The Role of Privacy as Human Dignity: Constitutional Interpretation of Data Protection Rights in India's Digital Democracy

Mrs M Razia Begum[1], Dr. Md Adil [2]

[1]Assistant Professor in Law, Osmania University, Hyderabad.

[2]Associate professor, MSS Law College

DOI: 10.64823/ijter.2606002

© ***2026 The Author(s).*** Published by ***Ambesys Publications***. This is an open-access article distributed under the terms of **Creative Commons Attribution License (CC BY 4.0)** (https://creativecommons.org/licenses/by/4.0/)

Abstract**:** The notion of privacy being the foundation of human dignity marks a revolutionary development in the constitutional architecture of India's digital democracy. It is a manifestation of the profound philosophic recognition that the core of one's personality lies in his or her mind, that is, his or her choice, intimacy, and data. In the present age, where data is often referred to as the "new oil" fueling progress and governance, the legal system finds itself faced with the challenge of reconciling the efficacy of the data-driven state with the sacredness of the individual. This paper gives a comprehensive overview of the philosophic, judicial, and legislative foundations that underpin the right to privacy in India. Along with that, this paper proposes a probable roadmap to alleviate the stricter implementation of the laws in the DPDP Act, in the backdrop of the protection of digital privacy of the citizens in India.

Keywords: security, privacy , dignity, protection, technology

I. INTRODUCTION

The right to privacy was not a new legal discovery, but a codification of an old instinct of man that is as old as the desire to have a private sphere in which he could live his life in a dignified way. This instinct has been expressed in the sacred personal space of temples; it is also reflected in the common law concept of the home as a "castle", a place where the entry of others from outside was construed not only as a trespass of property, but an intrusion upon the person. Discussions of this area, as part of the philosophical tradition, have been linked to that of natural law, of John Locke and Immanuel Kant. Locke's ideas of "property in the person" gave the basic terminology to describe the claims made when the Person is being violated, like when personal information is being violated, it is part of the Person.

In contrast, Kant's moral philosophy provides a deeper basis for privacy as dignity by stating the categorical imperative, that is, the absolute moral obligation to treat each person as an end and never as a means. When a person's data is mined, analysed and monetised without their permission, this constitutes the act of treating a person as a means, a consumable or a data point for predictive modelling, as opposed to a sovereign person with inherent value. This disregard of the moral value of personhood is a dignitary harm, not a financial loss

or reputation loss. Spying on another's private life, or revealing intimacies to public view without a person's permission is basically a violation of the equal moral value that forms the essence of personhood.

In the 20th century other writers, such as Edward Bloustein, elaborated further on the "Dignity Dimension" of privacy, identifying a common underlying wrong in all invasions of privacy as "the deprivation of human dignity and individuality". Bloustein's argument came in reaction to earlier perspectives that privacy was the sum of separate concerns, such as one's reputation and emotional peace. Rather, he suggested that the principal interest in question is the "interest in one's own personhood. That is in keeping with the seminal 1890 case of Samuel Warren and Louis Brandeis, which established the right to be let alone as a form of privacy, and protection of the inviolate personality.

With the advent of the digital age, Julie Cohen has reworked these perspectives, asserting that privacy is necessary for "sheltering dynamic, emergent subjectivity". In a society where everything is shaped socially and is subject to predictive analysis, Cohen argues that privacy is the “breathing room” that allows people to think critically and experiment on their own without being "fixed, transparent, and predictable" by the state or other commercial entities. So it is not only a matter of seclusion, but also of "boundary management," the process by which the ability to self-determine is built.

Privacy involves the ability to control personal data, and the ability to exercise this control is an essential aspect of selfhood. When people share intimate details, they entrust others and create a bond. Privacy guarantees the satisfaction of dignity and is thus the essential principle that the right to life and liberty seeks to realize. It appears that privacy underpins freedom and acts as its "necessary condition precedent.”

