Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1958–1969

RECALIBRATING THE RIGHT TO PRIVACY IN THE DIGITAL AGE: LEGAL CHALLENGES AND CONSTITUTIONAL SAFEGUARDS IN THE ERA OF TECHNOLOGICAL INTRUSION

Rachna Yadav[1*], Dr. Rahul Varshney[2]

[1] Ph.D. Scholar, MVN University
[2] Dean, School of Law, MVN University, Haryana

DOI
10.29121/shodhkosh.v5.i6.2024.5121

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The right to privacy started as a secondary constitutional matter before it elevated to basic status because of technological advancements. The constitution of India witnessed a major transformative moment following the decision made in Justice K.S. Puttaswamy v. Union of India [1]. The 2017 Union of India (2017) decision legitimized privacy protections under the purview of Article 21. The digital age has introduced multiple sophisticated threats to privacy rights which cover both corporate information collection through AI systems and state-level surveillance and predictive law enforcement. The paper explores privacy law development while assessing protection mechanisms in the constitution and statutes alongside investigating fresh technology hurdles. The research uses GDPR standards together with the American sectoral model in a comparative analysis to show that existing legal norms require adjustment. The paper advocates for extensive regulatory structures together with ethical governance systems and court-based privacy protections because technological surveillance has become commonplace.

Keywords: Right to Privacy, Digital Age, Surveillance, Artificial Intelligence, Data Protection, Constitutional Law, Puttaswamy Judgment, GDPR, Privacy Jurisprudence, Technological Intrusion

1. INTRODUCTION

1.1. BACKGROUND AND CONTEXT

Despite our digital era society the right to privacy stands both vital and in constant danger. As digital technology spreads wide-reaching its control the fundamental value of privacy grew from its peripheral civil liberty position in traditional democracy to become a core element of democratic constitutionalism. The unlimited availability of smartphones along with biometric systems and data analytics and surveillance cameras and artificial intelligence reveals new privacy threats to individuals. In India, the recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017)[2] marked a significant constitutional milestone[3]. However, this recognition must now

[1]. Justice K.S. Puttaswamy vs. Union of India, 2017 10 SCC1
[2]. Ibid.
[3]. Chandrachud, D. Y. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*. Supreme Court of India, W.P. (Civil) No. 494 of 2012.

be tested against the challenges posed by state surveillance programs, corporate data monetization, as well as algorithmic profiling.

1.2. OBJECTIVES OF THE STUDY

This research aims to:

- Examine the evolution and scope of the right to privacy in India.
- Analyse legal and constitutional safeguards against digital-age intrusions.
- Evaluate the adequacy of current statutory frameworks, including the Digital Personal Data Protection Act, 2023.
- Explore comparative international legal standards for privacy protection.
- Suggest legal reforms and regulatory mechanisms to protect privacy in the digital ecosystem.

1.3. METHODOLOGY

The research employs a doctrinal legal research methodology, analysing constitutional provisions, landmark judgments, statutes, as well as legal commentaries. Additionally, it adopts a comparative legal research approach to study best practices from international jurisdictions such as the EU, USA, and UK (Sarat & Silbey, 1988)[4]. Secondary sources, including scholarly articles, law commission reports, and official policy documents, are critically examined to understand the evolving nature of the right to privacy.

2. CONCEPTUAL FRAMEWORK OF THE RIGHT TO PRIVACY

2.1. DEFINITION AND DIMENSIONS OF PRIVACY

The concept of privacy is inherently complex as well as multidimensional, extending beyond the mere right to be left alone. Alan Westin[5] defined privacy as the "claim of individuals to determine for themselves when, how, as well as to what extent information about them is communicated to others." This seminal understanding laid the foundation for modern privacy jurisprudence. Daniel J. Solove (2006)[6] expanded the scope by emphasizing privacy as a series of interconnected harms, such as surveillance, information processing, and dissemination, rather than a single definable interest. Privacy encompasses decisional autonomy, personal integrity, and control over personal data, forming a critical component of individual dignity and liberty (Regan, 1995)[7].

2.2. EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

India's constitutional recognition of the right to privacy has been gradual. The Supreme Court first adopted a limited viewpoint in Kharak Singh v. State of Uttar Pradesh[8], rejecting privacy as a fundamental right. This position was ultimately changed, most notably in Gobind v. State of Madhya Pradesh[9], when the Court acknowledged a penumbral right to privacy under Article 21. In the historic ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India[10], a nine-judge panel unanimously concluded that, in accordance with Article 21 of the Indian Constitution, the right to privacy is inextricably linked to the right to life and personal liberty (Chandrachud, 2017)[11]. By confirming privacy as a

