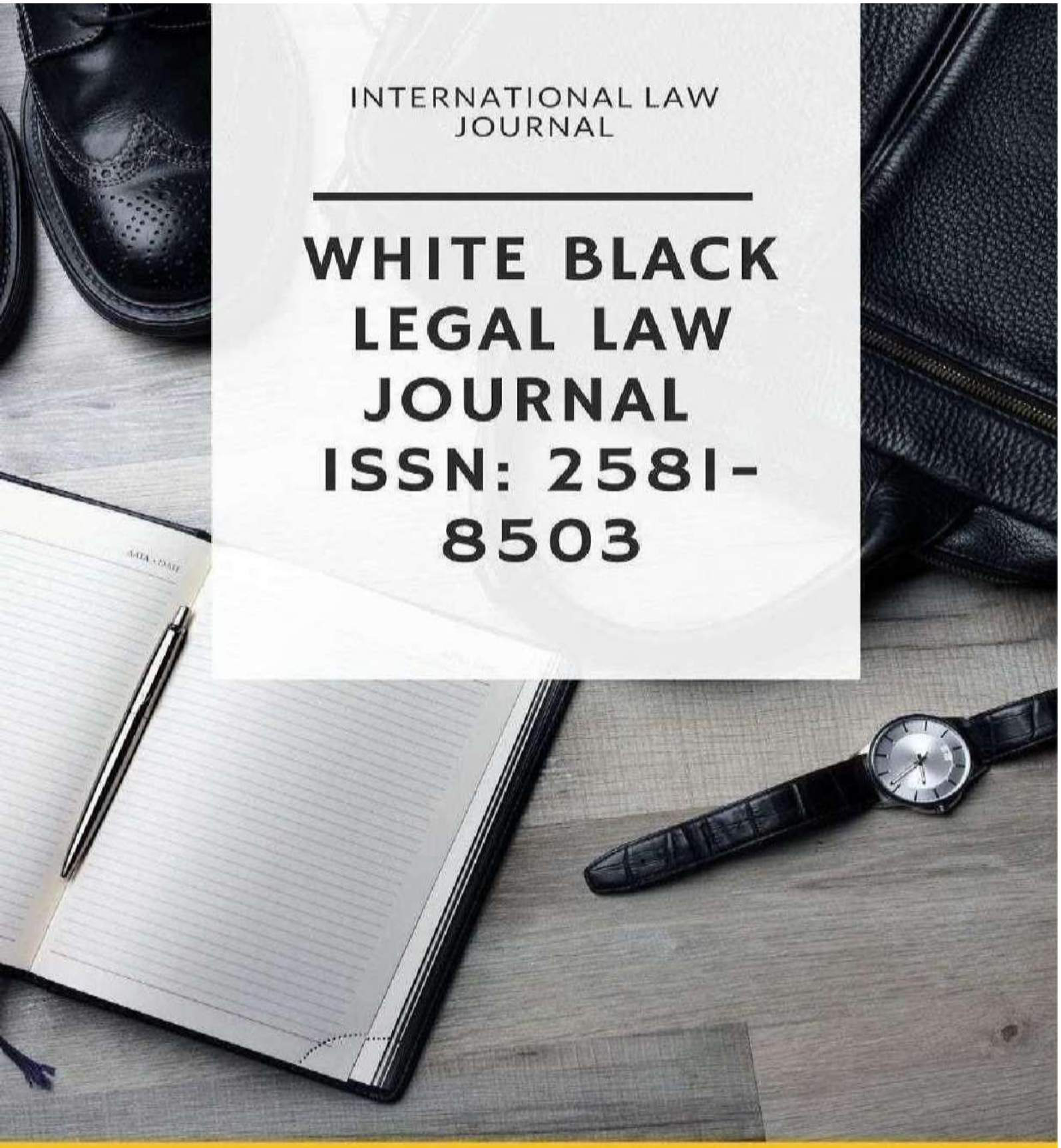

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 3 | Jan 2026 ISSN: 2581-8503

