INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

‘‘EVOLVING DIMENSIONS OF DIGITAL PRIVACY UNDER ARTICLE 21: A SOCIO-LEGAL PERSPECTIVE’’

AUTHORED BY - ANCY DORSHIA M[1],
JOYLIN JACOB Y[2] & AALAN JOE EDWIN[3]

ABSTRACT

This paper undertakes a comprehensive examination of the evolving concept of digital privacy as an intrinsic component of the right to life and personal liberty guaranteed under Article 21 of the Indian Constitution. In an era characterized by pervasive digitalization, algorithmic governance, and data-driven decision-making, the boundaries of constitutional privacy have expanded beyond traditional notions of physical and spatial autonomy. The study argues that Article 21 must be dynamically interpreted to encompass informational autonomy, technological self-determination, and digital dignity, thereby aligning constitutional jurisprudence with the realities of the digital age.

Tracing the constitutional trajectory from Kharak Singh v. State of Uttar Pradesh (1962) to the landmark Justice K.S. Puttaswamy v. Union of India (2017) judgment, this paper explores the three foundational dimensions of privacy bodily integrity, informational autonomy, and decisional freedom as articulated by the Supreme Court. It critically investigates the threats posed by surveillance capitalism, biometric profiling under the Aadhaar framework, intrusive AI-based analytics, algorithmic bias, and state-sponsored surveillance tools such as Pegasus spyware and facial recognition technologies.

The paper further evaluates the limitations of the Digital Personal Data Protection Act, 2023, especially its lack of robust institutional oversight, narrow consent architecture, and potential state exemptions, contrasting these with the European Union’s General Data Protection Regulation (GDPR) to underscore the need for a more rights-centric approach. Judicial

[1] Author- ANCY DORSHIA*
Research scholar in Dr MGR Educational and Research Institute at school of law/ Assistant Professor in Mugil college of Law, Tamil Nadu
[2] Co-Author: JOYLIN JACOB Y* Research scholar in Bharath Institute of Higher Education and Research at school of law/ Assistant Professor in Mugil college of Law, Tamil Nadu
[3]Co-Author- AALAN JOE EDWIN* Assistant Professor in Mugil college of Law, Tamil Nadu

ISSN: 2582-6433

responses through Public Interest Litigations (PILs) and constitutional review mechanisms are assessed to determine the judiciary's evolving role in balancing innovation with individual liberties.

Finally, the study advances a set of policy and judicial recommendations, including the establishment of specialized data protection benches, mandatory technological training for judicial officers, and enhanced accountability frameworks for both public and private data fiduciaries. It concludes that safeguarding digital privacy is not merely a matter of data protection but a constitutional imperative central to human dignity, autonomy, and democratic governance.

Thus, Article 21 must continue to evolve as a living instrument capable of protecting citizens in a technologically mediated society.

Key-Terms: Judicial Review, Public Interest Litigation, Technological Governance, Human Dignity, Artificial Intelligence, Biometric Data, Data Protection

INTRODUCTION

The digital revolution has profoundly reshaped the contours of personal liberty, ushering in an era where data is both a resource and a risk. In India, the proliferation of biometric authentication systems, ubiquitous mobile connectivity, and algorithmic governance mechanisms has created a complex ecosystem of surveillance and datafication. Citizens now navigate a digital landscape where every interaction—from Aadhaar-based identity verification and Unified Payments Interface (UPI) transactions to social media engagement and location tracking—generates a persistent data trail. This trail, often invisible and involuntary, is susceptible to profiling, commodification, and misuse by both state and private actors.

Against this backdrop, the constitutional guarantee under Article 21 [4]of the Indian Constitution which enshrines the right to life and personal liberty demands a renewed interpretation. Traditionally associated with physical liberty and procedural fairness, Article 21 must now evolve to encompass the nuanced dimensions of digital privacy, informational autonomy, and the right to be forgotten. The Supreme Court's landmark judgment in *Justice K.S. Puttaswamy*

[4] CONSTITUTION OF INDIA ARTICLE 21

ISSN: 2582-6433

(Retd.) v. Union of India (2017) [5]marked a pivotal moment in this evolution, affirming privacy as a fundamental right intrinsic to human dignity. However, the jurisprudential journey remains incomplete, especially in the face of emerging threats such as AI-driven surveillance, predictive policing, and opaque data governance frameworks.