[4]. Sarat, A and Silbey, S.S., "The pull of the policy audience",10(2-3) Law and Policy 97-166 (1988)
[5]. Westin, Alan F., Privacy and Freedom, Atheneum, New York, 1967.
[6] . Solove, Daniel J., "A Taxonomy of Privacy", 154 U. Pa. L. Rev. 477 (2006)
[7]. Regan, Priscilla M., Legislating Privacy: Technology, social values, and public policy, University of North Carolina Press, Chapel Hill (1995)
[8]. Kharak Singh vs. State of Uttar Pradesh (1962) AIR 1963 SC 1295
[9]. Govind vs. State of Madhya Pradesh, 1955 CrLJ 1275
[10]. Justice K.S. Puttaswamy vs. Union of India, 2017 10 SCC 1
[11]. Chandrachud, D. Y. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*. Supreme Court of India, W.P. (Civil) No. 494 of 2012.

multifaceted right that includes autonomy, dignity, and physical integrity, the ruling signalled a turning point in the constitution (Narayanan, 2018)[12].

2.3. INTERNATIONAL HUMAN RIGHTS STANDARDS ON PRIVACY (UDHR, ICCPR, ECHR)

International human rights standards state that privacy rights have continuously maintained their fundamental nature. Every individual has the right to be free from arbitrary violations of their privacy, family life, place of residence, or private communications, as stated in Article 12 of the 1948 Universal Declaration of Human Rights. The right to fight against unlawful assaults on one's own honour and reputation is protected under Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR). Article 8 of the European Convention on Human Rights (ECHR) guarantees the right to respect for one's "private and family life, home, and correspondence," which the European Court of Human Rights has broadly construed to include defence against biometric collection, surveillance, and data misuse (Helfer & Slaughter, 1997)[13]. These global norms emphasize that privacy is indispensable for human dignity and democratic participation (Bennett & Raab, 2006)[14].

2.4. DISTINCTION BETWEEN INFORMATIONAL, BODILY, AND SPATIAL PRIVACY

Informational privacy, physiological privacy, and geographical privacy are the three main categories into which privacy may be divided. Control over personal information and dissemination is known as informational privacy. It is particularly relevant in the digital age where data collection as well as surveillance systems pose significant threats (Solove, 2008)[15]. Bodily privacy encompasses the right to personal autonomy over one's body, including decisions related to reproduction, health, and bodily integrity, as emphasized in cases like *Suchita Srivastava v. Chandigarh Administration* (2009)[16]. Spatial privacy relates to the sanctity of private spaces such as one's home or workplace and the protection from unwarranted intrusions, both physical and digital (Wacks, 2010)[17]. These dimensions are interconnected and foundational to understanding privacy as a holistic right rather than a fragmented entitlement.

3. TECHNOLOGICAL INTRUSIONS AND EMERGING CHALLENGES

3.1. SURVEILLANCE TECHNOLOGIES (CCTV, FACIAL RECOGNITION, DRONES)

The proliferation of surveillance technologies such as closed-circuit television (CCTV), facial recognition systems (FRS), as well as drones has led to widespread monitoring of public and private spaces. In India, cities like Delhi and Hyderabad are among the most surveyed globally, raising concerns about mass surveillance without adequate legal frameworks (Banisar, 2011)[18]. Facial recognition, in particular, has been critiqued for its lack of consent-based use, high error rates—especially among marginalized groups—and potential misuse by state actors (Garvie et al., 2016)[19]. The Supreme Court in *Puttaswamy* recognized that surveillance must meet the tests of legality, necessity, as well as proportionality, yet the implementation of facial recognition and drone surveillance often bypasses these constitutional safeguards (Chandrachud, 2017)[20].

[12]. Lundberg, Ian, Narayanan, Arvind, Levy, Karen, and Salganik, Matthew. "Privacy, Ethics, and Data Access: A Case study of the Fragile Families Challenge" Socius: Sociological Research for a Dynamic World, vol. 4, 2018, pp. 1-13.
[13]. Helfer, L. R., & Slaughter, A. M. (1997). Toward a theory of effective supranational adjudication. *The Yale Law Journal*, 107(2), 273–391.
[14]. Bennett, Colin J. and Raab, Charles D., The Governance of Privacy: Policy Instruments in Global Perspective, 2nd edition, MIT Press, Cambridge, MA (2006)
[15]. Solove, Daniel J., Understanding Privacy, Harvard University Press, Cambridge, MA (2008)
[16]. Suchita Srivastava and another vs. Chandigarh Administration, (2009) 9 SCC 1
[17]. Wacks, Raymond, Privacy: A Very Short Introduction, Oxford University Press, Oxford (2010)
[18]. Banisar, David, The Right to Information and Privacy: Balancing Rights and Managing Conflicts, World Bank Institute Governance Working Paper Series, World Bank, Washington, DC (2011)
[19]. Garvie, Clare, Bedoya, Alvaro and Frankle, Jonathan, The Perptual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy and Technology at Georgetown Law, Washington DC (2016)
[20]. Supra, 4.

