INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

HUMAN RIGHTS 2.0: PRIVACY AND SURVEILLANCE CHALLENGES IN INDIA'S DIGITAL REGIME

AUTHORED BY - RASHITHA MUNAVAR. S
K.K Nagar, Tiruchirappalli, Tamil Nadu, India.

"Balancing right to freedom, privacy, and memory in the digital era amidst growing state access to personal data"

ABSTRACT

"Human rights" refer to the fundamental freedoms and protections that allow every individual to live with dignity, autonomy, and equality. These principles, drawn from the Indian Constitution and reflected in key international agreements, serve as the foundation for personal liberty and justice. In today's rapidly evolving digital environment, the concept of privacy has emerged as an essential element of human rights. However, this advancement has created a complex landscape where personal freedom must constantly be balanced against the expanding powers of the state, especially regarding access to digital data. This explores how effectively India's legal and constitutional safeguards protect citizens from intrusive surveillance in an era where technology can record, predict, and influence individual behaviour. By relying on doctrinal research, supported by landmark judgements and ongoing policy debates, the study evaluates whether the current framework including the Digital Personal Data Protection (DPDP) Act is capable of regulating modern surveillance systems. The analysis indicates that although privacy is a recognized constitutional right, the mechanisms for checking state monitoring remain inadequate. Key concerns include broad executive exemptions within the data protection regime, limited judicial oversight, and insufficient transparency in intelligence operations. The paper argues that technological progress must be accompanied by stronger accountability measures and clear legal boundaries. Only a rights-centered approach to digital governance can prevent unchecked surveillance from weakening the personal freedoms that form the basis of a democratic society. Strengthening procedural safeguards, improving institutional oversight, and ensuring public awareness about data rights are essential steps toward preserving privacy in a digitally interconnected world.

KEYWORDS: Human Rights, Right to privacy, Right to freedom, Personal Data Protection, Digital regime.

ISSN: 2582-6433

1. INTRODUCTION

In 2025, the number of global internet users surpassed 6 billion, representing over 73% of the world's population, the digital world undeniably shapes our daily lives, influencing social interactions, economic activities, and access to information.[1] Digital technologies are profoundly intertwined with constitutionalism now a days. Digital Constitutionalism can be track all over the world after the European Union's General Data Protection Regulation (GDPR) in 2018 and In India after the landmark judgement of the Justice K. S. Puttaswamy case in 2017. Digital constitutionalism is a concept of establishing a set of principles, norms, and rules that govern the use, protection, and regulation of digital technologies within a society.[2] It insists on the importance of privacy and free speech, asserting that neither the state nor private corporations should be allowed to use technology to circumvent the constitution. Human Rights 2.0 focuses on "Right to control the flow of information" and "Protection of digital information" of individual person. Because of this protection the new concept of Informational Autonomy was established. Many times, technology violates your informational autonomy by taking data without your knowledge. Once the autonomy was lost, the state use individual data or took control of individual digital privacy. The solution to resolve this to bring the digital constitutionalism. This paper employs a **doctrinal research methodology**, involving a systematic analysis of primary legal sources, including the Constitution of India, the Digital Personal Data Protection (DPDP) Act 2023, and landmark judicial pronouncements such as *Justice K.S. Puttaswamy v. Union of India and etc.* To provide a global perspective of Human Rights 2.0, the study utilizes **comparative jurisprudence**, contrasting India's digital regime with the European Union's GDPR. The research is an analytical, descriptive and right-centered approach aimed at identifying gaps in the current legal framework regarding state surveillance and individual informational autonomy.

[1] Kumar, P. (2025) 'Locating Digital Constitutionalism in India and south asia- preliminary enquiry', *Kathmandu School of Law Review*, pp. 87–103. doi:10.46985/kslr.v13i1.2237.
[2] Celeste, E. (2022) 'The constitutionalisation of the Digital Ecosystem: Lessons From International Law', *Digital Transformations in Public International Law*, pp. 47–74. doi:10.5771/9783748931638-47.