DIGITAL SURVEILLANCE AND THE RIGHT TO PRIVACY: RECONCILING NATIONAL SECURITY WITH HUMAN RIGHTS IN INDIA

AUTHORED BY – SIMRAN

Abstract

Digital surveillance has become a defining feature of contemporary governance. While the State's interest in national security and public order is legitimate, bulk and opaque surveillance threaten core human rights—particularly privacy, dignity, equality, free speech, and due process. In India, the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (2017) recalibrated the constitutional balance and imported a rigorous proportionality standard into all restrictions on rights. Yet the statutory architecture—the Telegraph Act, 1885 and the Information Technology Act, 2000 with their interception and monitoring rules—predates modern, data-saturated reality and lacks independent authorization, meaningful oversight, notice, or remedies. This paper situates India's debate within international human rights law (ICCPR) and comparative practice (EU data protection norms), critically assessing gaps in legality, necessity, and proportionality. It proposes a rights-conform surveillance law with judicial warrants, independent supervision, transparency obligations, and strong data-governance safeguards, arguing that constitutional security is maximized when privacy and accountability are structurally protected.

Keywords

Privacy, Surveillance, Proportionality, National Security, ICCPR, India, GDPR, Free Speech, Rule of Law

Literature Review

Early Indian commentary treated surveillance as an administrative police function justified by public order, with courts historically deferring to executive necessity. Post-Emergency scholarship shifted toward rights-protective analysis, foregrounding chilling effects on speech and association. The seminal PUCL (1997) judgment prompted a burst of doctrinal writing on "legality" and "procedure established by law" in wiretapping, highlighting the need for clear

rules, recorded reasons, and review. After 2017, literature largely re-centred on privacy as a fundamental right and proportionality as the test for all restrictions, with scholars drawing on European and Canadian jurisprudence to critique mass, indiscriminate collection and metadata dragnet programs.

Policy think-tanks and rights groups (focusing on interception orders, facial recognition deployments, and data retention) consistently identify four deficits in India: (1) executive-only authorization (no independent warrants), (2) bulk collection and function creep without purpose limitation, (3) opacity (secrecy around orders, vendor systems, accuracy), and (4) weak remedies (limited user notice or ex post challenge). Comparative literature on the EU GDPR and ECHR case law (e.g., data minimization, purpose limitation, necessity, partial anonymization/pseudonymization, and independent supervisory authorities) is frequently invoked as a reference model. Constitutional scholars further underscore that surveillance regimes have equality impacts—they disproportionately chill journalists, minorities, activists, and opposition voices, thereby shaping democratic participation.

Research Methodology

This study adopts a doctrinal and comparative methodology:

- **Primary legal sources**: Supreme Court jurisprudence on privacy and communications restrictions; constitutional text (Arts. 14, 19, 21); and statutory provisions enabling interception/monitoring/search.
- **International law**: ICCPR Article 17 and General Comment-level principles; EU data-protection concepts for comparative context.
- **Secondary sources**: academic monographs, journal articles, and policy reports mapping institutional design and technical risks (e.g., facial recognition, data lakes, linkage).

The approach is qualitative and normative-evaluative, applying proportionality and rule-of-law benchmarks to assess India's framework and proposing a rights-conform redesign.

Introduction

Surveillance technology has evolved from targeted wiretapping to always-on, data-exhaust ecosystems: pervasive sensors, telecom metadata, device-location trails, platform logs, facial recognition, and AI-assisted analytics. In constitutional terms, the challenge is not merely

informational capture but aggregability the ability to link, infer, and profile at scale. This transforms surveillance from episodic investigation to ambient governance, altering citizens' behaviour through self-censorship and inhibiting association, journalism, and dissent.

The Indian Constitution does not explicitly mention "privacy," but the Supreme Court's nine-judge bench in Puttaswamy (2017) declared privacy a fundamental right intrinsic to life and personal liberty (Art. 21) and guaranteed by equality and free speech (Arts. 14 and 19). The Court constitutionalized proportionality requiring a lawful aim, suitability, necessity (least-restrictive means), and balancing. This standard obliges the State to justify surveillance through clear law, narrow tailoring, and structured oversight. Parallelly, international norms (ICCPR Art. 17) prohibit arbitrary or unlawful interference with privacy and call for legality, necessity, and proportionality.

Yet India's interception architecture relies on colonial-era or early-IT-era statutes and rules, designed for narrow wiretaps, not pervasive data ecosystems. The result is a legality that is formally authorized yet substantively under-protected: broad executive discretion, minimal transparency, limited independent checks, and sparse remedies.

