*Page: 324-338* *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

# LawFoyer International Journal of Doctrinal Legal Research

**[ISSN: 2583-7753]**

**Volume 4 | Issue 1**

**2026**

*DOI: https://doi.org/10.70183/lijdlr.2026.v04.15*

# CYBER SECURITY LAWS AND ROLE OF JUDICIARY IN PROTECTING PRIVACY RIGHTS IN INDIA

**Arpit Tripathi**[1]

## I. ABSTRACT

*The rapid digitisation of India's socio-economic framework has intensified concerns regarding cybersecurity and the protection of privacy rights. Recognised as a fundamental right under Article 21 of the Constitution, the right to privacy attained definitive constitutional status through the Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). This judgment not only affirmed privacy as intrinsic to human dignity and personal liberty but also established the principles of legality, necessity, and proportionality to assess state intrusion. India's cybersecurity regime is primarily governed by the Information Technology Act, 2000, and strengthened by the Digital Personal Data Protection Act, 2023. While the IT Act addresses cyber offences such as hacking, identity theft, and unauthorised access, the DPDP Act introduces a structured framework regulating data collection, processing, storage, and consent-based governance. Together, these statutes seek to ensure accountability of data fiduciaries and enhance digital security. The judiciary continues to play a pivotal role in balancing individual privacy with competing state interests, including national security and public order. Through constitutional interpretation and judicial review, courts have imposed procedural safeguards on surveillance mechanisms and reinforced limitations on arbitrary state action. This paper critically examines the evolving interplay between legislative measures and judicial oversight in shaping India's digital privacy landscape, highlighting the need for robust enforcement and rights-oriented governance in the era of expanding digital infrastructure.*

## II. KEYWORDS

Cybersecurity, Right to Privacy, Article 21, Digital Personal Data Protection Act 2023, Judicial Review

[1] LLM student at DSNLU Visakhapatnam (India). Email: arpittripathi45025@gmail.com

 (ISSN: 2583-7753)

# III. INTRODUCTION

The exponential growth of digital technologies, internet penetration, and data-driven governance has transformed India's socio-economic structure, simultaneously intensifying concerns regarding cybersecurity and informational privacy. The proliferation of cyber threats such as identity theft, hacking, data breaches, and online fraud necessitates a robust and coherent legal framework. India's primary legislative response is embodied in the Information Technology Act 2000, No 21 of 2000 (OSCOLA), along with its subsequent amendments, which regulate electronic governance, cyber offences, and data protection obligations.

Parallel to legislative developments, the Indian judiciary has played a transformative role in recognising and strengthening privacy as an intrinsic component of Article 21 of the Constitution. The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) affirmed privacy as a fundamental right and established constitutional standards for evaluating state interference.

## A. Research Problem

Despite constitutional recognition of privacy and the enactment of statutory safeguards, concerns persist regarding surveillance practices, enforcement gaps, and the adequacy of institutional mechanisms to protect digital privacy in India. The central problem lies in assessing whether the existing cyber security framework sufficiently aligns with constitutional mandates.

## B. Research Objectives

1. To examine the evolution of cybersecurity laws in India.
2. To analyse the judicial expansion of privacy rights under Article 21.
3. To evaluate the effectiveness of the Digital Personal Data Protection Act, 2023 in operationalising constitutional privacy.
4. To assess the balance between national security imperatives and individual privacy rights.

### C. Research Questions

1. How has judicial interpretation shaped the right to privacy in India's digital era?
2. Does the current cybersecurity framework adequately safeguard constitutional privacy guarantees?
3. What challenges persist in enforcement and regulatory oversight?

### D. Research Hypotheses

1. The judiciary has been instrumental in transforming privacy into a substantive constitutional guarantee in India.
2. While recent legislative reforms strengthen data governance, structural and enforcement limitations continue to undermine effective privacy protection.

### E. Research Methodology

This study adopts a doctrinal research methodology, relying primarily on secondary sources. Data has been collected from constitutional provisions, statutes such as the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023, landmark Supreme Court judgments, government reports, and scholarly articles. The research employs analytical and comparative methods to evaluate statutory provisions against constitutional principles, particularly the proportionality standard evolved in privacy jurisprudence.