3.2. DATA MINING, SOCIAL MEDIA, AND BIG DATA ANALYTICS

With the advent of Web 2.0 platforms, the volume of personal data generated online has increased exponentially. Social media platforms collect vast amounts of user data, often through opaque terms of service and cookies (Tufekci, 2015)[21]. Data mining and big data analytics allow companies and governments to profile individuals, predict behavior, and even influence decision-making processes, as witnessed in the Cambridge Analytica scandal (Isaak & Hanna, 2018)[22]. The lack of comprehensive data protection laws exacerbates the risk of commodification of user data. This phenomenon not only undermines informational privacy but also threatens democratic discourse and autonomy (Zuboff, 2019)[23].

3.3. ARTIFICIAL INTELLIGENCE AND PREDICTIVE ALGORITHMS

Artificial Intelligence (AI) has brought a paradigm shift in how personal data is processed as well as utilized. Predictive policing algorithms, credit scoring systems, and automated hiring tools operate with limited transparency, often embedding biases and errors (Eubanks, 2018)[24]. These systems make critical decisions based on datasets that may not have been consensually collected or appropriately anonymized, violating the principles of fairness and accountability (Crawford & Paglen, 2019)[25]. In the Indian context, concerns over AI-driven surveillance in law enforcement and welfare schemes such as Aadhaar have highlighted the urgent need for ethical frameworks and legal safeguards (Ramanathan, 2021)[26].

3.4. CYBERSECURITY AND DATA BREACHES

Cybersecurity lapses have become frequent, with major institutions, including banks, government portals, and healthcare providers, facing data breaches. In 2020 alone, India reportedly experienced over 1.16 million cybersecurity incidents (CERT-IN, 2021). These breaches expose sensitive personal data, leading to identity theft, financial fraud, as well as reputational harm. Despite the introduction of the Digital Personal Data Protection Act, 2023, enforcement mechanisms remain weak, and penalties are often insufficient to deter negligent practices. A strong cybersecurity infrastructure, coupled with individual data protection rights, is vital to securing informational privacy in the digital era (Solove & Citron, 2022)[27].

3.5. ROLE OF PRIVATE TECH GIANTS IN DATA HARVESTING

Multinational technology companies such as Meta, Google, and Amazon possess unprecedented access to user data through ecosystems that include search engines, social media, e-commerce, and smart devices. These corporations have built their business models around the surveillance capitalism framework, which involves tracking user behavior to tailor ads and influence user preferences (Zuboff, 2019)[28]. The lack of data localization and jurisdictional clarity allows these entities to evade domestic privacy laws. In India, the absence of robust regulatory oversight has allowed tech giants to monetize user data with minimal accountability, raising concerns over digital colonialism and consent-based data governance (Bhatia, 2020)[29].

---

21. Tufekci, Zeynep, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency", 13 Colo. Tech. L.J. 203 (2015)
22. Isaak, Jim and Hanna, Mina J., "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", 51 Computer 56 (2018)
23. Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York (2019)
24. Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile and Police punish the poor, St. Martin's Press, New York (2018)
25. Crawford, Kate and Paglen, Trevor, Excavating AI: The Politics of Images in Machine Learning Training Sets, (2019) available at https://excavating.ai/
26. Ramanathan, Usha, "Aadhaar and the Right to Privacy", 13 Indian J. Const. L. 1 (2021)
27. Solove, Daniel J. and Citron, Danielle Keats, "Privacy Harms", 102 B.U. L. Rev. 793 (2022)
28. Supra, 24.
29. Bhatia, Gautam, "India's Executive Response to COVID-19", The Regulatory Review, May 4, 2020, available at: https:/www.theregreview.org/2020/05/04/Bhatia-indias-executive-response-covi-19/

4. LEGAL FRAMEWORK GOVERNING PRIVACY IN INDIA

4.1. CONSTITUTIONAL RECOGNITION POST-*PUTTASWAMY* (2017)

The Supreme Court's ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India[30] marked a turning point in Indian privacy jurisprudence. The nine-judge panel unanimously ruled that the right to privacy is a fundamental right under Article 21 of the Constitution, constituting a component of the right to life and personal liberty (Chandrachud, 2017)[31]. The ruling underlined that privacy includes a variety of safeguards, such as decision-making autonomy, informational self-determination, and physical integrity. Inspired by international law such as the Canadian Charter and the European Court of Human Rights, it established the triple criteria of legality, need, and proportionality for any governmental interference into the right to privacy (Bhatia, 2018)[32]. But at the time, there was no specific privacy statute, thus the right was essentially aspirational.

4.2. THE INFORMATION TECHNOLOGY ACT, 2000 AND ITS AMENDMENTS

The Information Technology Act, 2000 (IT Act) remains the primary legislation addressing electronic data and cybersecurity in India. Sections 43A and 72A of the Act provide for compensation in cases of negligence in handling sensitive personal data and for unauthorized disclosure by intermediaries or service providers (Basheer, 2015)[33]. While these provisions acknowledge privacy concerns in digital spaces, they are limited in scope and lack comprehensive safeguards. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Section 43A apply only to corporate entities, thus leaving state actors largely unaccountable. Moreover, enforcement has been sporadic, and penalties under the Act are not strong enough to deter major breaches.