II. Significance

This study is highly significant as it addresses a revolutionary development in India's constitutional architecture: the recognition of privacy as the bedrock of human dignity within a digital democracy. In an era where data is hailed as the "new oil" driving state governance and progress, this research explores the critical tension between data-driven state efficacy and individual sacredness.

Why This Research Matters:

Dignitary Harm vs. Financial Loss: It shifts the understanding of privacy violations from mere financial or reputational risks to profound "dignitary harms" that infringe upon the core of human personhood.

Constitutional Integrity: It contextualizes privacy within the Preamble's promise of "Fraternity assuring the dignity of the individual," elevating privacy from an elitist concern to a fundamental value necessary for a humane social order.

Legislative and Technological Critique: By evaluating the landmark Puttaswamy judgments alongside the Digital Personal Data Protection (DPDP) Act, 2023 and the Draft 2025 Rules, this study exposes critical regulatory gaps. It highlights how unchecked technologies like Facial Recognition Technology (FRT), AI biases, and sweeping state exemptions risk facilitating an "Orwellian state" or a "surveillance society".

III. Scope Of The Study

The scope of this study encompasses the philosophical, judicial, and legislative dimensions of data privacy rights in India. Specifically, the boundaries of this research include:

Philosophical Foundations: An examination of privacy through the lenses of natural law, John Locke's "property in the person," Immanuel Kant's categorical imperative, and 20th-century legal theories regarding personhood.

Judicial Evolution: A review of Indian privacy jurisprudence tracing back from early restrictive rulings (M.P. Sharma and Kharak Singh) to the expansion of Article 21 (Maneka Gandhi), culminating in the historic 2017 Puttaswamy judgment and the 2018 Aadhaar challenge (Puttaswamy II).

Legislative Analysis: An evaluation of the DPDP Act, 2023 and the Draft DPDP Rules of 2025, focusing on the roles of Data Principals, Data Fiduciaries, and Consent Managers.

IV. Aims And Objectives

Aims

The primary aim of this paper is to provide a comprehensive analysis of the evolution of the right to privacy as an essential facet of human dignity in India's digital democracy, and to propose a strategic roadmap to ensure stricter, dignity-centric implementation of data protection laws.

Objectives:
To analyze the philosophical underpinnings of privacy as an absolute moral obligation and a prerequisite for human individuality and self-determination.
To trace the jurisprudential shift of the Supreme Court of India from a rigid, "compartmentalized" view of fundamental rights to the absolute recognition of privacy under Article 21.

- To evaluate the structural forms of privacy, specifically informational, spatial, and decisional privacy, established by the watershed Puttaswamy judgment.
- To dissect the regulatory framework of the DPDP Act, 2023 and its 2025 Rules, identifying the shifting power dynamics, duties, and liabilities imposed on Data Principals and Data Fiduciaries.
- To critique potential areas of state overreach, such as the "oversight vacuum" created by blanket government exemptions under Section 17, and the absence of consumer restitution or compensation for privacy breaches.

V. Hypothesis

While India's constitutional jurisprudence implicitly safeguards mental privacy, the current statutory framework, specifically the DPDP Act, 2023, is fundamentally unequipped to regulate neuro-data. Without a dedicated, neuro-specific legal regime and an explicit constitutional amendment for cognitive liberty, citizens remain highly vulnerable to commercial exploitation and invasive State surveillance.

VI. Research Methodology

This study adopts a qualitative doctrinal research approach, focusing on the analysis of legal, strategic, and policy-oriented materials related to DPDP Act

Primary Sources:
Government reports, policy documents (such as national quantum missions), defence white papers, and official publications related to India's strategic and technological initiatives.

Secondary Sources:
Scholarly articles, research papers, books, think-tank reports, and expert analyses on quantum technologies and their defence applications.
The methodology aims to provide a critical and analytical understanding of the strategic, legal, and policy dimensions of cybersecurity, offering both descriptive insights and normative recommendations.