Constitutional Foundations After Puttaswamy

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) fundamentally redefined the contours of personal liberty and privacy in India. The nine-judge bench unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21 of the Constitution, as well as to the freedoms guaranteed by Articles 14 and 19. This decision did not merely add a new right—it restructured the constitutional relationship between the individual and the State by placing autonomy, dignity, and choice at the core of constitutional morality. In the post-*Puttaswamy* era, every aspect of intimate life—including relationships, sexuality, and cohabitation—is shielded by this expanded constitutional protection.

A. Privacy as the Core of Personal Liberty

The *Puttaswamy* judgment recognized privacy as a multifaceted right encompassing decisional, informational, and bodily autonomy. It affirmed that the freedom to make personal choices in matters of love, intimacy, and partnership lies within the protected zone of privacy. This includes the right to live with a partner of one's choice, regardless of marital status. The Court's reasoning emphasized that the State has no authority to

intrude upon consensual adult relationships that do not harm others or disrupt public order. This acknowledgment elevated individual choice to a constitutionally protected domain, insulating relationships like live-in unions from societal interference and moral policing.

B. Autonomy, Dignity, and Equality

In linking privacy with dignity and equality, *Puttaswamy* anchored personal relationships within the larger framework of human dignity. The judgment underscored that dignity is not conferred by marriage or religion but is inherent in every individual. Thus, denying legal or social recognition to live-in relationships, or subjecting them to stigma, violates the equal protection guarantee under Article 14. The emphasis on *autonomy* as a constitutional value also implies that adults have the inherent right to choose how to organize their emotional and domestic lives without coercion from the State or society. This autonomy extends to decisions regarding companionship, sexual intimacy, and cohabitation—areas that form the essence of personal identity and fulfillment.

C. Constitutional Morality Over Social Morality

A crucial outcome of *Puttaswamy* was its reaffirmation of constitutional morality—the principle that the Constitution, not societal convention, must guide the interpretation of rights. This doctrine was later reinforced in *Navtej Singh Johar v. Union of India* (2018), which decriminalized same-sex relationships and emphasized that constitutional morality protects choices that may not conform to majoritarian norms. In the same vein, live-in relationships are protected not because society accepts them, but because the Constitution mandates respect for individual liberty and privacy. By prioritizing constitutional morality, the judiciary has provided a shield for consensual adult relationships from patriarchal, religious, and cultural intrusion.

D. From Privacy to Positive Protection

While *Puttaswamy* recognized privacy as a shield against arbitrary state action, it also laid the foundation for positive obligations—requiring the State to protect individuals from societal and structural violations of privacy. In the context of live-in relationships, this means ensuring legal protection from harassment, domestic violence, and discrimination. Statutes like the Protection of Women from Domestic Violence Act, 2005, which extend safeguards to relationships "in the nature of marriage," reflect this positive constitutional duty to protect rather than penalize alternative forms of companionship.

E. The Transformative Vision

Ultimately, *Puttaswamy* symbolizes the transformative character of the Indian Constitution. It marks a shift from collective morality to individual rights, from social conformity to personal choice. By recognizing privacy as an enabling condition for autonomy and dignity, the judgment provides the constitutional foundation for live-in relationships, same-sex partnerships, and other forms of non-traditional unions. In doing so, it reframes the Indian constitutional order as one that celebrates diversity in personal choices, grounding human relationships in liberty rather than legality.

A. Privacy as a Structural Right

Puttaswamy reconceived privacy as a cluster: bodily, spatial, communicational, informational, decisional. It rejected the "nothing to hide" fallacy, recognizing that surveillance chills liberty and rearranges power. Because surveillance is power-asymmetry in action, rule-of-law controls must be front-loaded (authorization) and back-loaded (oversight, remedies).

B. Proportionality and Narrow Tailoring

By constitutionalizing proportionality, Puttaswamy compels the State to prove that (i) surveillance serves a legitimate aim (e.g., national security); (ii) the chosen tool suitably furthers that aim; (iii) no less-restrictive alternative would achieve it; and (iv) rights costs are balanced by safeguards. Subsequent decisions (e.g., Anuradha Bhasin) applied proportionality to internet restrictions, insisting on reasoned, time-bound, reviewable measures.

C. Free Speech and Association

Surveillance indirectly constrains Article 19(1)(a) speech and 19(1)(c) association by producing anticipatory conformity. Where programs lack transparency, citizens cannot know or contest the scope or legality—eroding democratic accountability and press freedom.