4.3. THE PERSONAL DATA PROTECTION BILL, 2019 (NOW DPDP ACT, 2023) – ANALYSIS AND GAPS

After years of deliberation and the Justice B.N. Srikrishna Committee Report (2018), India introduced the Digital Personal Data Protection Act, 2023 (DPDP Act) to create a legal regime governing the collection, processing, and storage of personal data. The Act introduces concepts like consent-based processing, data fiduciaries, as well as data principals, aligning to some extent with global standards like the GDPR (Mehta, 2023)[34]. However, it has drawn criticism for exempting government agencies from the purview of the law under broad grounds of national interest, thus weakening the principle of purpose limitation and proportionality (Ramanathan, 2023)[35]. Additionally, the implementation framework is inherently inadequate due to the lack of a robust as well as independent data protection body and the restricted mechanisms for user redressal.

4.4. SECTORAL REGULATIONS: UIDAI (AADHAAR), RBI GUIDELINES, TELECOMMUNICATION LAWS

Beyond general legislation, privacy in India is regulated through sector-specific frameworks. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 allows the use of biometric and demographic data for identification purposes, but has been challenged for enabling mass surveillance and data centralization (Khera, 2019)[36]. Although the Supreme Court, in the *Aadhaar* judgment (2018)[37], upheld the constitutional validity of Aadhaar, it has limited its use to welfare schemes and PAN-linking, thus, invalidating its mandatory use by private entities. The RBI has introduced data localization norms for payment system operators. Though telecom regulations mandate the

30. Supra 1
31. Supra 4
32. Bhatia, G. (2018). *The Transformative Constitution: A Radical Biography in Nine Acts*. HarperCollins India.
33. Basheer, S. (2015). India's Tryst with Data Privacy. *Indian Journal of Law and Technology*, 11(1), 1–18.
34. Mehta, P. B. (2023). A Fragile Promise: The Digital Personal Data Protection Act, 2023 and Constitutional Concerns. *India Forum*.
35. Supra 27.
36. Khera, R. (2019). Aadhaar and the Right to Privacy. *Seminar*, 713, 34–38.
37. Justice K. S. Puttaswamy (Retd.) and another vs. Union of India and others, (2019) 1 SCC 1.

retention of metadata, which has raised concerns over privacy violations through passive surveillance. Yet, the lack of unified oversight across these sectoral laws results in regulatory fragmentation and inefficiency in protecting user privacy.

5. JUDICIAL TRENDS AND KEY CASE LAWS

5.1. KHARAK SINGH V. STATE OF UTTAR PRADESH (1963)

The right to privacy entered the Indian constitutional discussion in Kharak Singh v. State of UP[38], when the petitioner challenged police surveillance practices under the Uttar Pradesh Police Regulations. The majority of the Supreme Court rejected privacy as a basic right since it was not specifically protected by the Constitution. But in a landmark dissent, Justice Subba Rao contended that unlawful entry into a person's house constituted a violation of "ordered liberty" as defined by Article 21. This dissent established the groundwork for later privacy jurisprudence, despite the fact that it was not recognised at the time (Austin, 2001)[39].

5.2. GOVIND V. STATE OF MADHYA PRADESH (1975)

In Govind v. State of Madhya Pradesh[40], the Supreme Court took a more nuanced stance. The Court did not specifically acknowledge privacy as a separate fundamental right, but it acknowledged that it may be inferred from Articles 19(1)(d) and 21. Justice Matthew said that the right to privacy was not absolute and might be restricted in the case of a strong governmental interest. This case marked the start of a balanced strategy which allowed for both legitimate restrictions and privacy protection.

5.3. JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA (2017)

The historic *Justice K.S. Puttaswamy v. Union of India*[41] case fundamentally altered Indian constitutional law by unanimously recognizing the right to privacy as a fundamental right embedded in Article 21 and flowing from the entire Part III of the Constitution. Justice D.Y. Chandrachud, delivering the lead opinion, stated that privacy includes decisional autonomy, bodily integrity, and informational self-determination (Chandrachud, 2017)[42]. The Court adopted the three-fold test of legality, necessity, and proportionality, heavily influenced by international jurisprudence. The judgment explicitly overruled previous rulings in *M.P. Sharma* and the majority opinion in *Kharak Singh*, firmly placing privacy within the ambit of fundamental rights (Bhatia, 2018)[43].