ISSN: 2582-6433

2. THE EVOLUTION OF SURVEILLANCE IN INDIA: *FROM COLONIAL ERA TO DIGITAL ERA*

2.1 The Colonial Era:

In Colonial era, the two significant legislations were introduced. The Indian Telegraph Act, 1885 and The Indian Post Office Act, 1898. These two Acts focuses on Communication interception and mail surveillance. The surveillance in India was born for colonial stability not for public safety. And also, this legislation for executive Prerogative of British government. There was no judicial threat for these legislations at that time.

2.2 The Post-Independence Era

In this era, the judicial system grew fast and steady. In this period, the judiciary laid the foundation for rights we enjoy today, like the right to life, equality, freedom of speech, etc. And the Indian judiciary began to limit the State's "absolute" power. In the way of interpreting the constitution, they gave so many landmark judgements related to Right to privacy and surveillance.

2.2.1 Denial of Privacy (1950-1970)

The 1954 decision in *M.P. Sharma v. Satish Chandra*[3] represents the earliest judicial attempt to address the right to privacy in post-independence India. An eight-judge bench of the Supreme Court examined whether the search and seizure powers under the Code of Criminal Procedure were constitutional. Ultimately, the Court refused to recognize privacy as a standalone legal right, concluding that state-led searches did not constitute an infringement. The bench reasoned that because the Indian Constitution lacks an explicit provision for privacy, such a right could not be invoked to challenge state actions.

In the case of *Kharak Singh vs State of Utter Pradesh*[4], the Supreme Court struck down Regulation 236(b) of the UP Police Regulations, which permitted nighttime "domiciliary visits." The Court ruled that such nocturnal intrusions violated the sanctity of the private home and

[3] M.P. Sharma v. Satish Chandra [1954] 1 SCR 1077
[4] Kharak Singh vs State of Utter Pradesh AIR 1963 SC 1295

ISSN: 2582-6433

infringed upon "personal liberty" as protected by Article 21. Although the majority did not explicitly use the term "privacy," their reasoning drew significantly from the US Supreme Court's decision in *Wolf v. Colorado*[5], which is centered on privacy protections. Despite this indirect validation, the Court paradoxically upheld other surveillance measures, explicitly stating that the Indian Constitution did not recognize an independent right to privacy can take it as partial recognize of privacy. Nevertheless, this decision served as a crucial stepping stone for later benches to expand on the concept of personal liberty. This "tacit acknowledgement" created a legal opening that later courts exploited to eventually recognize privacy as a fundamental right, effectively bridging the gap between colonial-era control and modern informational autonomy.

2.2.2 Recognition of Privacy (1970-1990)

The *Govind vs State of Madhya Pradesh*[6] decision is significant for introducing a nascent version of the proportionality test to India. By referencing US privacy jurisprudence like *Griswold v. Connecticut* [7]and *Roe v. Wade*[8], the Court categorized privacy as an essential element of personal dignity, particularly regarding domestic and bodily autonomy. Crucially, *Govind* established that state interference is only permissible if it meets a dual-standard: it must serve a **compelling interest** and be narrowly tailored to avoid excessive intrusion. Also, the Court pioneered the **"Penumbral Theory"** of rights, suggesting that privacy exists in the shadows and overlaps of other fundamental rights. This shifted the debate from whether privacy exists to how the State must justify its violation a precursor to the modern "Human Rights 2.0" framework.