This paper argues that safeguarding digital dignity is not merely a technological or regulatory challenge it is a constitutional imperative. It critically examines how Indian jurisprudence has responded to the digital transformation of personal liberty, tracing key judicial pronouncements, legislative developments, and policy debates. The study also interrogates the gaps in existing legal frameworks, including the limitations of the Information Technology Act, 2000 [6]and the evolving contours of the Digital Personal Data Protection Act, 2023.[7]

By situating digital rights within the broader framework of constitutional morality and democratic accountability, the paper proposes a set of reforms aimed at strengthening informational self-determination. These include judicial guidelines for data minimization, statutory recognition of algorithmic transparency, and the establishment of independent data protection authorities with robust oversight powers. Ultimately, the paper seeks to contribute to a jurisprudence of digital liberty one that affirms the citizen's right to exist, express, and evolve freely in a data-driven society.

CONSTITUTIONAL FOUNDATION OF PRIVACY IN INDIA

The constitutional recognition of privacy in India has undergone a profound jurisprudential transformation from a marginal concern in early surveillance cases to a central pillar of the right to life and personal liberty under Article 21 of the Indian Constitution. This evolution reflects the judiciary's increasing awareness of the shifting nature of liberty in a digitally networked society, where the boundaries between the public and private spheres are constantly being renegotiated.

[5] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[6] The Information Technology Act, 2000
[7] The Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

EARLY JUDICIAL ENGAGEMENT: THE SEEDS OF PRIVACY

The first significant judicial engagement with the concept of privacy emerged in *Kharak Singh v. State of Uttar Pradesh* (1962)[8], a case that challenged the constitutional validity of police surveillance regulations under the Uttar Pradesh Police Regulations. The majority of the Supreme Court held that the right to privacy was not a guaranteed fundamental right under the Constitution. However, Justice Subba Rao's powerful dissent laid the doctrinal foundation for future developments. He argued that unauthorized intrusion into a person's home and private life violated the sanctity of personal liberty under Article 21. His dissent emphasized that liberty is not merely the absence of physical restraint but includes the right to be let alone a sentiment that would echo in later privacy jurisprudence.

This early tension between majoritarian restraint and minority foresight illustrates how privacy, though initially peripheral, was already gestating as a constitutional value. The dissent in *Kharak Singh* would later be vindicated and elevated to constitutional orthodoxy.

THE PUTTASWAMY PARADIGM: PRIVACY AS A FUNDAMENTAL RIGHT

The jurisprudential landscape shifted dramatically with the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)[9]. In this case, a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution, particularly under Article 21. The Court overruled earlier decisions such as *M.P. Sharma* (1954) and *Kharak Singh* (to the extent of the majority view), affirming that privacy is not merely a derivative right but an intrinsic and inalienable component of the right to life and personal liberty.

The Court's reasoning was deeply rooted in constitutional morality, human dignity, and the evolving nature of liberty. It recognized that privacy is essential for the realization of autonomy, freedom of thought, bodily integrity, and the ability to make personal choices without coercion. The judgment also emphasized that the Constitution is a living document, and its interpretation must adapt to the changing realities of society—especially in the face of technological advancements that enable unprecedented surveillance and data collection.

[8] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[9] K.S. Puttaswamy (Retd.) v. Union of India (2017)

ISSN: 2582-6433

THE THREEFOLD DIMENSIONS OF PRIVACY

The *Puttaswamy* judgment articulated a tripartite framework for understanding privacy, each dimension carrying distinct constitutional implications:

- **Bodily Integrity**: This dimension protects individuals from physical intrusions and coercive state actions. It encompasses the right to refuse medical treatment, protection against custodial violence, and safeguards against compulsory biometric data collection. In the digital context, it raises critical questions about the voluntariness of biometric authentication systems like Aadhaar and the potential for bodily surveillance through wearable technologies and facial recognition.
- **Informational Autonomy**: Perhaps the most relevant in the digital age, this aspect of privacy affirms the individual's right to control the collection, storage, processing, and dissemination of personal data. It challenges the unchecked expansion of state and corporate surveillance, data mining, and algorithmic profiling. Informational autonomy forms the normative basis for data protection laws, including the recently enacted **Digital Personal Data Protection Act, 2023 (DPDP Act)**[10], and aligns with global standards such as the EU's General Data Protection Regulation (GDPR).
- **Decisional Freedom**: This dimension safeguards the individual's right to make intimate and personal decisions without undue interference. It includes choices related to reproductive rights, sexual orientation, religious beliefs, and digital expression. In the online realm, it extends to the freedom to curate one's digital identity, express dissent, and access information without fear of profiling or censorship.

TOWARDS A DIGITAL CONSTITUTIONALISM

Together, these dimensions construct a robust and dynamic constitutional framework for privacy in India. The *Puttaswamy* judgment not only affirms privacy as a fundamental right but also provides a normative compass for navigating the challenges posed by digital surveillance, algorithmic governance, and data capitalism. It mandates that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality thus placing substantive limits on state and corporate power.

In essence, the judgment serves as the constitutional bedrock for contemporary debates on digital privacy, data protection, and informational self-determination. It calls for a rights-based

[10] Digital Personal Data Protection Act, 2023 (DPDP Act)

ISSN: 2582-6433

approach to digital governance, where the dignity and autonomy of the individual are placed at the centre of technological development and regulatory design.

Digital Ecosystem and Threats to Privacy in India

India's rapid digital transformation has brought convenience, connectivity, and innovation to millions. Yet, beneath this progress lies a growing concern: the erosion of privacy through pervasive data collection, opaque algorithms, and inadequate safeguards. As digital interactions become integral to everyday life, the constitutional right to privacy—affirmed under Article 21—faces unprecedented threats.

Surveillance Capitalism: Monetizing Human Experience

Surveillance capitalism, a term popularized by Shoshana Zuboff, describes an economic model where tech companies extract behavioural data to predict and influence user behaviours. In India, platforms like Google, Meta, and Amazon routinely track:

- Browsing history, app usage, location data, and purchase patterns
- User interactions across devices and platforms, often without explicit consent

This data is fed into AI-driven predictive systems that shape advertisements, content feeds, and even political messaging. The lack of transparency and informed consent undermines informational autonomy and can lead to:

- Behavioural manipulation
- Profiling based on caste, religion, or socio-economic status
- Exclusion from services or opportunities due to algorithmic targeting

Such practices commodify personal data, turning citizens into products and eroding their autonomy.

Aadhaar Infrastructure: Between Inclusion and Surveillance

India's Aadhaar system, the world's largest biometric ID program, was designed to streamline access to welfare and services. However, it also centralizes sensitive biometric data fingerprints, iris scans, and demographic details raising serious privacy concerns:

- Data breaches and unauthorized access have been reported, despite encryption protocols
- Mandatory Aadhaar linkage for services like banking, SIM cards, and school admissions has led to coercive data collection

ISSN: 2582-6433

- Potential misuse for surveillance, especially in law enforcement and predictive policing contexts

While the Supreme Court upheld Aadhaar's constitutionality in Puttaswamy (II) (2018), it imposed restrictions on its use. Yet, implementation gaps persist, and the risk of function creep—where data collected for one purpose is used for another—remains high.

AI and Algorithmic Bias: Invisible Discrimination

Artificial Intelligence now influences decisions in critical sectors—credit scoring, recruitment, healthcare, and policing. However, these systems often inherit biases from the data they are trained on:

- Historical discrimination in datasets can lead to biased outcomes (e.g., caste-based exclusion in hiring algorithms)
- Opaque decision-making makes it difficult to challenge or understand automated rejections
- Lack of accountability for AI errors or harms, especially in law enforcement and predictive analytics

For instance, facial recognition systems have shown higher error rates for darker-skinned individuals, raising concerns about disproportionate targeting of SC/ST communities. Without algorithmic transparency and audit mechanisms, AI can reinforce systemic inequalities under the guise of efficiency

Case Studies

• **Pegasus Spyware**: This military-grade software was allegedly used to secretly monitor journalists, activists, and public figures. It raised serious questions about unlawful surveillance and violation of privacy.