### F. Literature Review

The evolution of privacy jurisprudence in India has generated substantial academic discourse, particularly following the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). Gautam Bhatia, in *The Transformative Constitution*, argues that the Puttaswamy judgment constitutionalised dignity and autonomy, embedding privacy within a broader rights-based framework.[2] Similarly,

[2] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins 2019).

Apar Gupta has analysed the proportionality doctrine emerging from Puttaswamy as a structural limitation on executive surveillance powers.[3]

Scholars such as Usha Ramanathan have critically examined the Aadhaar project, contending that mass data collection frameworks risk normalising state surveillance absent strong procedural safeguards.[4] Chinmayi Arun has further highlighted how surveillance technologies disproportionately affect vulnerable populations, thereby implicating equality concerns under Article 14.[5]

On the statutory front, comparative analyses of India's data protection regime have drawn parallels with the European Union's General Data Protection Regulation (GDPR). Graham Greenleaf notes that while India's Digital Personal Data Protection Act, 2023 reflects global data protection principles such as consent and accountability, it diverges significantly in terms of state exemptions and regulatory independence.[6] Likewise, Kamlesh Bajaj and Debjani Ghosh have examined India's cybersecurity framework under the Information Technology Act 2000, identifying fragmentation and enforcement challenges.[7]

International scholarship also contextualises cybersecurity within broader human rights paradigms. David Kaye underscores the tension between national security surveillance and freedom of expression under international law.[8] Comparative constitutional analyses by Orin S. Kerr on digital searches and privacy in the United States provide instructive insights into judicial adaptation to technological change.[9]

Despite these contributions, existing literature reveals notable gaps. First, while doctrinal analyses of Puttaswamy are extensive, fewer studies critically assess the operational effectiveness of the Digital Personal Data Protection Act, 2023 in light of constitutional standards. Second, scholarship often treats cybersecurity and privacy

[3] Apar Gupta, 'Privacy and the Proportionality Doctrine after Puttaswamy' (2018) 10 NUJS L Rev 1.
[4] Usha Ramanathan, 'Aadhaar: From Welfare to Surveillance' (2014) 49(50) Econ & Pol Wkly 33.
[5] Chinmayi Arun, 'Privacy and the Public Interest in the Digital Age' (2019) 12 Indian J L & Tech 45.
[6] Graham Greenleaf, 'India's Data Protection Act 2023: Global Convergence and National Divergence' (2023) 169 Privacy Laws & Business Int'l Report 1.
[7] Kamlesh Bajaj and Debjani Ghosh, 'Cyber Security and Data Protection in India' (Data Security Council of India Report 2020).
[8] David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019).
[9] Orin S Kerr, 'A Theory of Fourth Amendment Protection' (2001) 60 Stan L Rev 503.

as distinct domains, overlooking their structural interdependence. Third, limited attention has been paid to enforcement architecture and institutional independence in India's emerging data protection regime.

This study seeks to bridge these gaps by integrating constitutional analysis, statutory evaluation, and governance-based critique to assess whether India's cybersecurity framework adequately operationalises the fundamental right to privacy in the digital era.

## IV. LEGAL FRAMEWORK IN INDIA

India's cybersecurity and privacy safeguards are based on a complex legal system that includes numerous laws, regulations, and court rulings that work together to handle the changing issues of data security and cyber threats.

The main piece of legislation controlling cybersecurity in India is the Information Technology Act, 2000 (IT Act). It publishes clauses pertaining to digital signatures and electronic governance and defines cybercrimes such hacking, data theft, and identity theft. In order to strengthen the legal framework and impose harsher punishments for cybercrimes, the IT Act was amended, most notably in 2008. It also gives the government the power to establish regulations pertaining to private information that should be protected by organisations that handle it.

The Digital Personal Data Protection Act, 2023, which is a major step toward formalizing privacy rights in India, complements the IT Act. This law emphasizes people's rights to consent, access, correct, and erase their personal data while introducing extensive guidelines on data collection, processing, storage, and sharing. It creates regulatory bodies to monitor adherence to established standards, look into violations, and penalize data custodians who do not.