2.2.3 The Proceduralisation of Privacy (1990-2000)

In *PUCL v. Union of India*[9], the Supreme Court confronted the lack of statutory regulation regarding telephone interception. The Court

[5] Wolf v. Colorado 338 U.S. 25 (1949**)**
[6] 1975 AIR 1378
[7] Griswold v. Connecticut 381 U.S. 479 (1965)
[8] Roe v. Wade 410 U.S. 113 (1973)
[9] People's Union for Civil Liberties (PUCL) vs Union of India AIR 1997 SC 568

ISSN: 2582-6433

determined that a telephone conversation is a private act, and its unauthorized interception constitutes a breach of Article 21 of Indian Constitution. While the Court did not strike down the Telegraph Act, it mandated a rigorous "procedural safeguard" system, requiring that all surveillance orders be authorized by high-ranking executive officials and be subject to periodic review. This judgement shifted surveillance from an unchecked sovereign power to a regulated administrative function. The Court proceduralised by creating the "PUCL Guidelines".

2.3 Birth of Information Technology Act, 2000: *Digitalising State Surveillance*

The IT Act 2000 marked the end of the 'Physical Era' of surveillance. By providing the State with the legal authority to decrypt and monitor digital traffic, it created a procedural framework that prioritised national security over the nascent digital privacy of the Indian citizen. For the first time, the law empowered the Central and State governments to compel any "intermediary" to assist in the decryption of data[10]. IT Act treated digital privacy as a secondary interest and the law viewed the internet primarily as a space for commerce and a threat to security, completely ignoring its role as a space for personal liberty and individual autonomy until 2017. The structural evolution of the IT Act reached a critical juncture in Shreya Singhal v. Union of India[11]. By striking down the overbroad Section 66A, the Supreme Court prevented the 'digitalisation of criminal intimidation.' The judgement reinforced that constitutional safeguards for free speech do not vanish in cyberspace. It served as a vital precursor to the Puttaswamy case by insisting that any state-mandated restriction on digital communication must be specific, narrow, and constitutionally sound. By prioritising the State's need to decrypt and monitor over the citizen's need for anonymity, the Act set a precedent for the Digital Absolutism that we see today in the DPDP Act 2023.

2.4 The Digital Era: Human Right 2.0

In this era, Privacy shift from the 'Spatial Privacy' of the physical world to

[10] The Information Technology Act, 2000, § 69.
[11] Shreya Singhal v. Union of India AIR 2015 SC 1523

ISSN: 2582-6433

the 'Informational Autonomy' of the virtual realm. While previous eras were concerned with the state's ability to physically intrude into a citizen's life, the Digital Era is marked by the judicial recognition of privacy as an inalienable fundamental right under the Puttaswamy doctrine. However, this era also presents a significant paradox. And also, era of digitalisation has posed grave challenges in the way of right to privacy, some of the prominent challenges are Data breaches, Surveillance by corporations and government, Social Media Information Policy, Corporate Accountability, Weak Grievance Redressal Systems[12].

2.4.1 Privacy accepted and protected by Constitution

Ultimately, the Digital Era represents a transition from 'Search and Seizure' to 'Predict and Prevent.' While the judiciary has provided a robust shield through the *Justice K.S. Puttaswamy (Retd) vs Union of India*[13] judgement. While the legal battle began with a writ petition in 2012 challenging the biometric Aadhaar scheme, it culminated in the historic 2017 judgement. This 2017 ruling is the definitive authority that recognized informational privacy as a constitutional guarantee, moving India into the modern Digital Era of human rights.

2.4.1.1 Explained in Puttaswamy Judgement

This judgement represents a paradigm shift in Indian jurisprudence, moving the country from a **"State-Centric"** to an **"Individual-Centric"** surveillance model. And most significant legal achievement of Puttaswamy was the explicit overruling of the judgement of *M.P. Sharma* and *Kharak Singh*. The Court held that privacy is an intrinsic part of the Right to Life and Personal Liberty under Article 21 of Indian Constitution. Rather than offering a narrow definition, the judiciary recognized privacy as a multifaceted right essential to human dignity. This framework includes **spatial and bodily privacy**, which guards against physical trespass; **informational control**, which is crucial in the digital age for governing personal records; and **decisional independence**, which ensures that the State cannot dictate a citizen's most private life choices, including their sexual

[12] Ananya Agarwal, *Right to Privacy in the Digital Age: Challenges and Solutions* (Aug. 20, 2024) (unpublished manuscript): https://ssrn.com/abstract=4955726 or http://dx.doi.org/10.2139/ssrn.4955726

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

ISSN: 2582-6433

orientation or personal affiliations.