5.4. AADHAAR JUDGMENT (2018)

In K.S. Puttaswamy v. Union of India[44] (Aadhaar) Supreme Court decision validated the Aadhaar project by implementing restrictions to limit its scope. Justice A.K. Sikri supported the Aadhaar architecture through his majority opinion because he maintained data protection safeguards protected privacy rights. The Supreme Court blocked private entities from obtaining Aadhaar data and also specified that metadata storage requirements needed reduction. The ruling faced criticism because it weakened the proportionality standard that Puttaswamy (2017) established and did not implement proper safeguards according to Khera (2019)[45].

[38]. Kharak Singh vs. State of Uttar Pradesh, AIR 1963 SC 1295.
[39]. Austin, G. (2001). Working a Democratic Constitution: The Indian Experience. Oxford University Press.
[40]. Govind vs. State of Madhya Pradesh, AIR 1975 SC 1378
[41]. Supra 1.
[42]. Supra 4.
[43]. Supra 33.
[44]. Justice K. S. Puttaswamy (Retd.) and another vs. Union of India and others, (2019) 1 SCC 1.
[45]. Supra 37.

5.5. INTERNET FREEDOM FOUNDATION V. UNION OF INDIA (2020)

In Internet Freedom Foundation vs. Union of India the petitioners opposed facial recognition system (FRS) implementation because state agencies lacked proper legal authorization. The court proceedings have yet to conclude yet they exposed privacy risks associated with biometric monitoring alongside the essential requirement for data protection legislation. The petition uses Puttaswamy framework to demonstrate that unconstitutional conditions exist when government conducts mass surveillance without legal authorization. According to Ramanathan (2021)[46] the growing pattern demonstrates how civil society organizations resort to constitutional remedies to substantiate state digital rights infringements.

6. COMPARATIVE ANALYSIS: GLOBAL PRIVACY FRAMEWORKS

6.1. GENERAL DATA PROTECTION REGULATION (GDPR) – EUROPEAN UNION

The EU established the General Data Protection Regulation or GDPR as the leading global example of privacy protection through data regulation. It started enforcing this model of privacy law in 2018. GDPR functions under a framework comprised of eight principles, which include lawfulness, justice, accountability, openness, purpose limitation, data minimisation, correctness, and storage limitation and integrity (Voigt & Von dem Bussche, 2017)[47]. GDPR enables users to exercise multiple rights which include obtaining access to personal data, fixing data inaccuracies and requiring information disclosure and requesting erasure of their information also known as the "right to be forgotten." Additionally, it requires Data Protection Impact Assessments (DPIAs) and punishes non-compliance with severe fines for data controllers. Organisations throughout the world now handle data processing and user permission differently as a result of the regulation's focus on privacy by design and default (Kuner, 2020)[48]. For India, GDPR serves as a benchmark in enacting comprehensive, consent-driven data protection laws.

6.2. USA'S SECTORAL APPROACH AND FOURTH AMENDMENT RIGHTS

The United States employs a sectoral model, as opposed to the EU's omnibus approach, in which privacy is governed by a patchwork of laws like the Gramm-Leach-Bliley Act (GLBA), the Children's Online Privacy Protection Act (COPPA), as well as the Health Insurance Portability & Accountability Act (HIPAA). Although the U.S. Constitution does not expressly guarantee a right to privacy, courts have interpreted the Fourth Amendment, which forbids unjustified searches and seizures, to give certain privacy safeguards, mainly against governmental monitoring (Solove, 2008)[49]. However, the rise of surveillance programs like PRISM and corporate data collection practices has exposed significant privacy gaps (Greenwald, 2014)[50]. There is no overarching federal data protection authority, and consumer rights vary across states. This fragmented approach provides lessons for India on the perils of inadequate and inconsistent privacy protections across sectors.

6.3. SURVEILLANCE REFORMS IN THE UK AND CANADA

The countries of Canada as well as the United Kingdom have strengthened their privacy regulatory systems substantially. Under the Data Protection Act (2018) the United Kingdom implements GDPR requirements while localized enforcement falls under the authority of the Information Commissioner's Office (ICO) with strong supervisory powers. The British legal system has invalidated surveillance methods that create disproportionate invasions into privacy through ruling in Privacy International v. Investigatory Powers Tribunal[51]. The Investigatory Powers Tribunal of 2019 established judicial control of mass surveillance following an important in that case. Public sector entities like Canada's Government must follow the Privacy Act (1983) in combination with the Personal Information Protection and Electronic

[46]. Supra 27.
[47]. Voigt, Paul and von dem Bussche, Axel, The EU General Data Protection Regulation (GDPR): A Practical guide,1st ed., Springer International Publishing, Cham, 2017
[48]. Kuner, Christopher, Bygrave, Lee A., and Docksey, Christopher (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020.
[49]. Supra 16.
[50]. Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books.
[51]. R (Privacy International) vs. Investigatory Powers Tribunal, (2019) UKSC 22

Documents Act (PIPEDA) to control the manner in which they collect and utilize personal data together with private sector organizations. The Office of the Privacy Commissioner (OPC) requests increased privacy legislation to handle both AI along with facial recognition technologies . The enforcement framework of both countries recognizes transparent independent institutions and strong regulatory powers which India continues to develop in its privacy regulations.