Regulations issued by the Reserve Bank of India (RBI) for the banking industry, guidelines from the Securities and Exchange Board of India (SEBI) regarding information security and data privacy, and directives from the Telecom Regulatory Authority of India (TRAI) are examples of sector-specific regulations that also support cybersecurity governance.

The Indian Penal Code (IPC), which punishes crimes including criminal intimidation, defamation, and forgery when they are committed online, also interacts with cyber laws.

In order to improve privacy protections, the judiciary has been crucial in interpreting these laws. After the Supreme Court's historic ruling in K. S. Puttaswamy case, the right to privacy was deemed a basic constitutional right, necessitating judicial monitoring and legislative changes to improve online privacy protections.

The National Cyber Security Policy, 2013, offers a governmental framework for safeguarding vital information infrastructure, raising awareness of cyber threats, and enhancing institutional capability in addition to legislation.

## V. EVOLVING PRIVACY JURISPRUDENCE IN INDIA'S DIGITAL ERA

India's constitutional framework on privacy has experienced a significant shift, largely due to the interpretation of Article 21 and the passage of the Digital Personal Data Protection Act, 2023. The right to privacy was not originally included in the Constitution; nonetheless, it was brought about by vigorous judicial activism, in which judges imaginatively construed Article 21's "right to life and personal liberty" to encompass privacy as a fundamental, unalienable aspect of human dignity. Beginning with early precedents such as Kharak Singh and Govind, the right to privacy gained definitive status in the Supreme Court's unanimous declaration of privacy as a basic right under Article 21 in the historic case of Justice K.S. Puttaswamy v. Union of India (2017).

As a result, judicial activism in India has played a crucial role in the development of privacy protection, forcing the legislation to adjust to the new digital landscape. In order to maintain a balance between the rights of individuals and the interests of the state, courts have determined that any invasion of privacy must pass the legality, necessity, and proportionality tests. The Digital Personal Data Protection Act, 2023, India's first comprehensive data protection law, was founded on these ideas. By granting people explicit control over their data, requiring consent and transparency,

and placing obligations on organizations that handle personal data, the Act operationalizes constitutional privacy.

In essence, the journey from Article 21 to the Digital Personal Data Protection Act showcases how judicial activism has dynamically reshaped Indian privacy jurisprudence for the digital era, reaffirming the judiciary's role as a constitutional guardian and paving the way for robust data protection in cyberspace.

## VI. JUDICIAL EXPANSION OF PRIVACY RIGHTS: KEY SUPREME COURT CASES

The right to privacy in India has evolved from being a moral claim to a constitutional guarantee under Article 21. Initially seen as the "right to be let alone," it later expanded to protect citizens from arbitrary state surveillance through procedural safeguards. The Supreme Court ultimately recognized privacy as a fundamental right essential to dignity, autonomy, and informational control. This judicial evolution laid the foundation for the Digital Personal Data Protection Act, 2023, which transformed constitutional principles into concrete statutory protection in the digital era.. Collectively, these instances serve as the cornerstone of India's contemporary privacy framework under the constitution, especially in light of the growing scope of digital governance and monitoring:

### A. R. Rajagopal v. State of Tamil Nadu[10]

In *R. Rajagopal & Ors. v. State of Tamil Nadu & Ors.*, (1994) 6 S.C.C. 632, the Supreme Court explicitly recognised the right to privacy as implicit in Article 21 of the Constitution. Popularly known as the "Auto Shankar case," the dispute arose when prison authorities sought to restrain the publication of the autobiography of a condemned prisoner. The Court held that the right to privacy encompasses the "right to be let alone," protecting individuals against unauthorised publication of personal matters relating to family, marriage, procreation, and education.

Significantly, the judgment advanced privacy jurisprudence beyond mere recognition by delineating the constitutional balance between privacy and freedom of the press

[10] (1994) 6 S.C.C. 632 (India)

under Article 19(1)(a). The Court ruled that public officials cannot claim privacy in respect of acts performed in their official capacity, thereby strengthening democratic accountability. At the same time, it rejected prior restraint by the State in the absence of compelling reasons, holding that the government could not impose pre-publication censorship unless justified by law. The decision thus established a structured approach to reconciling press freedom with individual privacy, laying an early doctrinal foundation for later constitutional privacy jurisprudence.