2.4.1.2 Triple test: The Constitutional Standard for State Intrusion

The most enduring legacy of the *Puttaswamy* (2017) judgment is the creation of a rigorous judicial standard the "Triple Test.[14]" This framework serves as a constitutional barrier, ensuring that the State's power to conduct surveillance is not absolute. For any state action to legally infringe upon a citizen's digital or physical privacy, it must satisfy three cumulative conditions:

The Principle of Legality (Existence of Law): Surveillance cannot be carried out through mere executive discretion or administrative "standard operating procedures." There must be a specific, valid **statutory law** in place that authorizes the interference. This ensures that the state remains accountable to the legislature and the people.

The Requirement of Need (Legitimate State Aim): The State must prove that the intrusion is necessary to achieve a valid social or national goal. The Court clarified that while "National Security" is a legitimate aim, it cannot be used as a vague, catch-all excuse. The objective must be clear, such as preventing a specific crime or maintaining public order.

The Doctrine of Proportionality (Rational Nexus): This is the most critical pillar for "Human Rights 2.0". The State must demonstrate that the extent of the surveillance is **strictly proportional** to the objective. It must employ the "least restrictive" method available. In the digital age, this means mass, indiscriminate data harvesting is generally unconstitutional because it is inherently disproportionate compared to targeted, specific interception. In the current Digital Era, proportionality has evolved from a simple balancing act into a structured four-part inquiry that prevents the State from using 'National Security' as a carte blanche for mass surveillance.

[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 310 (India) (per Chandrachud, J.)

ISSN: 2582-6433

3. HUMAN RIGHTS 2.0 AND LEGISLATIVE TURN: *THE EMERGENCE OF INDIA'S DIGITAL PERSONAL DATA REGIME*

3.1 Justice Srikrishna Committee (2018)[15]

The Government of India constituted a High-Level Committee headed by Justice B.N. Srikrishna to draft a data protection law. It introduced the specialized vocabulary that governs India's digital regime today. While the EU's GDPR uses the term "Data Subject" suggesting a person who is governed or passive the Srikrishna report coined the term "Data Principal." This terminology reinforces the idea of Informational Sovereignty, positioning the individual as the primary authority and the entity handling the data as a mere representative or agent. This report also mentions that "the State must collect only the data that is strictly necessary for a specific, pre-defined goal". The report called for a Data Protection Authority (DPA) that was independent of the Executive. The Justice Srikrishna Committee Report is the bridge between the *Puttaswamy* judgment and the DPDP Act 2023.

3.2 The Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection (DPDP) Act 2023 marks the final step in India's transition to a formal data regime. While it provides a statutory framework for data processing, it introduces several "Surveillance Challenges" that test the limits of the Puttaswamy doctrine. The Act mandates that consent must be free, specific, informed, and unconditional. Yet, for most citizens, digital consent is often a "contract of adhesion". DPDP Act introduced the "Duties of the Data Principal" this creates a **"Chilling Effect"** Citizens may be hesitant to enforce their Right to Privacy if they fear being penalized by the Data Protection Board. This shifts the burden of the "Digital Regime" from the powerful Fiduciary to the individual citizen. Under Section 17(2)(a)[16], the Central Government can exempt any "instrumentality of the State" from the Act's requirements in the interest of sovereignty, integrity of India, or public order. The

[15] Committee of Experts on Data Protection, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)
[16] The Digital Personal Data Protection Act, 2023

ISSN: 2582-6433

Act establishes a "Data Protection Board" to adjudicate disputes. However, the Central Government controls the appointment, salary, and terms of the Board members. The Act does not require a Judicial Warrant before the State invokes an exemption. But this lacks Independent Regulator proposed by Justice Srikrishna report in 2018.