Constitutional Architecture and the Preamble

The word "dignity" is explicitly mentioned in the Preamble of the Indian Constitution which aims to foster "Fraternity assuring the dignity of the individual and the unity and integrity of the Nation". This is the significance of the textual placement of the Preamble; under the Basic Structure Doctrine laid down by Kesavananda Bharati, the Preamble is a part of the core of the Constitution and is to be interpreted in terms of the other provisions. The Preamble is the "Identity Card of the Constitution" and it is the essence of the democratic ethos of the nation and the basic principles of Justice, Liberty and Equality.
The meaning of "Dignity" in the Preamble is moral and spiritual with an implication that the Union has a duty to honour the personality of each individual citizen and provide opportunities for self-fulfillment. This Preamble clause has been interpreted as meaning that it is linked to the Fundamental Rights in Part III, including Article 21 of the Constitution which states that "no person shall be deprived of his life or personal liberty except according to the procedure established by law". The Supreme Court of India has been enhancing the definition of "life" in Article 21 from being simply an animal life to a life with dignity over the past few decades. This growth was prompted by the judgment in Maneka Gandhi (1978) which said that the fundamental rights are not "water-tight compartments", but constitute a "Golden Triangle".
The relation between fraternity and dignity is very special in Indian jurisprudence. Fraternity is often considered as "duty-apt", that is to say, it is something that the state and its citizens must do; dignity is "rights-apt", something they must come with. The Court observed in Puttaswamy that dignity is guaranteed by the brotherhood which allows a person to grow to his full potential in a society of compassion. This communal component of dignity implies that privacy is not merely an "elitist construct" but a fundamental value which aids a civil and humane social order.

The Supreme Court has used different perspectives in defining the constitutional role of dignity, including the "minimalist perspective," which forbids torturous and degrading punishments against prisoners, to the "maximalist perspective," whereby the state is obliged to ensure that citizens have access to basic necessities such as food, shelter, and clothes. These inconsistent uses have resulted in what some authors describe as "dignity inflation," whereby the concept of dignity is used to justify many rights, although its definition in law is controversial. Despite all these uncertainties, the Supreme Court holds that dignity is the fundamental principle that binds all Fundamental Rights since they strive to attain a "dignity of existence"

Jurisprudential Evolution: From Secrecy to Fundamental Right

The path to the inclusion of privacy as a fundamental right in India was a long one, characterized by ambiguity in the law and judicial restraint. “The right to privacy was a constitutional legacy that was left to the future by early decisions such as M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1964). In M.P. Sharma, an eight-judge bench on search and seizure found that a right to privacy could not be read into the protection against self-incrimination of the Indian Constitution, in the absence of a clause similar to the Fourth Amendment of the US Constitution. “

In the same vein, the Kharak Singh verdict by a six-judge bench said that under the Constitution, “privacy” was not a “guaranteed” right. The Court, however, had an interesting contradiction in its judgment: although it didn't accept the notion of a “general right to privacy”, it did invalidate “domiciliary visits” (the practice of police visiting people at night), as a violation of “ordered liberty” under Article 21. The approach of “silos”, examining the concept of fundamental rights in separate compartments was much influenced by the doctrine of A.K. Gopalan which was subsequently struck down by the landmark Maneka Gandhi judgment of 1978.

“Since 1978, smaller benches have started to find that privacy is a part of “ordered liberty.” Gobind v. State of M.P. (1975) recognised that privacy also involves "personal intimacies of the home, the family, marriage, motherhood, procreation and child rearing". In R. Rajagopal v. State of Tamil Nadu, by 1994, the Court came to a conclusion that the right to be let alone was an inherent part of Article 21. In PUCL v. Union of India (1997), the Court limited unchecked telephone tapping, demanding that certain procedural measures would be implemented in order to safeguard the privacy of communication. This incremental process culminated in the watershed Justice K.S. Puttaswamy (Retd.) v. Union of India judgment of 2017, delivered by a nine-judge bench unanimously, which made privacy a fundamental right inhuman nature. The Court noted that the right to life and liberty are "inalienable" and that Article 21 does not contain them all but rather only "reflects" them. Privacy was regarded as a manifestation of individual autonomy and dignity, a way in which a human being can lead a dignified life and protect the ‘inner recesses of the human personality' from 'unwanted intrusion'.