6.4. LESSONS INDIA CAN LEARN

India can gain critical insights regarding privacy management from existing global regulatory approaches. Indian data protection needs a single law comparable to the GDPR because its present sector-by-sector regulation creates confusion. The trust between the public and compliance is built best through a data protection authority which possesses quasi-judicial powers to independently oversee operations (Mehta, 2023)[52]. The nation needs to adopt the data protection standards of data minimization together with purpose limitation and user consent especially during government data handling procedures. The judicial system needs to establish both surveillance measure review systems and protecting both biometric data and AI-generated content through institutional regulations. To achieve its digital transformation India needs to shift its data handling approach from operations compliance to human rights protection along with democratic oversight (Bhatia, 2020)[53].

7. CONSTITUTIONAL AND ETHICAL IMPLICATIONS

7.1. BALANCE BETWEEN NATIONAL SECURITY AND INDIVIDUAL RIGHTS

National security considerations have been at odds with individual rights protection to create one of the main points of dispute within privacy laws. Indian authorities use national security as justification for surveillance activities while those justifications need to pass constitutional scrutiny. According to Puttaswamy (2017)[54] the Supreme Court declared that states must apply strict tests of legality and necessity and proportionality for their privacy restrictions to stop being arbitrary or too far-reaching (Chandrachud, 2017)[55]. The absence of legislative or judicial oversight about executive power creates dangers because scholars suggest that security-justified unlimited power can destroy civil liberties (Ramanathan, 2021)[56]. Constitutionalism requires the state to maintain proper equilibrium between its security objectives and individual rights to privacy as well as freedom from invasive actions (Bhatia, 2020)[57].

7.2. ETHICAL CONCERNS IN MASS SURVEILLANCE AND AI

The implementation of face recognition together with prediction systems and AI-powered biometric systems creates serious ethical challenges. These monitoring tools function without sharing their processes or seeking permission from individuals and do not hold anybody accountable as they produce discriminatory patterns that especially affect marginalized populations (Eubanks 2018)[58]. Determination of algorithmic choices remains inscrutable because of the "black box" problem which hinders challenges and comprehension of decision-making processes (Pasquale 2015)[59]. The ethical standards of fairness along with non-discrimination and autonomy permit violation through this practice. The Indian state's AI-powered public system development stands out because there are no sufficient ethical standards which creates privacy problems that turn citizens into surveillance subjects who lose their fundamental privacy rights.

52. Supra 35.
53. Supra 30.
54. Supra 1.
55. Supra 4.
56. Supra 27.
57. Supra 30.
58. Supra 25.
59. Pasquale, Frank, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge, MA, 2015.

7.3. PUBLIC INTEREST VS. INDIVIDUAL AUTONOMY

The debate around public interest and individual autonomy is central to discussions on privacy. The state often argues that data collection and surveillance are necessary to promote welfare schemes, detect crime, or improve governance. However, courts and scholars alike emphasize that public interest cannot be a blanket justification for infringing personal liberty. As highlighted in the *Aadhaar* judgment, even beneficial projects must be constitutionally valid and minimally intrusive. When the individual becomes a data point rather than a rights-bearing citizen, the risk is that autonomy is subordinated to utilitarian goals (Khera, 2019)[60]. Thus, ethical governance must uphold the privacy of the individual over the collectivist ambitions of the state, especially in digital systems where consent is often illusory or coerced (Solove, 2006)[61].

7.4. NEED FOR DIGITAL CONSTITUTIONALISM

The rapid digitization of governance, commerce, and civil life calls for a new constitutional framework—Digital Constitutionalism—that protects fundamental rights in digital environments. This approach seeks to apply constitutional values such as privacy, dignity, freedom of speech, and equality in regulating digital technologies and platforms (de Gregorio, 2020)[62]. It emphasizes the responsibility of both state as well as non-state actors in ensuring that technological advancements do not come at the cost of civil liberties. India's current legal regime lacks this holistic approach, especially as private tech giants increasingly mediate social and political life (Zuboff, 2019)[63]. Digital rights need integration into constitutional legislation immediately in order to prevent authoritarian control of technological power (Balkin 2014)[64].

8. POLICY RECOMMENDATIONS AND REFORM PROPOSALS

8.1. STRENGTHENING THE DATA PROTECTION AUTHORITY

To establish informational privacy in India requires the establishment of an autonomous as well as potent Data Protection Authority (DPA). The DPDP Act, 2023 establishes a Data Protection Board through which concerns have emerged because of its insufficient structural independence and limited authority to settle disputes (Mehta, 2023)[65]. Indian authorities should model the Data Protection Authority after the GDPR standards by making it independent, transparent and giving it auditing authority along with enforcement power that extends to both public and private sectors (Voigt & Von dem Bussche, 2017)[66]. The authority needs enough funding along with a specific directive to resolve data violations quickly and equally (Ramanathan, 2021)[67].

