Privacy Rights in India: Evolution, Legal Developments, and Contemporary Challenges in the Digital Age

Mr. Akshaj Garg & Mr. Siddhant Naresh Pathak

5BBA LLB (Honours) & 3BBA LLB (Honours)

School of Law, Christ University, Lavasa campus, Pune – 412112, Maharashtra State,

Abstract

The right to privacy plays a vital role in shaping human dignity and freedom. It has evolved into a fundamental right in India through landmark judgements and legislative advancements. Initially it was not a part of the Indian Constitution, rather it gained recognition as a fundamental right under Article 21 of the Constitution, following the transformative judgment in *Justice K.S. Puttaswamy v. Union of India* (2017). This paper explores the historical development of privacy rights in India, tracing their evolution through relevant case laws, such as *M.P. Sharma v. Satish Chandra* (1954) and *Kharak Singh v. State of Uttar Pradesh* (1963). The study also examines how the legislative body responded to the privacy concerns that arose due to the advancements in the digital era such as *Digital Personal Data Protection Act, 2023*, Through a comparative analysis with global frameworks such as the General Data Protection Regulation (GDPR), the paper highlights the need to strengthen privacy protection laws in India.

The paper also explores the societal implications of privacy. While focusing on its impact on individuals & freedom of expressions. It examines challenges in maintaining a proper balance between national security and civil liberties. The paper also examines the impact of the Cambridge Analytica scandal and Aadhaar-related breach which raised concerns regarding the urgent need for stronger privacy protection laws.

The research concludes by advocating for continuous legal reforms, public awareness initiatives, and international collaboration to address emerging privacy challenges. India can uphold individual freedom and promote democratic principles by protecting privacy of individuals in this digital era. This analysis highlights that privacy is not merely a legal right but a cornerstone of human liberty.

1. Introduction

Privacy is an ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively. However, the idea of privacy is still complicated and depends on context. A jurist, Jude Cooley equated privacy with the right to be left alone while Edward Shills developed on this and defined privacy as a "zero relationship" between individuals or groups in order to enjoy autonomy without unwanted interaction. Thus, privacy is viewed as a cultural value that varies between cultures and serves the actualization of the individual or the group.According to It has been recognized internationally as Human Rights under Article 12 of UDHR[1] (The Universal Declaration of Human Rights) which provides that everyone has the liberty not to get interfered with his privacy, correspondence, family, and also not to be permitted to defame its reputation or honor. Many thinkers have recognized the right to privacy as a civil and political right. The right to privacy is a human right and it has been recognized by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights[2] (ICCPR). Under Article 17 of the ICCPR, everybody's privacy has to be protected. States which are parties to ICCPR have a positive obligation to take legislative and other measures in order to prevent interference and attacks on the privacy of individuals as well as in order to protect this right.

[1] United Nations, Universal Declaration of Human Rights, United Nations (1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights (last visited Jan 4, 2025).
[2] the United Nations Commission on Human Rights, International Covenant on Civil and Political Rights, OHCHR (1976), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (last visited Jan 9, 2025).

The right to privacy is a fundamental aspect of personal freedom and Dignity. The concept of right to privacy is defined by Black's Law Dictionary[3] as the "right to be let alone," which means that it is the right to protect a person from unwarranted interference. Privacy, as a legal principle, serves as a cornerstone in safeguarding personal autonomy. Historically, the evolution of the right to privacy has been closely linked to societal advancements and the development of legal systems. Because of its global significance, it has been incorporated in a number of legal documents, such as national laws, human rights treaties, and constitutions. In modern contexts, the scope of privacy rights has increased significantly, addressing challenges like technological advancements such as the internet, social media, and data analytics.

2. Evolution of the Right to Privacy in India

The evolution of privacy as a fundamental right in India has been shaped by judicial interpretation in different case laws.

2.1 Early Lack of Privacy as a Constitutional Right

2.1.1 The Constitution of India,1950[4]

When the Constitution of India was drafted, it did not Specifically include the right to privacy as a fundamental right. Whereas it focused on other fundamental rights like right to equality (Article 14), right to freedom of speech (Article 19), and protection against arbitrary detention (Article 22)[5]. This was majorly due to the end of colonial rule, where the emphasis was on nation-building and economic development rather than individual rights like privacy.

During that time, privacy was a concept famous in the western countries and differed from India's perspective of collective nation's growth. The framers of constituion gave importance to societal, economic and political welfare rather than personal freedom.