The Puttaswamy Judgment: Privacy as the Core of Dignity

India's recent privacy jurisprudence has been built on the 2017 Puttaswamy judgment. It has affirmed that privacy is not an independent right but a part of the dignity of the human person and that violation of privacy is "inextricably bound up with all exercises of human liberty". In emphasizing that dignity cannot exist without privacy, the Court made clear that privacy is essential to the space needed for individuals to make choices they need to make and live without unwarranted state intrusion.

It was one of the most important findings of the judgment that it introduced the concept of privacy in three forms: informational, spatial, and decisional. In particular, informational privacy was deemed to be essential in a world built on information and plagued by both state and non-state agents of danger. Decisional privacy was associated with personal intimacies such as the right to choose one's sexual orientation, a "natural right" that was vested in virtue of being human. This reasoning was applied to invalidate the previous Suresh Koushal judgement and the bench said the rights of LGBTs are based on "sound constitutional doctrine" of life, privacy and dignity.

The Court also rejected the argument that the right to privacy should be abandoned in order to secure welfare benefits, known as the “elitist construct.” It believed that civil and political rights had a lower priority than their socio-economic status; that they were rights of all people, not just the disadvantaged, and that they were there to safeguard the disadvantaged against state profiling and surveillance. This repudiation of a compromise between "bread" and "privacy" helped to reinforce the notion of dignity as being common to all, not reserved for the few.

The judgment set up a strict "Three-fold Requirement" for a state invasion of privacy. Any restriction must meet the test of:

- Legality: A lawfulness.
- Legitimate Aim: A necessary state objective (security, welfare, etc.).
- Proportionality: A logical link between the object and the means, so the intrusion is as minimal as can be.

In its immediate aftermath, this standard was adopted in the challenges to the Aadhaar project, a case in which the Court had to consider structural hazards of a biometric identity system in a surveillance intensive digital era.

Informational Privacy and the Surveillance State: The Aadhaar Challenge

Aadhaar, the biometric-based identity system pioneered in India, provided the prime context for the Puttaswamy reference. When biometric-registration commenced in 2010, there was no overarching legislation, or privacy safeguards, about the biometric system, creating a "policy vacuum" which led to the system becoming ubiquitous and persistent, and possibly functioning as a device of mass control or surveillance. In the 2018 Aadhaar judgment (Puttaswamy II), the Supreme Court largely upheld the validity of the Aadhaar Act, holding that it could function as a de-duplication mechanism for false identities and as an "empowering device" providing subsidy benefit to vulnerable populations.

The Court found that the system used "minimal data" and was purpose blind in that the collection process did not depend on information about location or purpose or even transactions. Still, the Court invalidated Section 57 that allowed private institutions to mandate Aadhaar, finding that it was not "illegal" under the Puttaswamy test. The minority judgment (by Justice Chandrachud) was a more critical analysis of the structural threats to dignity.

Under the architecture of Aadhaar, he explained, the state was able to create a "surveillance society": by proliferating Aadhaar numbers throughout multiple databases, bank accounts, tax returns, etc., it was able to mirror a subject's entire history of interaction. This "'structural inroad' on privacy" was "distinct from targeted or concerted surveillance" and had "the tendency to diminish the barrier of distance in public". The Aadhaar case demonstrated the balance between "informational self-determination" and the "wampum of the state". Though the Court did impose some restrictions, critics still feel the absence of technologies to prevent data breaches and continued government exemptions Much endanger the new baseline of privacy.