India's Statutory Architecture: Legality vs. Legitimacy

While the *Puttaswamy* judgment transformed the constitutional understanding of privacy and autonomy, India's statutory framework on relationships and personal associations continues to lag behind this constitutional evolution. The legal recognition of companionship-based unions such as live-in relationships remains fragmented—acknowledged in limited contexts yet

lacking a coherent statutory foundation. The tension between **legality** (formal recognition under law) and **legitimacy** (social and moral acceptance) defines the current state of live-in relationships in India. The law oscillates between protecting individual autonomy and upholding traditional family structures, resulting in a framework that is protective in intent but inconsistent in practice.

A. Absence of a Codified Framework

India has no specific legislation governing live-in relationships. Unlike marriage, which is regulated through personal laws such as the Hindu Marriage Act, 1955, or the Special Marriage Act, 1954, live-in relationships exist in a legal vacuum. Their recognition has emerged primarily through judicial interpretation and selective statutory inclusion, particularly under the **Protection of Women from Domestic Violence Act, 2005 (PWDVA)**. The absence of a codified framework creates ambiguity around issues such as maintenance, inheritance, child legitimacy, and property rights. While courts have extended limited protections, the lack of legislative clarity continues to leave individuals—especially women—in precarious positions when such relationships dissolve or become abusive.

B. The PWDVA and "Relationships in the Nature of Marriage"

The PWDVA, enacted to protect women from domestic abuse, marked a turning point by recognizing non-marital relationships. Section 2(f) defines a "domestic relationship" to include associations "in the nature of marriage." Judicial interpretation of this phrase in *Indra Sarma v. V.K.V. Sarma* (2013) laid down essential criteria for identifying such relationships: duration of cohabitation, shared household, pooling of resources, sexual relationship, social representation, and intention to live as a couple. This acknowledgment provides women in live-in relationships access to remedies against violence, abandonment, and economic exploitation. However, the protection is contingent upon the relationship resembling marriage, implying that companionship-based unions are still validated through a marital lens, not as autonomous relationships in their own right.

C. Legitimacy of Children Born from Live-In Relationships

Judicial developments have progressively moved toward recognizing the rights of children born out of live-in relationships. In *Tulsa v. Durghatiya* (2008) and *Bharata Matha v. R. Vijaya Renganathan* (2010), the Supreme Court held that children from long-term live-in relationships should be considered legitimate under Section 16 of the Hindu Marriage Act. This approach aligns with constitutional principles of equality and

dignity, ensuring that the status of parents does not deprive children of legal rights. Yet, such recognition is indirect and derived from presumptions of marriage rather than explicit acknowledgment of alternative family structures.

D. Maintenance and Economic Protection

The question of maintenance in live-in relationships highlights the gap between constitutional ideals and statutory reality. Courts have occasionally extended maintenance rights under Section 125 of the Code of Criminal Procedure (CrPC), interpreting "wife" broadly to include women in stable live-in relationships. However, this remains a judicial innovation rather than a legislative guarantee. The reliance on discretionary interpretation means that economic security for women in such unions depends heavily on the facts of each case and the court's perception of the relationship's "marital character."

E. Social Legitimacy and Constitutional Morality

While the law cautiously expands protection, societal legitimacy remains contested. Traditional morality continues to stigmatize cohabitation outside marriage, framing it as a moral lapse rather than a constitutional choice. This creates a dual reality: relationships may be lawful under constitutional and statutory interpretation yet socially disapproved, subjecting individuals to harassment, eviction, or familial coercion. The judiciary, in cases such as *S. Khushboo v. Kanniammal* (2010), has emphasized that live-in relationships, though unconventional, do not constitute a criminal or immoral act. The Court observed that "not all relationships will amount to marriage, but such relationships cannot be regarded as illegal or immoral." Despite such pronouncements, law enforcement agencies and local authorities often act under the influence of social morality, undermining constitutional protections in practice.

F. The Legality–Legitimacy Paradox

The dissonance between legality and legitimacy reflects a deeper constitutional struggle—between a progressive judiciary that interprets autonomy as a constitutional value and a legislature hesitant to codify or endorse non-traditional relationships. This gap sustains uncertainty and reinforces social hierarchies. A rights-consistent framework must, therefore, go beyond reactive judicial protection and establish proactive statutory recognition that validates consensual partnerships as independent expressions of liberty and equality, not merely as imitations of marriage.