2.1.2 Early Judicial Approach to Privacy

[3] Asst. Prof. Anjum Ansari, International Perspective of Right to Privacy, DR. D. Y. PATIL INSTITUTE OF TECHNOLOGY (Mar. 16, 2022), https://law.dypvp.edu.in/Blogs/international-perspective-of-right-to-privacy (last visited Jan 6, 2025).
[4] The Constitution of India, (1950).
[5] Unfold Law, The Golden Triangle of the Indian Constitution Article 14, 19 & 21, Unfoldlaw (2023), https://unfoldlaw.in/the-golden-triangle-of-the-indian-constitution/ (last visited Jan 9, 2025).

In the early years of independence, the judiciary subordinated individual rights in favor of collective interests and often gave more weight to state interests and public welfare. Privacy was not viewed as a natural component of constitutional rights, and courts were generally loath to interfere with state actions that intruded into personal lives.

For example, courts often sided with state power in cases of police surveillance or government action on the grounds that security and public order had to be preserved against individual self-direction. The effect was to limit the scope of privacy rights and to leave individuals vulnerable to state intrusion.

2.2 Early Judicial Recognition and Developments (1950s–70s)

2.2.1 M.P. Sharma v. Satish Chandra (1954)[6]

Case Facts:

This case came before the Court in the course of winding up of Dalmai Airways Ltd., in which the government authorities had ordered searches and seizures to collect evidence of financial mismanagement and siphoning of assets. The company urged that such searches were violative of an implied right to privacy, and the said invasions were not justified by law and violated constitutional limitations.

Judgment and Implications:

The Supreme Court, through an eight-judge bench decision, held that the right to privacy was not a fundamental right under the Indian Constitution. The Court noted that the Constitution has expressly provided protection under certain articles, for example, Article 20(3), which protects against self-incrimination. However, these protections only operated in the realm of testimonial evidence and not in the context of searches and seizures of property.

The Court went on to state that India's Constitution did not acknowledge privacy as an intrinsic or independent right, unlike the U.S. Constitution. This judgment firmly negated the inclusion of privacy within constitutional guarantees and emphasized the framers' deliberate omission of such a right. As a result, the case set a restrictive precedent, discouraging broader interpretations of privacy for many years.

[6] B. Jagannadhadas, M. P. Sharma And Others vs Satish Chandra (1954).

2.2.2 Kharak Singh v. State of Uttar Pradesh (1962)[7]

Case Facts:

Kharak Singh, suspected of dacoity, was subjected to "surveillance" under the U.P. Police Regulations, including such measures as domiciliary visits and keeping a record of his movements. Singh contended that these practices infringed upon his fundamental rights, particularly his personal liberty under Article 21 of the Constitution.[8]

Judgment and Recognition of Personal Liberty:

By a majority judgment, the Supreme Court held that personal liberty under Article 21 did not specifically and explicitly include the right to privacy. The Court, however, struck down domiciliary visits as unconstitutional, holding that they constituted an unreasonable invasion into the sanctity of an individual's home and a violation of his personal liberty. The Court, however, upheld other forms of surveillance as lawful.

Justice Subba Rao's Dissent:

Justice Subba Rao, in his dissenting opinion, took the progressive stance that the right to privacy is an integral part of personal liberty under Article 21. He opined that any physical or psychological invasion on a person's private space must be held unconstitutional. The dissenting opinion was the first recognition of privacy as an implied fundamental right. The majority separated "liberty" from "privacy," while Justice Rao's dissent showed their interdependence. The dissent by Justice Subba Rao provided a crucial role in introducing privacy as a constitutional consideration for future judgments to enlarge its scope. Justice Subba Rao's dissent became a foundation for future arguments for privacy as an essential component of personal liberty, ultimately influencing landmark decisions such as Govind v. State of Madhya Pradesh (1975) and Justice K.S. Puttaswamy v. Union of India (2017).

2.3 Gradual Development in Later Decades (1970s–90s)

2.3.1 Govind v. State of Madhya Pradesh (1975)[9]

[7] N. Rajagopala Ayyangar, Kharak Singh vs The State Of U. P. & Others (1962).
[8] Right to Privacy: Court in Review, Supreme Court Observer (2017), https://www.scobserver.in/journal/right-to-privacy-court-in-review/ (last visited Jan 9, 2025).
[9] Kuttyil Kurien Mathew, Govind vs State Of Madhya Pradesh & Anr (1975).