The Digital Personal Data Protection Act (DPDP), 2023: Rights and Fiduciaries

After the Puttaswamy judgment and its statement of need for a stringent data protection structure, India brought into force the Digital Personal Data Protection (DPDP) Act in 2023. It seeks to strike a balance between the individual right to protect his data and the need to process that data for "lawful purposes". It is a replacement to the previously effective IT Act and the rules under it, which were seen as archaic. The Act establishes two main legal persons: the Data Principal(d being, the person) and the Data Fiduciary(d deciding for what purpose of processing). Purpose of processing is Mostly allowed on a "consent" that should be "free, specific , informed, unconditional and unambiguous with a clear affirmative action" [7].

Moving away from the draft bills, the 2023 Act categorises all digital personal data as one category (unlike the GDPR that had a separate classification called sensitive personal data which would cover data related to

health genetics, biometrics, sex life, sexual orientation, religion caste etc) [8]. While these rights enable the citizen, the Act also imposes duties on the Data Principal under Section 15.This obligation includes a duty to adhere to applicable laws and provide "verifiably authentic" information when seeking correction. The imposition of individual duties with data rights is considered a tectonic shift, as non-compliance with this duty could disqualify a citizen from invoking the right to privacy or attract penalties.

Fiduciary Obligations and Regulatory Oversight

Data Fiduciaries shall also entail a comprehensive compliance obligation in Section 8 of the DPDP Act, where a Data Fiduciary is "responsible for complying with the provisions of this Act", even if there is an agreement to the contrary or the Data Principal has failed to do his/her part. The obligation Because of this set out is one of "absolute, non-delegable, vicarious liability" on the Data Fiduciary. They shall also adhere to 'reasonable security safeguards', disclose security breaches to the Data Protection Board, and stop using such data once the purpose for which data was collected has been fulfilled. For 'Significant Data Fiduciaries' (SDFs), which can be categorized based on quantity of data processed, or risk to the sovereignty and integrity of India, the duties are closer to those of a commercial enterprise.

SDFs have to appoint a Data Protection Officer in India and an independent data auditor, and conduct periodic Data Protection Impact Assessment (DPIAs) to identify risks. The act is enforced by the Data Protection Board of India, which is a central agency; members of it are nominated by the Central Government. This has motivated concerns about the institutional independence of the Board and the Government's ability to hold government institutions to account. The Board can impose civil penalties between ' 10,000 to 250 crore' per incident, given the severity of the breach.

The 2025 Rules: Operationalizing Consent and Control

In an effort to bring the DPDP Act alive, the Ministry of Electronics and Information Technology(MeitY) published the Draft Digital Personal Data Protection Rules in early 2025. These rules articulate guidelines for how entities are to communicate with Data Principals that Center on openness and clarity. For example, Rule 3 states that consent notices be "clear and easily comprehensible without any reference to other information, including in the form of Terms of Service or Privacy Policies.

" The rules further create a new category of regulatory intermediaries called "Consent Manager ", a method of giving individuals a centralized control point for managing their consents across multiple fiduciaries. Consent Managers will be required to act in a fiduciary capacity toward the Data Principal and provide interoperable platforms for giving, reviewing, and withdrawing consent.
There are also a number of important "Purpose-specific retention" limits in the 2025 Rules. Some providers (social media sites, online gaming sites with millions of users for example) must delete personal data after three years of the last user activity. Fiduciaries have to inform individuals of this deletion 48 hours before conclusion. This prevents personal data from eternally living in interconnected systems preventing social/political control.

Critiques of State Overreach and the Oversight Vacuum

Although the Puttaswamy judgment was based on a rights-based approach, the DPDP Act 2023 has faced scrutiny for inadequate provisions of sweeping 'government exemptions'. Section 17 permits the Central Government to exempt government agencies from virtually the entire statute, save security standards, on the grounds of 'security of the State', 'public order etc. Critics contend that the phrase "as may be prescribed"used 26 times throughout the 44-section Act "aggravates the potential for 'blanket exemptions. Contrary to the UK's Data Protection Act that involves warrants issued by the judiciary and oversight by Parliament for information held of a national security nature, the Indian DPDP ACT states that there is "absolutely no oversight upon the government's use of personal data".