8.2. ENSURING TRANSPARENCY AND ACCOUNTABILITY IN SURVEILLANCE

Surveillance mechanisms in India often operate in legal grey zones with minimal transparency or public scrutiny. Existing laws such as the Indian Telegraph Act, 1885(Act No. 13 of 1885) and the Information Technology Act, (Act No. 21 of 2000) provide broad powers to intercept communications without sufficient judicial oversight (Banisar, 2011)[68]. To address this, the government must establish transparent authorisation protocols, independent review mechanisms, and publish annual transparency reports detailing surveillance requests and approvals (Greenleaf, 2020)[69]. Additionally,

---

60. Supra 37.
61. Supra 7.
62. de Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70.
63. Supra 24.
64. Balkin, J. M. (2014). Digital speech and democratic culture: A theory of freedom of expression for the information society. *NYU Law Review*, 79(1), 1–58.
65. Supra 35.
66. Supra 48.
67. Supra 27.
68. Supra 19.
69. Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 165, 10–13.

surveillance technologies like facial recognition systems must undergo mandatory privacy impact assessments to evaluate proportionality and necessity.

8.3. PROMOTING PRIVACY LITERACY AND DIGITAL HYGIENE

As digital technologies become ubiquitous, there is a growing need to educate citizens on privacy rights, data protection, as well as responsible digital behaviour. Most users remain unaware of how their data is collected, processed, and shared by apps and platforms (Solove, 2008)[70]. Privacy literacy programs should be integrated into school curricula, public awareness campaigns, and digital training initiatives. Government, civil society, and tech companies must collaborate to promote digital hygiene practices, such as managing app permissions, enabling two-factor authentication, and understanding consent mechanisms (Tufekci, 2015)[71]. Empowering citizens through knowledge is crucial for fostering a rights-conscious digital society.

8.4. INTRODUCING PRIVACY BY DESIGN IN TECH DEVELOPMENT

The principle of Privacy by Design (PbD) must be embedded into all digital systems and platforms developed by both public and private entities. PbD emphasizes building privacy protections into the architecture of technological systems rather than treating privacy as an afterthought (Cavoukian, 2010)[72]. Developers should minimize data collection, ensure anonymization, enable user control over personal information, and provide clear opt-in mechanisms. Government procurement policies must mandate privacy standards in software and hardware development. Incentivizing privacy-friendly innovations through tax benefits or certifications can further encourage compliance and ethical tech practices (Bhatia, 2020)[73].

8.5. JUDICIAL AND PARLIAMENTARY OVERSIGHT OF STATE SURVEILLANCE

The success of checks and balances depends upon thorough judicial together with legislative review of surveillance methods. India has no central authority which checks surveillance programs for compliance with legal requirements and proportionality standards and essential necessity. Indian oversight requires the creation of a Parliamentary Standing Committee on Surveillance and Privacy that would provide intelligence and law enforcement agencies with democratic accountability. The judiciary needs to actively inspect all metadata actions while establishing firm directives for surveillance metadata management and utilization processes. National security objectives need supervision through properly structured oversight systems which prevent constitutional liberties from being lost (Balkin, 2014)[74].

9. CONCLUSION

9.1. RECAPITULATION OF KEY ISSUES AND LEGAL CHALLENGES

Research investigates the historical development and current struggles as well as imminent trends in privacy rights within India's digital domains. Progress in privacy advocacy began with Kharak Singh (1963)[75] where judges showed reluctance which changed in 2017 with Puttaswamy that moved privacy to the heart of constitutional discussions (Chandrachud, 2017)[76]. The growing recognition of privacy rights faces new challenges because states and private sector actors employ AI profiling together with mass surveillance while collecting data without proper oversight (Zuboff, 2019)[77]. The Digital Personal Data Protection Act, 2023 represents progress yet failures exist because of exemptions given to states in addition to weak enforceability and missing institutional autonomy (Mehta, 2023)[78]. Modern

[70]. Supra 16.
[71]. Supra 22.
[72]. Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada.
[73]. Supra 30.
[74]. Supra 69.
[75]. Supra 9.
[76]. Supra 4.
[77]. Supra 24.
[78]. Supra 35.

technology has progressed faster than legal protection has developed therefore exposing personal rights to growing invasion and reduction to market transactions.

9.2. THE WAY FORWARD FOR PRIVACY JURISPRUDENCE IN THE DIGITAL AGE

A rights-oriented digital governing framework should become a new direction for privacy jurisprudence development throughout India. The Data Protection Authority and state surveillance practices need proper proportionality checks together with integration of privacy by design principles into public and private digital infrastructure (Cavoukian, 2010)[79]. Courts must maintain their support of the Puttaswamy doctrine by requiring proper legal foundations which meet tests of legality and necessity along with proportionality (Ramanathan 2021)[80].