3.3 Triple test in DPDP Act, 2023

Requirement of Triple test are Legality, Neccesity and proportionality. In DPDP Act 2023 complied the legality, legitimate aim of this triple test but fail to comply the proportionality because Section 17(2)(a), the State is provided with expansive exemptions that effectively bypass the core requirements of necessity and 'least restrictive means.' By relieving government entities of the duty to follow data minimization and purpose limitation, the Act facilitates a level of information gathering that is fundamentally disproportionate to its legitimate objectives, thereby clashing with the Puttaswamy proportionality standard.

3.4 The Pegasus Precedent: A Check on Digital Absolutism

The *Manohar Lal Sharma*[17] judgment also known as the "Pegasus Case" is a landmark in Indian digital jurisprudence. It addresses the legal vacuum surrounding military-grade spyware and the limits of the "National Security" defence used by the State. The case arose following a global investigation 'The Pegasus Project' which alleged that the devices of over 300 Indian citizens including journalists, opposition leaders, and even a sitting Supreme Court judge were targeted using the Pegasus spyware. The petitioners sought an independent probe into whether the Union Government had authorized this surveillance. The court said "*The State does not get a free pass every time the spectre of 'national security' is raised. National security cannot be the bugbear that the judiciary shies away from"*. The Court noted that the "chilling effect" of surveillance leads to self-censorship, particularly among journalists and activists. This violates Article 19(1)(a) of Indian Constitution. The Court reiterated that even for security purposes, any surveillance must meet the Puttaswamy Triple Test.

[17] Manohar Lal Sharma v. Union of India, (2022) 3 SCC 25

ISSN: 2582-6433

4. BALANCING FREEDOM, PRIVACY AND MEMORY: THE CONSTITUTIONAL CHALLENGES

The modern digital regime has created a "trilemma" where the enhancement of one right often comes at the expense of another. In the wake of the DPDP Rules 2025[18], this balance has shifted significantly toward state access.

4.1 The Right to Freedom: Expression vs. Surveillance

The "Right to Freedom" (Article 19) is increasingly threatened by the "invisible" nature of digital surveillance. Under Rule 23 of the DPDP Rules 2025, the Union Government can demand information from platforms Meta, Google, etc. And explicitly prohibit them from informing the user about the data request. This creates a “Chilling Effect” on free speech. If a citizen knows the State can access their metadata without a trace, they are less likely to exercise their freedom of expression or dissent.

4.2 The Right to Privacy: Consent vs. State Necessity

While Section 6 of the DPDP Act mandates “free and informed” consent, the State has carved out a "Blanket Immunity" for itself. Section 17(2)(a) of DPDP Act,2023 exempts state instrumentalities from core obligations in the interest of “public order" or "sovereignty.”

4.3 The Right to Memory

The "Right to be Forgotten" (RTBF) is the most contested area in your paper. It is the right to have one's "Digital Shadow" erased. Section 12 of the DPDP Act 2023 recognizes the "Right to Erasure. However, the DPDP Rules 2025 (Rule 8) introduced a “one-year mandatory retention requirement for logs”. The State argues this is for "national security," but it effectively creates a "Digital Memory" that the citizen cannot erase.

The judiciary has increasingly utilized 'John Doe' orders to enforce the Right to be Forgotten. In Nitin Bhatnagar v. ANI Media Pvt. Ltd.[19] , the Patiala House Court issued a landmark directive for the de-indexing of articles linking an exonerated

[18] Digital Personal Data Protection Rules, 2025, (notified Nov. 14, 2025).
[19] *Nitin Bhatnagar v. ANI Media Pvt. Ltd.*, CS No. 510/2025, Order dated Nov. 10, 2025.