• **Facial Recognition Technology**: Cameras in public places can now identify people using

facial recognition. Without proper legal rules, this can lead to mass surveillance and loss of anonymity in public spaces. These examples show that digital tools, if not properly regulated, can weaken constitutional protections. They highlight the urgent need for stronger laws, better safeguards, and public awareness to ensure that technology respects individual rights.

ISSN: 2582-6433

COMPARATIVE JURISPRUDENCE: INDIA, EU, AND GLOBAL NORMS

In the age of data-driven governance, comparative legal analysis offers valuable insights into how different jurisdictions conceptualize and protect digital privacy. India's Digital Personal Data Protection Act, 2023 (DPDP Act)[11] marks a foundational step toward regulating personal data, but its normative and structural limitations become evident when juxtaposed with the European Union's General Data Protection Regulation (GDPR) and the United States' Fourth Amendment jurisprudence. This section critically examines these frameworks, highlighting gaps in enforcement, consent architecture, and algorithmic transparency.

□□ India's DPDP Act, 2023: A Rights-Affirming but Power-Conceding Framework

The DPDP Act was enacted in response to the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). It introduces principles such as consent-based processing, data minimization, and grievance redressal. However, the Act suffers from several structural and normative deficiencies:

- Enforcement Weakness: The Data Protection Board of India lacks institutional independence. Its composition and oversight are controlled by the central government, raising concerns about executive influence and regulatory capture.
- Vague Exemptions: Terms like "public interest," "national security," and "legitimate use" are undefined, allowing broad and discretionary data access by state actors.
- Limited Algorithmic Oversight: The Act does not mandate transparency in automated decision-making or profiling, leaving individuals vulnerable to opaque and potentially discriminatory systems.

These gaps dilute the constitutional promise of informational autonomy under Article 21 and risk normalizing surveillance practices without adequate checks.

EU'S GDPR: A GOLD STANDARD FOR DATA PROTECTION

The General Data Protection Regulation (GDPR), effective since 2018[12], is widely regarded as the most comprehensive data protection law globally. It is grounded in the Charter of Fundamental Rights of the European Union, particularly Article 8, which guarantees the protection of personal data.

[11] India's Digital Personal Data Protection Act, 2023 (DPDP Act)
[12] The General Data Protection Regulation (GDPR)2018

ISSN: 2582-6433

Key strengths of the GDPR include:

- Independent Regulators: Data Protection Authorities (DPAs) operate autonomously, ensuring impartial enforcement.
- Explicit Consent Architecture: Consent must be freely given, specific, informed, and revocable. Pre-ticked boxes and bundled consents are prohibited.
- Algorithmic Transparency: Individuals have the right to explanation in automated decision-making under Article 22, including the logic involved and potential consequences.
- Heavy Penalties: Non-compliance can attract fines up to €20 million or 4% of global turnover, creating strong deterrence.

The GDPR's emphasis on accountability, transparency, and user empowerment stands in contrast to India's more state-centric and discretionary model.

□□ US Fourth Amendment Jurisprudence: Privacy as Protection from State Intrusion

The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures. While it does not explicitly mention data privacy, courts have interpreted it to include digital surveillance and metadata collection.

Notable developments include:

- Carpenter v. United States (2018)[13]: The Supreme Court held that accessing historical cell-site location data without a warrant violates the Fourth Amendment.
- Katz v. United States (1967)[14]: Introduced the "reasonable expectation of privacy" test, which has been extended to digital communications.
- Digital Rights Ireland v. Minister for Communications (CJEU): Though a European case, it resonates with US concerns. The Court of Justice of the European Union struck down blanket data retention laws, affirming that indiscriminate surveillance violates fundamental rights.

While the US lacks a unified data protection law like the GDPR, its constitutional jurisprudence offers robust protections against state overreach, especially in criminal and surveillance contexts.