### B. PUCL v. Union of India[11]

In *People's Union for Civil Liberties v. Union of India*, (1997) 1 S.C.C. 301; AIR 1997 SC 568, the Supreme Court examined the constitutional validity of telephone interception under section 5(2) of the Indian Telegraph Act 1885.[12] The Court held that telephone tapping constitutes a serious invasion of privacy under Article 21 and must therefore be subject to strict procedural safeguards.

To prevent arbitrary surveillance, the Court prescribed detailed guidelines: (i) interception orders may be issued only by the Union or State Home Secretary; (ii) such orders must record reasons and satisfy the necessity requirement under section 5(2); (iii) interception shall remain valid for two months, extendable up to a maximum of six months; and (iv) a Review Committee comprising the Cabinet Secretary, Law Secretary, and Secretary for Telecommunications (at the Union level) must periodically examine the legality of such orders. These safeguards marked a decisive shift toward procedural constitutionalism, ensuring executive accountability while recognising legitimate security concerns.

### C. Justice K.S. Puttaswamy v. Union of India[13]

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, a nine-judge Bench unanimously affirmed that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The Court conceptualised privacy as intrinsic to dignity, autonomy, and informational self-determination, thereby

[11] (1997) AIR SC 568, 1 S.C.C. 301 (India)
[12] Indian Telegraph Act 1885, s 5(2).
[13] (2017) 10 S.C.C. 1 (India).

situating it within the broader framework of equality, freedom, and life and personal liberty.

The judgment articulated a structured proportionality test requiring that any restriction on privacy must satisfy legality, legitimate state aim, necessity, and proportionality, coupled with procedural safeguards against abuse. Importantly, the Court expressly overruled earlier precedents in *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300[14], and *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295[15], to the extent that they denied constitutional recognition of privacy. By grounding privacy across multiple fundamental rights provisions, the Court entrenched it within India's constitutional architecture and provided the normative basis for subsequent data protection legislation.

Together, these rulings show how advanced the judiciary is in its interpretive activism. Through the expansion of the definition of "personal liberty" under Article 21, the Court has protected people from private and governmental incursions into cyberspace. The Digital Personal Data Protection Act 2023, which converted judicial thought into legislation protection, was made possible by this developing body of precedent. Thus, in India's constitutional democracy, the trilogy illustrates the transition from tacit judicial acknowledgment to explicit legal codification of digital privacy.

## VII. CHALLENGES IN PRIVACY PROTECTION: SURVEILLANCE, ENFORCEMENT, AND TRANSNATIONAL CYBERCRIME

Even with the passage of the Digital Personal Data Protection Act (DPDP Act), 2023, and the constitutional recognition of privacy as a fundamental right under Article 21, India's digital privacy environment still faces major obstacles that compromise the efficacy of its legal system. Unchecked mass monitoring, lax enforcement, and the complexity of multinational cybercrime are three crucial areas that require immediate attention.

[14] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[15] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

India's surveillance architecture has evolved from targeted interception to expansive mass surveillance systems that pose serious threats to constitutional privacy guarantees. Without strong monitoring procedures, technologies like the Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and Lawful Intercept and Monitoring System (LIMS) give government organizations direct, real-time access to citizens' private emails, social media, and conversations. The Information Technology Act's Sections 69 and 69B give the government broad authority to monitor, intercept, and decrypt data on the basis of widely defined justifications such as "public order" and "sovereignty," without the need for judicial review. According to Meta's (Facebook) Transparency Report (January–June 2019), India submitted 49,382 requests for user data, one of the highest globally during that reporting period, thereby illustrating the scale of state access to digital communications.[16] While such requests may be grounded in legitimate law enforcement objectives, their volume underscores the importance of robust procedural safeguards consistent with constitutional proportionality standards laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017).

Concerns regarding governmental exemptions under the Digital Personal Data Protection Act, 2023 (DPDP Act) further complicate the privacy landscape. Section 17 of the DPDP Act[17] (which empowers the Central Government to exempt certain state instrumentalities from the Act's provisions on grounds such as sovereignty, integrity, and security of the State) has attracted criticism for potentially diluting accountability mechanisms. Broadly framed exemptions, particularly in the absence of independent prior judicial review, risk creating asymmetry between citizen obligations and state responsibility.