ISSN: 2582-6433

individual to a financial crime. This protection was subsequently affirmed by the Delhi High Court[20], which held that continued digital dissemination of arrest reports following a discharge constitutes a violation of the Right to Dignity under Article 21.

4.4 Sanchar Saathi Controversy

Government initiatives such as Sanchar Saathi[21] are often presented as citizen-friendly tools that improve consumer security and reduce telecom-related fraud.

At a policy level, these goals are legitimate. However, the constitutional concern arises from the method through which these goals are achieved especially when systems rely on centralised identity linkages.

The Sanchar Saathi ecosystem reportedly connects IMEI and Aadhaar-linked identity structures, creating a centralised repository of metadata.

While such linkability may improve fraud detection, it also increases the risk of surveillance by building a single point through which a citizen's digital activity can be traced across devices and networks.

From a constitutional perspective, this raises issues under the necessity and proportionality prongs of the Puttaswamy Triple Test. Fraud prevention may be a legitimate aim, but the creation of an identity-linked "master key" to communication systems may not be the least restrictive means of achieving that aim.

Further, when identity links are stored for long periods, the system begins to resemble a permanent digital ledger. This not only limits anonymity but also undermines the effectiveness of erasure-based protections and the broader right to be forgotten. In that sense, Sanchar Saathi demonstrates the "surveillance paradox": a system can be technologically effective while remaining legally under-regulated.

Therefore, initiatives of this kind require clear purpose limitation, strict safeguards against function creep, and meaningful independent oversight. Without these protections, public trust may weaken and the digital regime risks becoming inconsistent with the rights-centred vision of Human Rights 2.0}

[20] *IE Online Media Services (P) Ltd. v. Nitin Bhatnagar*, 2025 SCC OnLine Del 9281

[21] *Sanchar Saathi Portal*, Department of Telecommunications, Government of India, https://www.sancharsaathi.gov.in

ISSN: 2582-6433

5. CONCLUSION

India's journey from fragmented privacy protections to a structured personal data regime under the Digital Personal Data Protection (DPDP) Act, 2023, and the subsequent 2025 Rules represents a major legislative shift in the country's digital governance.

However, this transition also reveals a serious contradiction at the heart of the new framework.

On the surface, the DPDP regime appears to empower individuals by recognising them as "Data Principals" and by presenting consent as the foundation of lawful data processing.

Yet, when the Act is examined more closely, it becomes clear that the State retains extensive discretion through broad exemptions and retention powers. As a result, the legal framework risks strengthening State access to personal data while offering limited institutional resistance against misuse.

As this paper has argued, the exemptions under Section 17 and the retention-based approach reflected in the 2025 Rules threaten to weaken the practical value of the proportionality standard established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).

If proportionality becomes a formality rather than an enforceable safeguard, constitutional privacy may remain strong on paper but fragile in practice.

The idea of "Human Rights 2.0" requires a modern understanding of privacy. In the digital era, privacy is not simply the right to be left aloneit is the right to participate in society without the fear of constant and invisible monitoring.

The chilling effect of surveillance does not only restrict individual freedom; it also weakens democratic culture by discouraging dissent, reducing open debate, and limiting meaningful participation.

Judicial interventions remain a critical safeguard in this evolving landscape. Decisions such as Manohar Lal Sharma (Pegasus) and Nitin Bhatnagar reflect the judiciary's role in protecting constitutional values against unchecked digital power.

Ultimately, while Parliament may design the legal structure of the digital regime, the Constitution continues to serve as the central boundary that prevents governance from turning into digital control.

ISSN: 2582-6433

6. RECOMMENDATIONS

To ensure that India's data protection framework aligns with constitutional privacy and the broader goals of Human Rights 2.0, the following reforms are recommended:

(a) Judicial Warrant Requirement for State Access

The broad exemptions permitted under Section 17 should be narrowed and subjected to stronger procedural checks.