Depending upon the implementation of the law, section 36 otherwise ascribes limitless authority to the State or the government to require Data Fiduciaries to provide single individual information in absolute secrecy and without informing the individual, Because of this opening a "loophole" that might mean "being watched in every waking moment" leading to a "self-fulfilling prophecy of an 'Orwellian state'". The concern with this But is that it is accompanied by a loophole or gap through which privacy violations will go unaddressed, the Act has no provision for compensation or restitution to be paid to violations of privacy.

This absence of the ability to claim damages, despite Truth is the existence of such damages claims will now be Much less likely, may frustrate the principles of privacy by tilting the power balance toward surveillance interests and the state of the Data Principal. Several researchers have pointed out that these loopholes are 'the beginning of the end of liberty' in India.

Global Benchmarking: GDPR, US Sectoralism, and the Indian Hybrid

India's DPDP Act is purportedly a unique approach in the contemporary global privacy universe, functioning between the "highly rights-based approach" of the General Data Protection Regulation, and the more "governance-based approach" aimed at agglomerating data for development; Key differences exist between the structure of the GDPR and the structure of the DPDP Act [], Unlike the GDPR "white-list" approach (i.e. only allow cross-border flow to "adequate" countries), India has chosen a "black-list" approach of allowing transfers unless To be exact prohibited by the Central Government to a particular country or territory (90). This is more trade-permissive but less procedural assurance of the standard of protection of the destination country's regime.

Compared to the "fragmented" US sectoral approach (e.g. HIPAA applies to Healthcare alone), the DPDP Act offers a more "unified" digital data protection. Yet, US state laws - CCPA (California) and CPRA (California), for example - have detailed consumer rights for the restriction of sales of personal data that exceeds Indian law, which may benefit from the consideration of current state versions such as those proposed in Tennessee, Minnesota and Maryland.

AI, Facial Recognition, and the Chilling Effect on Dissent

The most immediate frontier for privacy in India is the deployment of Artificial Intelligence (AI) and Facial Recognition Technology (FRT). Initiatives like DigiYatra, which uses facial verification to process air travelers, have been criticized for creating a "defective model of consent". Although the service is marketed as voluntary, reports of passengers being coerced to sign up at airport gates raise concerns about whether such consent is genuinely "free".

The use of AI in law enforcement and public security also poses grave risks to human dignity. FRT systems are prone to "algorithmic bias," often exhibiting higher error rates for women, children, and marginalized

minorities. In the context of criminal justice, a "false positive" can lead to wrongful suspicion or arrest, violating the fairness and reasonableness required under Article 21. Furthermore, "black box" algorithms deny individuals the "right to an explanation," making it impossible to contest decisions that affect their lives.

Mass surveillance through FRT treats every citizen as a potential suspect, eroding the anonymity that is a key component of democratic participation. This constant monitoring can lead to a "chilling effect," where individuals alter their behavior, avoiding protests or dissenting speech, for fear of being profiled. Because India currently lacks a dedicated statute regulating the use of facial recognition, these technologies operate in a "legal vacuum," posing a severe threat to the constitutional vision of a humane and compassionate society.

Conclusion: Toward a Dignity-Centric Digital Democracy

The Role of Privacy as Human Dignity in India is at a pivotal crossroads. While the Puttaswamy judgment provided a powerful "Rights as Trumps" framework, the subsequent transition to statutory law and draft rules suggests a pragmatic shift toward "strategic governance". The resulting legal infrastructure is one of both promise and fragility.

The DPDP Act 2023 represents a significant step forward from the silence of previous decades, establishing clear obligations for fiduciaries and rights for individuals. However, for the Act to truly uphold the "dignity of the individual," several gaps must be addressed:

Regulatory Independence: The Data Protection Board must operate with genuine autonomy from the executive to ensure that state violations are penalized as rigorously as corporate ones.