Institutional design concerns also arise in relation to the Data Protection Board of India. Section 27(3) of the DPDP Act[18] (which authorises the Central Government to issue directions binding on the Board) has been questioned for undermining

[16] Meta Platforms Inc., *Government Requests for User Data – India (Jan–Jun 2019)*, Facebook Transparency Report (2019) https://transparency.fb.com accessed 10 February 2026.
[17] Digital Personal Data Protection Act 2023, s 17.
[18] Digital Personal Data Protection Act 2023, s 27(3).

adjudicatory independence. Civil society analyses, including commentary by the Internet Freedom Foundation and the Centre for Communication Governance (NLU Delhi), argue that executive control over appointment, tenure, and operational directives may compromise regulatory autonomy and weaken enforcement credibility[19]. Such structural limitations may impede effective redress against state and private-sector data breaches, thereby affecting the overall integrity of India's privacy protection framework.

## VIII. WEAK ENFORCEMENT ARCHITECTURE

The Data Protection Board of India (DPB), which is the centralized enforcement mechanism under the DPDP Act, has serious enforcement deficiencies due to basic design problems. Because Section 27(3)[20] gives the Central Government the authority to change or revoke the Board's directives, the DPB lacks institutional independence, and the executive branch is essentially permitted to meddle in adjudication decisions. By allowing the government to have an impact on cases involving state entities, this goes against the natural justice concept and makes it very impossible to hold government agencies responsible for data breaches. A single Delhi-based body that is in charge of enforcement for 1.4 billion people is unable to adequately handle millions of complaints, especially from rural areas, which is another practical drawback of the centralized arrangement. As a result, there is an "enforcement imbalance" where many infractions and smaller organizations go unnoticed.

Together, these interrelated issues weak institutional enforcement capacity, transnational jurisdictional gaps, and mass monitoring that circumvents constitutional protections undermine India's internet privacy protection regime. Structural reforms are needed to address these, such as the creation of independent oversight mechanisms, the decentralization of enforcement architecture, the reinforcement of frameworks for international cooperation, and the alignment of

[19] Internet Freedom Foundation, 'Analysis of the Digital Personal Data Protection Act 2023' (Policy Brief, 2023); Centre for Communication Governance, National Law University Delhi, 'Comments on the DPDP Bill and Regulatory Design' (2023).
[20] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Aug. 11, 2023, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

domestic laws with international best practices while upholding constitutional privacy principles.

## IX. THE ROAD AHEAD: LEGISLATIVE IMPERATIVES AND JUDICIAL VIGILANCE IN CYBER SECURITY GOVERNANCE

India's path to strong cyber security governance must balance constitutional principles especially the basic right to privacy guaranteed by Article 21 with technological protections. The future of digital ecosystems depends on extensive legislative changes, improved judicial supervision, and the implementation of human rights-based governance structures that strike a compromise between personal liberties and security requirements.

### A. Legislative Imperatives for Constitutional Alignment

The proportionality test, which was outlined in Puttaswamy judgement and requires that any privacy-infringing measure meet the conjunctive requirements of legality, legitimate goal, suitability, necessity, proportionality, and procedural safeguards, is desperately needed in India. The necessity requirement may be broken by current surveillance laws, especially Sections 69 and 69B of the Information Technology Act 2000[21], which permit interception on the basis of vague justifications like "public order" and "expediency" without making a distinction between proportionate responses to varying threat levels.

In order to ensure minimal rights encroachment, legislative measures must limit the term of "state security" and require that surveillance be permitted only for major acts. The Digital Personal Data Protection Act of 2023 calls for changes to restrict broad government exemptions under Section 17, which permits data processing for ill-defined "state functions" without consent. It is essential to establish an independent Data Protection Board that is shielded from executive intervention by Section 27(3). The current provisions that permit the Central Government to alter Board orders are

[21] Information Technology Act, 2000, No. 21 of 2000, Gazette of India (2000), https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077.

in violation of natural justice principles and compromise state organizations' accountability.