In conclusion, India's statutory architecture reveals an incomplete evolution. It recognizes live-in relationships indirectly through scattered provisions and judicial

creativity but stops short of granting them full legal status. Bridging this gap requires a legislative approach anchored in constitutional morality—one that affirms the legitimacy of all consensual adult relationships, upholds gender justice, and aligns the law with the transformative spirit of *Puttaswamy*.

A. Telegraph Act, 1885 & Telegraph Rules

Section 5(2) permits interception on specified grounds (public emergency, public safety) subject to procedural rules. In PUCL, the Court required recorded reasons, high-level authorization, and periodic review. These were important but executive-centric controls; they did not install independent judicial warrants or user notice, and predate digital metadata complexities.

B. IT Act, 2000 & Interception/Decryption Rules

The IT Act and its rules enable interception, monitoring, and decryption of digital communications and data flows. However, authorizations remain largely within the executive, with service-provider compliance built into licensing. The framework lacks ex ante judicial scrutiny, rigorous necessity showings, purpose limitation, or data-minimization mandates. Where bulk datasets (e.g., CDRs, tower dumps, platform logs) are touched, the law offers limited guidance on targeting vs. dragnet collection.

C. Facial Recognition & Emerging Tech

Facial recognition systems raise issues of accuracy, bias, and function creep. Without a specific statutory basis, independent audits, and impact assessments, deployments risk breaching proportionality (overbreadth, no least-restrictive measures) and equality (disparate error rates).

Jurisprudential Landmarks

1. People's Union for Civil Liberties (PUCL) v. Union of India (1997) — *Procedural Guardrails for Wiretapping*

This case remains the first constitutional checkpoint on surveillance in India. The Supreme Court held that telephone tapping under Section 5(2) of the Telegraph Act is a serious invasion of privacy and can only be justified under exceptional circumstances such as public emergency or public safety. The Court mandated procedural safeguards: prior written approval by the Home Secretary, recording of reasons, limited duration, periodic review, and destruction of intercepted material after use. However, these were

administrative rather than judicial safeguards, lacking the independence necessary for meaningful oversight.

2. **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) — *Privacy and Proportionality as Structural Principles***

   The nine-judge bench in *Puttaswamy* recognized privacy as intrinsic to life and liberty under Article 21, and foundational to dignity and autonomy. Importantly, it constitutionalized proportionality—requiring any limitation on privacy to satisfy four tests: legitimate aim, suitability, necessity (least restrictive means), and balancing. The judgment transformed privacy into a structural right, compelling all surveillance regimes to pass constitutional scrutiny. It also explicitly rejected the "nothing to hide" argument, observing that informational control is essential to freedom itself.

3. **K.S. Puttaswamy (Aadhaar) v. Union of India (2018–19) — *Purpose Limitation and Data-Governance Obligations***

   While upholding Aadhaar's limited use for welfare and taxation, the Court insisted on purpose limitation, data minimization, and storage restrictions. The dissenting opinions (Chandrachud, J.) warned against the creation of a surveillance state through centralized biometric databases. Even the majority emphasized that any data collection by the State must meet necessity and proportionality, laying the groundwork for future constitutional review of digital surveillance projects.

4. **Anuradha Bhasin v. Union of India (2020) — *Transparency, Publication, and Periodic Review***

   This case extended *Puttaswamy's* logic to information restrictions during the internet shutdown in Jammu & Kashmir. The Court required all orders to be published, subject to periodic review, and justified on proportionality grounds. The judgment underlined that indefinite or opaque restrictions fail constitutional tests—principles equally applicable to continuing surveillance operations.

5. **Manohar Lal Sharma v. Union of India (2021) — *The Pegasus Spyware Case: Judicial Oversight and Accountability***

   In response to allegations that the State used Pegasus spyware against journalists and activists, the Supreme Court affirmed that "national security cannot be a talisman to avoid judicial review." The Court appointed an independent technical committee supervised by a retired judge to examine the allegations. This marked the first explicit judicial recognition that opaque digital surveillance, absent independent oversight, undermines constitutional trust. The Court's insistence on accountability, even in

matters of security, reflects a maturing privacy jurisprudence.