9.3. CLOSING REFLECTIONS ON BALANCING INNOVATION AND RIGHTS

A rights-oriented digital governing framework should become a new direction for privacy jurisprudence development throughout India. The Data Protection Authority and state surveillance practices need proper proportionality checks together with integration of privacy by design principles into public and private digital infrastructure (Cavoukian, 2010)[81]. Courts must maintain their support of the Puttaswamy doctrine by requiring proper legal foundations which meet tests of legality and necessity along with proportionality (Ramanathan 2021)[82]. The GDPR framework allows countries to use its guidelines to construct sophisticated privacy defences and improve their international data protection efforts (Voigt & Von dem Bussche, 2017)[83].

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Austin, G. (2001). Working a Democratic Constitution: The Indian Experience. Oxford University Press.

Banerjee, S. (2022). Surveillance and the State in India: The Growing Use of Facial Recognition. *Economic and Political Weekly*, 57(2), 15–18.

Banisar, D. (2011). Speaking of Surveillance: The Need for Privacy Laws in India. Privacy International.

Balkin, J. M. (2014). Digital speech and democratic culture: A theory of freedom of expression for the information society. *NYU Law Review*, 79(1), 1–58.

Basheer, S. (2015). India's Tryst with Data Privacy. *Indian Journal of Law and Technology*, 11(1), 1–18.

Bennett, Colin J. and Raab, Charles D., The Governance of Privacy: Policy Instruments in Global Perspective, 2nd edition, MIT Press, Cambridge, MA (2006)

Bhatia, G. (2018). The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India.

Bhatia, G. (2020). State Surveillance and the Right to Privacy in India. *NUJS Law Review*, 13(2), 1–26.

Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada.

Chandrachud, D. Y. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*. Supreme Court of India, W.P. (Civil) No. 494 of 2012.

Cate, F. H. (2010). The failure of fair information practice principles. In R. Gellman & P. Dixon (Eds.), *Privacy, due process and the computational turn*. Routledge.

79. Supra 79.
80. Supra 27.
81. Supra 79.
82. Supra 27.
83. Supra 48.

Crawford, K., & Paglen, T. (2019). Excavating AI: The politics of images in machine learning training sets. *AI Now Institute*.
de Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1), 41–70.
Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.
Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown Law, Center on Privacy & Technology.
Govind vs. State of Madhya Pradesh, 1955 CrLJ 1275; Govind vs. State of Madhya Pradesh, AIR 1975 SC 1378
Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, 165, 10–13.
Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books.
Helfer, L. R., & Slaughter, A. M. (1997). Toward a theory of effective supranational adjudication. *The Yale Law Journal*, 107(2), 273–391.
Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59.
Justice K.S. Puttaswamy vs. Union of India, 2017 10 SCC1
Justice K. S. Puttaswamy (Retd.) and another vs. Union of India and others, (2019) 1 SCC 1.
Kharak Singh vs. State of Uttar Pradesh (1962) AIR 1963 SC 1295
Khera, R. (2019). Aadhaar and the Right to Privacy. *Seminar*, 713, 34–38.
Kuner, Christopher, Bygrave, Lee A., and Docksey, Christopher (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020.
Lundberg, Ian, Narayanan, Arvind, Levy, Karen, and Salganik, Matthew. "Privacy, Ethics, and Data Access: A Case study of the Fragile Families Challenge" Socius: Sociological Research for a Dynamic World, vol. 4, 2018, pp. 1-13
Mehta, P. B. (2023). A Fragile Promise: The Digital Personal Data Protection Act, 2023 and Constitutional Concerns. *India Forum*.
Pasquale, Frank, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge, MA, 2015.
R (Privacy International) vs. Investigatory Powers Tribunal, (2019) UKSC 22
Ramanathan, Usha, "Aadhaar and the Right to Privacy", 13 Indian J. Const. L. 1 (2021)
Regan, Priscilla M., Legislating Privacy: Technology, social values, and public policy, University of North Carolina Press, Chapel Hill (1995)
Sarat, A and Silbey, S.S., "The pull of the policy audience",10(2-3) Law and Policy 97-166 (1988).
Suchita Srivastava and another vs. Chandigarh Administration, (2009) 9 SCC 1
Tufekci, Zeynep, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency", 13 Colo. Tech. L.J. 203 (2015)
Voigt, Paul and von dem Bussche, Axel, The EU General Data Protection Regulation (GDPR): A Practical guide,1st ed., Springer International Publishing, Cham, 2017
Wacks, Raymond, Privacy: A Very Short Introduction, Oxford University Press, Oxford (2010)
Westin, Alan F., Privacy and Freedom, Atheneum, New York, 1967 Westin, Alan F., Privacy and Freedom, Atheneum, New York, 1967
Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, New York (2019)