Where the State seeks access to personal data for reasons such as "public order" or similar grounds, such access should require prior judicial authorisation, ideally through a warrant issued by a designated magistrate or court. This would ensure that executive authorities do not act as the sole decision-makers in matters involving fundamental rights.

(b) Ensuring Statutory Independence of the Data Protection Board (DPB)

To reflect the spirit of the Justice Srikrishna Committee's recommendations, the Data Protection Board should be institutionally insulated from executive control.

Appointment processes, tenure protections, and funding mechanisms should be structured to support independence. A multi-stakeholder appointment model involving the judiciary and civil society can improve legitimacy and reduce the risk of political influence.

(c) Strengthening the Right to be Forgotten Through Clear Rules

The DPDP framework should provide clearer, enforceable procedures for the Right to Erasure, especially for individuals who have been acquitted, discharged, or exonerated.

Building on the reasoning applied in Nitin Bhatnagar (2025), India should develop rules for automated or streamlined de-indexing in appropriate cases. A "digital exoneration" mechanism would help ensure that online records do not permanently punish individuals after the legal system has cleared them.

(d) Narrow and Precise Definition of "National Security"

The term "national security" should not remain open-ended within Section 17.

A narrow statutory definition is necessary to prevent misuse and to ensure that the State cannot rely on vague language to bypass necessity and proportionality standards. Clear definitions also improve judicial review by allowing courts to evaluate whether the claim of national security is genuine and evidence-based.

(e) Removing Penalties That Discourage Citizens From Enforcing Rights

The DPDP Act's provisions relating to the duties of the Data Principal and penalties

ISSN: 2582-6433

for "frivolous" complaints should be reconsidered.

If individuals fear punishment for raising complaints, the enforcement structure becomes discouraging rather than empowering. Data protection regimes should reduce barriers to accountability, not create new deterrents that silence valid grievances.

BIBLIOGRAPHY AND REFERENCES

Cases:

1. M.P. Sharma v. Satish Chandra, (1954) S.C.R. 1077 (India).
2. Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
3. Govind v. State of Madhya Pradesh, A.I.R. 1975 S.C. 1378 (India).
4. People's Union for Civil Liberties (PUCL) v. Union of India, A.I.R. 1997 S.C. 568 (India).
5. Shreya Singhal v. Union of India, A.I.R. 2015 S.C. 1523 (India).
6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
7. Manohar Lal Sharma v. Union of India, (2022) 3 S.C.C. 25 (India).
8. Nitin Bhatnagar v. ANI Media Pvt. Ltd., C.S. No. 510/2025 (Patiala House Ct. Nov. 10, 2025) (India).
9. IE Online Media Services (P) Ltd. v. Nitin Bhatnagar, 2025 S.C.C. OnLine Del 9281 (India).

Statutes / Rules:

10. Information Technology Act, 2000
    Information Technology Act, No. 21 of 2000, India Code (2000).
11. Digital Personal Data Protection Act, 2023
    Digital Personal Data Protection Act, No. __ of 2023, India Code (2023).
12. Digital Personal Data Protection Rules, 2025
    Digital Personal Data Protection Rules, 2025, Gazette Notification (14 Nov. 2025) (India).

Reports / Committee Documents:

13. Comm. of Experts on Data Prot., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018). (Justice Srikrishna Committee Report)

ISSN: 2582-6433

Statistics / Data:

14. Internet Statistics 2025: Usage, Speed, and Connectivity Insight, SQ Magazine
15. (Jan. 2025) (5.53 billion global users).
16. Digital 2025: India, Datareportal (Feb. 25, 2025) (806 million users).
17. India's internet user base to exceed 900 million by 2025, IBEF (Jan. 17, 2025). DPDP Rules Notification
18. Digital Personal Data Protection Rules, 2025, Gazette Notification (14 Nov. 2025) (India).