6. **Internet Freedom Foundation v. Union of India (Pending/Indicative References) — *Facial Recognition and Emerging Technologies***

   Recent petitions challenge the unregulated deployment of facial-recognition systems by law-enforcement agencies. These cases invoke *Puttaswamy* and *Anuradha Bhasin* to argue that mass biometric surveillance violates proportionality and equality due to inherent bias and lack of statutory authorization. Though sub judice, they signal the judiciary's growing attention to algorithmic governance and the need for a legislative framework.

7. **Shreya Singhal v. Union of India (2015) — *Free Speech and Chilling Effects***

   Though not a surveillance case, *Shreya Singhal* struck down Section 66A of the IT Act for vagueness and chilling effects on free speech. The reasoning—requiring precision, foreseeability, and narrow tailoring—parallels the constitutional requirements for surveillance law. Together with *Puttaswamy*, it builds a jurisprudential bridge between speech rights (Art. 19) and informational privacy (Art. 21).

Doctrinal Synthesis

Across these cases, four principles crystallize:

1. **Legality —** Clear, accessible, and specific laws must authorize any surveillance measure (*PUCL*, *Anuradha Bhasin*).
2. **Proportionality —** Every restriction must satisfy necessity and least-restrictive means tests (*Puttaswamy*, *Aadhaar*).
3. **Accountability** — Executive discretion must be subject to independent and judicial oversight (*Pegasus*).
4. **Transparency & Review —** Citizens must have visibility, remedies, and periodic reassessment of restrictions (*Anuradha Bhasin*, *Shreya Singhal*).

Together, these judgments establish the constitutional blueprint for a rights-conform surveillance regime—anchored in privacy, proportionality, and democratic accountability. They move India toward what scholars call *"constitutional security"*: a model in which the legitimacy of security measures depends on their compliance with the rule of law and the protection of rights.

International Human Rights & Comparative Perspectives

A. International Human Rights Framework: ICCPR and UN Principles

Article 17 of the *International Covenant on Civil and Political Rights (ICCPR)* guarantees that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence." The UN Human Rights Committee, in General Comment No. 16 (1988) and subsequent observations, clarified that any interference must satisfy the tests of legality, necessity, and proportionality—requiring precise laws, legitimate aims, and safeguards against abuse.

The Committee has repeatedly emphasized that "arbitrary" interference includes actions that, even if lawful, are unreasonable or disproportionate in context. In its 2014 Concluding Observations on the United States and 2015 Observations on the United Kingdom, the Committee warned that bulk and indiscriminate data collection are inconsistent with Article 17 because they fail the test of strict necessity.

Complementing this, the UN General Assembly Resolution 68/167 (2013) on "The Right to Privacy in the Digital Age" reaffirmed that rights offline must also be protected online. The UN High Commissioner for Human Rights' 2014 Report and the "Necessary and Proportionate Principles" (2013)—endorsed by civil society and jurists worldwide—distilled twelve criteria for rights-respecting surveillance: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, user notice, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, and due process.

These principles have become a de facto interpretive benchmark for democratic states and are routinely cited in comparative privacy jurisprudence.

B. European Convention on Human Rights (ECHR) Jurisprudence

The European Court of Human Rights (ECtHR) has developed a sophisticated body of surveillance jurisprudence under Article 8 of the European Convention on Human Rights ("right to respect for private and family life, home and correspondence"). The Court has consistently held that secret surveillance is only compatible with Article 8 when it is:

1. In accordance with law (accessible, precise, foreseeable),
2. Pursuing a legitimate aim (national security, crime prevention, etc.), and
3. Necessary in a democratic society, meaning proportionate and accompanied

by effective supervision.

Key judgments include:

- **Klass and Others v. Germany (1978)** — upheld limited secret surveillance but required procedural guarantees and independent review to prevent abuse.
- **Weber and Saravia v. Germany (2006)** — held that strategic monitoring must be clearly circumscribed by law, with ex ante and ex post oversight.
- **Zakharov v. Russia (2015)** — found Russia's interception regime in violation of Article 8 for lack of judicial authorization and effective remedies, holding that even the existence of a surveillance framework can chill freedom.
- **Big Brother Watch and Others v. United Kingdom (2018/2021 Grand Chamber**) — ruled that bulk interception without sufficient safeguards on selection, search terms, and oversight violated Article 8 and Article 10 (freedom of expression). The Court affirmed that independent authorization and supervision are indispensable to prevent abuse in mass surveillance regimes.