Narrowing State Exemptions: The "Oversight Vacuum" created by Section 17 must be filled with judicial or parliamentary checks to prevent the emergence of a "surveillance society".

Recognition of Sensitive Data: Following the "gold standard" of the GDPR, India should consider categorizing biometric and health data as "sensitive" to provide enhanced safeguards for these intimate aspects of personhood.

Algorithmic Transparency: As AI mediates more of the state's power, the "right to explanation" and mandatory audits for high-risk AI tools must be codified to prevent arbitrary and biased decision-making.

Ultimately, privacy is not merely a technical requirement for data management; it is the legal expression of the moral requirement to respect persons as persons. In a digital democracy, the individual must remain the "focal point" of the Constitution. Technological progress should fortify, rather than fracture, this constitutional commitment to a dignified existence. Only by ensuring that privacy rights are "real" and not "so-called" can India fulfill its aspirations as a sovereign, democratic republic that assures the dignity of every citizen.

VII. REFERENCES:

[1] . The Right to Privacy: History, Philosophy, and Law – NeGD ..., https://negd.gov.in/blog/the-right-to-privacy-history-philosophy-and-law/

[2] Digital Personal Data Protection Act, 2023 DPDPA SECTION 12 WITH INTERPRETATION, https://www.dpdpa.com/dpdpa2023/chapter-3/section12.htm

[3] Fraternity's Role in Indian Constitution | PDF | Justice | Crime & Violence - Scribd, https://www.scribd.com/document/739496314/FRATERNITY-SIDE-NOTES

[4] Preamble to the Indian Constitution: Meaning, Significance & More - NEXT IAS, https://www.nextias.com/blog/preamble-to-the-indian-constitution/

[5] Finding Method to Madness: The Indian Supreme Court's Dignity ..., https://repository.nls.ac.in/cgi/viewcontent.cgi?article=2029&context=nlsir

[6] Human Dignity in Indian Constitutional Adjudication (Chapter 1), https://www.cambridge.org/core/books/human-dignity-in-asia/human-dignity-in-indian-constitutional-adjudication/7BBB9960207BC44B913E61B155F87D84

[7] K.S. Puttaswamy v. Union of India [2017 SC] - Goa Police Constable PDF - EduRev, https://edurev.in/t/181628/k-s-puttaswamy-v-union-of-india-2017-sc-

[8] Constitutional Law Perspectives on Human Rights and Duties, https://ebooks.inflibnet.ac.in/hrdp01/chapter/constitutional-law-perspectives-on-human-rights-and-duties/

[9] Fundamental rights in India - Wikipedia, https://en.wikipedia.org/wiki/Fundamental_rights_in_India

[10] JUSTICE K.S. PUTTASWAMY (RETD.) & ANR. VS. UNION OF INDIA & ORS. - AWS, https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/justice-ks-puttaswamy-ors-vs-union-of-india-ors-5.pdf

[11] The POSH Act And Article 21: Dignity, Privacy, And Confidentiality In Workplace Harassment Proceedings - RJ Wave, https://www.rjwave.org/ijedr/papers/IJEDR2601086.pdf

[12] JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA - South Asian ..., https://translaw.clpr.org.in/case-law/justice-k-s-puttaswamy-anr-vs-union-of-india-ors-privacy/

[13] Puttaswamy v. Union of India - Wikipedia, https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India

[14] A Comprehensive Analysis of Data Privacy Evolution in India and Digital Personal Data Protection Act, 2023, https://research-communications.cmpcollege.ac.in/wp-content/uploads/2025/01/5-Raje-and-Dr.-Radheshyam-Prasad-REVISED-PAPER-A-Comprehensive-Analysis-of-Data-Privacy-Evolution-in-India-and-Digital-Personal-Data-Protection-Act-2023.pdf