this "surveillance capitalism," and honestly, it's a kind of power that's slipped right past the usual checks and balances you'd expect from the Constitution.

These data monopolies don't just sell ads. They shape what you see, what you click, and even what you think—using algorithms and carefully curated content. On the surface, it's all about business. But dig a little deeper, and you see the real impact. These tactics sway public opinion, nudge elections, and change how society talks to itself.

The law usually deals with what the government does, but the digital world isn't that simple anymore. Tech companies now do things you'd expect from public agencies—like verifying your identity, handling payments, running welfare systems, and basically acting as the town square. When they take on these roles, their choices start to matter in the same way government decisions do.

Here's the problem: the old rules don't fit. There are gaps—places where neither constitutional law nor regular regulations keep your privacy safe. As these companies become part of the backbone of daily life, it's clear that privacy protections can't just focus on the government. They need to keep up with this new reality.

Informational Inequality and Digital Exclusion

Privacy violations hit marginalized communities the hardest. People without much digital know-how, those struggling financially, or folks who can't easily fight back legally—they're the ones

most at risk for data abuse and constant surveillance.

This gap in who understands technology and who doesn't? It's another kind of discrimination. If you don't really get what companies are doing with your information, you can't give real consent. Those long privacy policies and so-called "agreements" end up being a sham when people aren't really choosing—just clicking through because they have to.

Look at digital identity systems. When they're not handled properly, they can actually shut people out of things they need, like welfare, healthcare, or public services. Suddenly, privacy isn't just some abstract right—it's about whether you can get the basics you need to live.

So, privacy isn't just something for the privileged to worry about. It's a justice issue. If we want real equality and inclusion, protecting privacy has to be part of the foundation in any democracy that claims to care about social justice.

State Power and Digital Surveillance

Digital surveillance is a new kind of government control. Unlike old-school surveillance, where someone was physically followed or watched, digital tools allow the state to monitor people constantly, automatically, and at a huge scale. Biometric IDs, facial recognition, metadata collection, predictive policing—these systems operate in the background, often without anyone noticing.

This kind of surveillance chills democracy. When people know they're always being watched, they start to hold back. They think twice before speaking, meeting, or moving around freely. Privacy, then, isn't just a luxury—it's vital for keeping democratic participation and free thought alive.

Proportionality and Constitutional Restraints

The Supreme Court's decision in Puttaswamy laid down a clear test to check state action against privacy. It comes down to five points: legality, a legitimate state goal, necessity, proportionality, and having real procedural safeguards.

That sounds solid on paper. But, honestly, putting this into practice is where things fall apart. Laws can be vague, government agencies often have blurry limits, and proper checks are missing. In the end, these loopholes make constitutional protections feel more like suggestions than real shields.

Comparative Perspective

Look at the European Union. There, privacy isn't just a nice idea — it's a fundamental right, locked into the Charter of Fundamental Rights. The GDPR actually enforces it, with strong rules on consent and independent watchdogs.

The U.S. takes a different route. Privacy law there is tied to liberty and due process. Even so, their national security agencies get a lot of leeway to watch people.

India is still figuring this out. The Constitution now recognizes privacy, but the systems to enforce it are shaky, and the regulators don't have enough teeth.

Findings / Observations

1. Privacy has solid backing in the Indian Constitution, but enforcement by institutions is weak.

2. Digital governance is moving faster than privacy protections.

3. Surveillance isn't very open or accountable.

4. Data protection laws talk about rights, but don't offer much in practice.

5. Courts are evolving the doctrine, but the government isn't really following through.

Conclusion / Recommendations

Recognizing privacy as a constitutional right was a turning point for India. But, let's be real — words on a page only go so far. In a world where data and algorithms hold real power, protecting privacy needs more than good intentions. It needs strong institutions that actually work.

Today, privacy isn't just about individuals. It's the backbone of democracy. Without it, freedom is just for show, dignity is hollow, and liberty comes with strings attached

Recommendations

1. Establishment of independent data protection authorities
2. Strong judicial oversight over surveillance mechanisms
3. Transparent data governance frameworks
4. Limitation of blanket exemptions to State agencies
5. Public accountability mechanisms for digital governance systems
6. Privacy impact assessments for government technologies

References / Bibliography (Bluebook Style)

1. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
2. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
3. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
4. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
5. Constitution of India, art. 21.
6. Digital Personal Data Protection Act, 2023 (India).
7. Granville Austin, The Indian Constitution: Cornerstone of a Nation (Oxford Univ. Press 1999).
8. Upendra Baxi, The Future of Human Rights (Oxford Univ. Press 2006).
9. Gautam Bhatia, Offend, Shock, or Disturb: Free Speech under the Indian Constitution (Oxford Univ. Press 2016).
10. Justice B.N. Srikrishna Committee Report on Data Protection Framework for India (2018).