In order to empower citizens and comply with international norms, India should implement user-centric rights such as data erasure, portability, and meaningful consent processes, taking inspiration from the EU's General Data Protection Regulation (GDPR).

Additionally, addressing transnational cybercrime requires legislative clarity on extraterritorial jurisdiction and consideration of international cooperation frameworks, potentially including accession to the Budapest Convention on Cybercrime to facilitate cross-border evidence collection and harmonize investigative procedures.

**B. Strengthening Judicial Oversight Mechanisms**

To guarantee constitutional conformity, the judiciary must take on a more watchful role in examining surveillance and data protection practices. Pre-Puttaswamy rulings, such as in PUCL v/s UOI[22] , accepted executive monitoring through Review Committees made up of top government officials but refused to require judicial consent for telephone eavesdropping. But in the wake of Puttaswamy, the proportionality test's necessary limb requires that fewer rights-restrictive options be taken into account. One such option that strengthens legitimacy while limiting executive overreach is independent judicial authority.

The creation of technical, specialist data protection tribunals can provide informed adjudication and speed up privacy-related litigation. In order to overcome the current opacity where the government denies Right to Information requests on surveillance statistics, the judge should impose transparency reporting standards for surveillance programs. These requirements should include periodic disclosure of interception orders granted, their rationale, and their results.

[22] 1997 AIR SC 568, 1 S.C.C. 301 (India)

### C. Human Rights-Centered Digital Governance

Transparency, accountability, and individual empowerment must be prioritized while integrating international norms into national frameworks in order to implement a human rights-based approach to cyber security. In order to ensure that digital governance upholds freedom of expression, association, and privacy in online settings, India should align its cyber security policies with the UN Guiding Principles on Business and Human Rights, the International Covenant on Civil and Political Rights, and the Universal Declaration of Human Rights. Government, civil society, the commercial sector, and technical specialists are all involved in multi-stakeholder governance models, which promote inclusive policymaking that prevents concentrated authority and balances a range of interests[23].

## X. CONCLUSION

Through persistent judicial activism, India's privacy jurisprudence has undergone a significant constitutional transition, culminating in Puttaswamy verdict, which acknowledged privacy as a basic right under Article 21. The Supreme Court established privacy as essential to human dignity and individual liberty, building on seminal rulings such as in the cases , R. Rajagopal and PUCL. It also introduced the proportionality test, which mandates that any privacy restriction be legal, necessary, and minimally intrusive.

Significant obstacles still exist, nevertheless, even after the Digital Personal Data Protection Act of 2023 was passed. Accountability is compromised by widespread government exemptions and lax enforcement measures, and mass surveillance technologies function without strong monitoring. The way forward necessitates establishing independent oversight organisations, implementing human rights-centered governance frameworks, and harmonising cyber security laws with constitutional values through extensive surveillance reform. India can only achieve a cyber security regime that upholds fundamental rights while addressing justifiable

[23] Juris Centre, Cybersecurity and Human Rights, Juris Centre (July 29, 2024), https://juriscentre.com/2024/07/29/cybersecurity-and-human-rights/

security concerns and fulfils the constitutional promise of online privacy through persistent judicial monitoring and legislative reform.

## XI. REFERENCES


### A. Cases

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 S.C.C. 1 (India).
2. People's Union for Civil Liberties v. Union of India, 1997 AIR SC 568, 1 S.C.C. 301 (India).
3. R. Rajagopal & Ors. v. State of Tamil Nadu & Ors., (1994) 6 S.C.C. 632 (India).

### B. Statutes & Acts

1. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Aug. 11, 2023, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
2. Information Technology Act, 2000, No. 21 of 2000, Gazette of India (2000), https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077.

### C. Reports & Articles

1. Jhalak M. Kakkar et al., *The Surveillance Law Landscape in India and the Impact of Puttaswamy* (Centre for Communication Governance at National Law University Delhi, June 15, 2023), https://globalnetworkinitiative.org/wp-content/uploads/2023/07/CCG-June-15.pdf.
2. Juris Centre, *Cybersecurity and Human Rights*, Juris Centre (July 29, 2024), https://juriscentre.com/2024/07/29/cybersecurity-and-human-rights/.