Comparative Gaps

[13]Carpenter v. United States (2018)
[14] Katz v. United States (1967)

ISSN: 2582-6433

The comparative analysis reveals three critical gaps in India's data protection regime:

1. Enforcement Architecture: Unlike the GDPR's independent regulators, India's Data Protection Board is vulnerable to executive control.
2. Consent Mechanisms: India's model allows for broad exemptions and lacks granular consent protocols, undermining user autonomy.
3. Algorithmic Accountability: India does not require transparency in automated decision-making, leaving citizens exposed to profiling and discrimination without recourse.

To align with global norms and fulfill the constitutional mandate of Article 21, India must:

- Define and limit exemptions through statutory clarity and judicial oversight.
- Empower regulators with structural independence and investigative powers.
- Introduce algorithmic audit requirements and rights to explanation in automated systems.

LEGISLATIVE LANDSCAPE: EVALUATING THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive attempt to regulate personal data in the digital age. It was introduced in response to the Supreme Court's affirmation of privacy as a fundamental right in the *Puttaswamy* judgment. The Act outlines several key protections:

- It mandates that personal data must be processed only with the individual's consent, which must be free, informed, specific, and unambiguous.
- It introduces the principle of data minimization, requiring that only necessary data be collected for a clearly defined purpose.
- It grants individuals rights to access, correct, and erase their personal data, and to file complaints with the Data Protection Board.
- It allows cross-border data transfers to countries notified by the central government.
- It includes special provisions for children's data, requiring parental consent for processing.

Despite these progressive features, the Act has drawn criticism for several reasons. First, it uses vague terms such as "public interest" and "legitimate use" without defining them clearly. This opens the door to broad and potentially arbitrary interpretations, especially by state agencies. Second, the enforcement mechanism the Data Protection Board of India—is not fully

ISSN: 2582-6433

independent. Its members are appointed by the central government, raising concerns about political influence and lack of institutional autonomy. Third, the Act provides minimal safeguards against government surveillance. It does not require judicial or parliamentary oversight for data collection by state actors, nor does it mandate transparency in surveillance practices.

In contrast, the European Union's General Data Protection Regulation (GDPR) offers a more robust framework. It requires explicit and revocable consent, establishes independent data protection authorities, and imposes heavy penalties for violations. The GDPR also includes rights such as data portability, the right to object to profiling, and the right to explanation in automated decision-making—all of which are absent or weakly defined in India's DPDP Act.

This comparison underscores the need for India to strengthen its privacy law. To truly protect digital rights under Article 21, the law must be grounded in constitutional principles of proportionality, transparency, and accountability.

JUDICIAL RESPONSES AND STRUCTURAL LIMITATIONS

Indian courts have played a pivotal role in shaping digital privacy jurisprudence. Through Public Interest Litigations (PILs), citizens have challenged issues such as unauthorized surveillance, data breaches, and algorithmic discrimination. The judiciary has responded with landmark decisions that affirm privacy as a constitutional right and impose limits on state power.

For instance, in ***PUCL v. Union of India***[15]**,** the Supreme Court laid down procedural safeguards for telephone tapping, emphasizing the need for judicial oversight. In ***Puttaswamy v. Union of India*****, the Court** recognized privacy as intrinsic to human dignity and liberty. In *Anuradha Bhasin v. Union of India*, the Court held that internet access is essential for freedom of speech and trade, indirectly reinforcing digital rights.

However, courts face significant challenges in adjudicating digital rights cases. One major hurdle is the technical complexity of digital systems. Judges often lack training in emerging technologies such as artificial intelligence, encryption, and data analytics. This can lead to

[15] PUCL v. Union of India

ISSN: 2582-6433

reliance on government narratives or technical experts without independent scrutiny.

Another challenge is the absence of specialized benches or procedural frameworks for handling digital rights cases. Most cases are heard by general benches, which may not have the expertise or bandwidth to engage deeply with technological nuances. Moreover, there is limited jurisprudence on algorithmic accountability, making it difficult to assess the legality of automated decisions.