Together, these decisions construct a rights-based architecture of surveillance control: clarity of law, independent authorization, proportionality, and redress mechanisms. They also underscore that metadata—though non-content—can reveal intimate personal patterns and therefore requires full privacy protection.

C. European Union Data Protection and Accountability Model

The EU General Data Protection Regulation (GDPR) and Charter of Fundamental Rights (Articles 7–8) operationalize privacy as both a negative liberty (freedom from arbitrary intrusion) and a positive right to informational self-determination. The GDPR codifies principles of *lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity/confidentiality, and accountability*.

In the surveillance context, the Court of Justice of the European Union (CJEU) has built a rigorous proportionality test through cases such as:

- Digital Rights Ireland (2014) — struck down blanket data retention as disproportionate.
- Tele2 Sverige AB v. Post- och telestyrelsen (2016) — prohibited general and indiscriminate retention of communications metadata.
- La Quadrature du Net v. France (2020) — reaffirmed that national security cannot justify indefinite or indiscriminate surveillance.

These decisions crystallize the EU approach: bulk collection violates the essence of privacy unless accompanied by judicial warrants, targeted scope, strict temporal limits, independent oversight, and effective remedies.

D. Comparative Common-Law Jurisdictions

1. **United Kingdom – Investigatory Powers Act (2016):**
   After the *Big Brother Watch* litigation, the UK enacted the Investigatory Powers Act, introducing *judicial commissioners* for ex ante approval of surveillance warrants (a "double-lock" mechanism). Although still criticized for bulk powers, it represents progress toward balancing secrecy with accountability.
2. **United States – Fourth Amendment and FISA Framework:**
   The U.S. Supreme Court's decision in *Carpenter v. United States (2018)* recognized that long-term cell-site location data collection constitutes a search requiring a warrant. While national security surveillance under the Foreign Intelligence Surveillance Act (FISA) remains opaque, post-Snowden reforms such as the *USA Freedom Act (2015)* limited bulk metadata collection and enhanced judicial review by the FISA Court.
3. **South Africa – AmaBhungane Centre for Investigative Journalism v. Minister of Justice (2021):**
   The Constitutional Court struck down portions of South Africa's interception law for lack of judicial oversight, absence of post-surveillance notice, and inadequate protection of journalists' sources. The Court mandated judicial warrants, independent oversight, and notification mechanisms—closely aligning with *Puttaswamy*'s proportionality standard and ICCPR principles.

E. Synthesis: Converging Standards

Across international and comparative practice, certain minimum guarantees emerge as essential to a rights-consistent surveillance regime:

1. Legality: Clear, precise statutory basis accessible to the public.
2. Legitimate Aim: Restriction only for narrowly defined purposes such as national security or public safety.
3. Necessity and Proportionality: Demonstrated least-restrictive means, subject to judicial review.

4. Independent Authorization and Oversight: Neutral judicial or quasi-judicial body with review powers.
5. Transparency and Accountability: Periodic public reporting, post-surveillance notification, and accessible remedies.

These standards collectively affirm that privacy is not a barrier to national security but its constitutional precondition. Comparative experience shows that democratic security is sustainable only when surveillance powers are exercised within a framework of legality, necessity, proportionality, and accountability—the very principles embedded in India's post-*Puttaswamy* constitutional order.

Anticipating Counter-Arguments

"Security requires secrecy."

Yes—but secrecy can coexist with ex ante judicial control, independent audits, and aggregate transparency. Security is not undermined by process discipline; it is strengthened by legitimacy.

"Judicial warrants slow operations."

Emergency carve-outs with after-the-fact judicial review and on-call duty judges address urgency without eroding rights.

"Metadata is harmless."

Modern analytics make metadata deeply revealing (social graphs, movement patterns, associations). Treat it as rights-sensitive data.

Conclusion

After Puttaswamy, the constitutional question is no longer whether India may surveil, but how it may do so. A security state governed by opaque executive orders is neither constitutionally secure nor democratically stable. Embedding judicial warrants, independent oversight, strict necessity, data-minimization, transparency, and redress would align India's surveillance practice with Articles 14, 19, and 21 and ICCPR norms, reducing rights costs while preserving operational effectiveness. The genuine measure of national security is not unreviewable power, but accountable power.