To address these limitations, the paper proposes several reforms. First, judges should receive structured training in digital law and technology through judicial academies and continuing education programs. Second, High Courts and the Supreme Court should establish dedicated Digital Rights Benches to handle tech-intensive cases. Third, courts should mandate judicial review of automated systems used in public services, law enforcement, and financial decision-making. This includes requiring transparency in algorithmic logic and ensuring that individuals have the right to challenge automated outcomes.

By strengthening judicial capacity and procedural safeguards, India can ensure that its courts remain effective guardians of privacy and liberty in the digital age.

Conclusion

This paper concludes that in the digital age, the right to privacy is no longer a peripheral concern—it is the very fulcrum upon which personal liberty, autonomy, and dignity rest. Privacy is not merely about protecting data from unauthorized access; it is about safeguarding the individual's right to exist freely, think independently, and make personal choices without coercion or surveillance. In a society increasingly governed by algorithms, biometric identifiers, and predictive analytics, the contours of liberty must be redrawn to include informational autonomy as a core constitutional value.

Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty, must evolve to meet the challenges of a data-driven society. The Supreme Court's recognition of privacy as a fundamental right in *Justice* ***K.S. Puttaswamy (Retd.) v. Union of India*** **(2017)** was a landmark affirmation of this principle. However, the journey from recognition to realization remains incomplete. The digital ecosystem—marked by surveillance capitalism, biometric centralization, and algorithmic bias—continues to expose citizens to risks that

ISSN: 2582-6433

threaten their constitutional protections.

To truly uphold the spirit of Article 21 in the digital era, India must move beyond abstract declarations and embrace concrete reforms. The future of liberty lies in recognizing that informational autonomy is as vital as physical freedom, and that digital dignity must be protected with the same Vigor as bodily integrity or freedom of speech.

SUGGESTIONS AND RECOMMMEDATIONS

To operationalize this constitutional vision, the following reforms are proposed:

1. Strengthen Legislative Safeguards

- Amend the Digital Personal Data Protection Act, 2023 to define vague terms like "public interest" and "legitimate use" with precision.
- Introduce judicial and parliamentary oversight for government surveillance programs.
- Mandate algorithmic transparency, especially in public sector decision-making.

2. Empower Regulatory Institutions

- Ensure the Data Protection Board of India is structurally independent, with transparent appointments and review mechanisms.
- Establish a Digital Rights Ombudsman to address citizen grievances and monitor compliance.

3. Enhance Judicial Capacity

- Create Digital Rights Benches in High Courts and the Supreme Court to handle tech-intensive cases.
- Provide technical training for judges, enabling informed adjudication of AI, encryption, and data governance issues.
- Mandate judicial review of automated systems, especially those used in law enforcement, welfare distribution, and financial services.

4. Promote Public Awareness and Digital Literacy

- Launch community outreach programs to educate citizens on their digital rights and privacy protections.
- Integrate digital ethics and privacy modules into school and university curricula.
- Encourage civil society participation in shaping data governance policies.

5. Foster International Alignment

- Align India's data protection framework with global standards such as the EU's GDPR, ensuring cross-border compatibility and investor confidence.

ISSN: 2582-6433

- Participate in international dialogues on AI ethics, privacy, and digital sovereignty.

References:

- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119)1.
- SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* (PublicAffairs 2019).
- Internet Freedom Foundation, *Pegasus Project: Surveillance and the Right to Privacy*, *https://internetfreedom.in* (last visited Nov. 6, 2025).
- NITI Aayog, *Responsible AI for All: Strategy Document* (June 2021), https://niti.gov.in.
- Indian Journal of Law and Technology, *Judicial Interpretation and Data Rights in India: From Puttaswamy to the DPDP Act, 2023*, *https://ijilt.in* (last visited Nov. 6, 2025).
- Drishti Singh, *The Right to Privacy in India's Digital Era: A Post-Puttaswamy Perspective*, 3 INT'L J. LEGAL SOC. SCI. STUD. 634 (2023), *https://ijlsss.com*
- Int'l J. Legal Res. & Pol'y, *The Right to Privacy Under Article 21: Implications of the DPDP Act*, *https://www.ijlrp.com* (last visited Nov. 6, 2025).