Case Facts:

Govind, the petitioner, questioned the validity of police surveillance under the Madhya Pradesh Police Regulations. He argued that the surveillance measures, including shadowing, reporting on movements, and tracking visitors, violated his fundamental rights under Articles 19 (freedom of movement) and 21 (right to life and personal liberty). Govind thus contended that in the absence of judicial oversight or a warrant, the surveillance was arbitrary and unconstitutional.

Judgement and Implications:

The Supreme Court upheld the constitutionality of certain surveillance practices, introducing a very important principle: the right to privacy, though not specifically mentioned in the Constitution, could be inferred as a fundamental part of the right to life and personal liberty under Article 21. However, it was underlined that the right to privacy is not an absolute right but must be balanced against compelling state interests in public order and security.

It also underlined the principle of proportionality, according to which state actions infringing on privacy must be reasonable and justifiable in order to serve a legitimate state interest, such as crime prevention or public safety, in a manner that is minimally intrusive to achieve the intended objective.

This case was a landmark in Indian jurisprudence, and for the first time, privacy was recognized as an implied constitutional right under Article 21. This marked a turn from previous judgments that categorically denied the existence of any such right to privacy. The Court laid down a framework for balancing individual privacy against state interests by holding that privacy must be weighed against considerations for public safety and order. Applying the doctrine of proportionality, it had ensured that state intrusions upon privacy would be justified only to the extent that they were both necessary and reasonable, thereby curtailing arbitrary government power.

2.3.2 ADM Jabalpur v. Shivakanta Shukla (1976)[10]

Case Background:

This case, popularly known as the Habeas Corpus case, came up before the court during the Emergency (1975–77) when the government suspended the fundamental rights of citizens,

[10] A.N. Ray, Additional District Magistrate, ... vs S. S. Shukla Etc. Etc (1976).

including those pertaining to life and personal liberty under Article 21. Preventive detention laws gave the government the authority to detain without trial, and many detainees moved habeas corpus petitions to get their detentions reviewed by the judiciary.

Judgement and Implications:

By a 4:1 majority, the Supreme Court controversially held that during the Emergency, there could be no remedies sought for the violation of even fundamental rights, upholding the government's case that Emergency powers were absolute and beyond judicial scrutiny.

Justice H.R. Khanna's Dissent:

Justice H.R. Khanna delivered a dissenting opinion which was historic, holding that the right to life and personal liberty is so basic that it cannot be extinguished even during an Emergency. He argued that no authority of the State could claim absolute power to detain a person without being accountable to anyone. His dissent emphasized the inviolability of personal liberty and the necessity of judicial oversight, even in extraordinary circumstances.

The majority judgment was widely criticized as an erosion of basic rights and a grant of unbridled power to the executive. It marked one of the lowest points in Indian judicial history and exposed the failure of the judiciary to act as a sentinel of individual rights during a crisis. Justice Khanna's dissent became a guiding principle for future constitutional interpretation. It underlined the inherent and non-derogable nature of personal liberty, laying the intellectual foundation for future judgments that expanded the scope of fundamental rights, including the right to privacy. The case reminded the judiciary of its duty to uphold the principles of the Constitution, even in difficult times. It showed the need for strong legal protections against the abuse of state power.

2.4 The Landmark Judgment: Justice K.S. Puttaswamy v. Union of India (2017)[11]

2.4.1 Case Background

The case of Justice K.S. Puttaswamy v. Union of India questioned the constitutionality of the Aadhaar Act, 2016, which mandated the collection of biometric and demographic data from citizens as a pre-condition for availing government welfare schemes. The petitioners, led by retired Justice K.S. Puttaswamy, thus contended that the mandatory nature of the Aadhaar

[11] A.K. Sikri, Justice K.S.Puttaswamy(Retd) vs Union Of India On (2018).

scheme violated the right to privacy. They pointed out the lack of protection for sensitive data such as fingerprints and iris scans, the possibility of breaches due to the centralized storage of data, and the surveillance state that Aadhaar created. This, they said, violated citizens' autonomy and made privacy a matter of grave concern for the courts.

The petitioners thus further argued that the right to privacy was an inherent part of Article 21, which covered the right to life and personal liberty. They emphasized that compulsory biometric registration not only disregarded individual choice but also put citizens at risk of misuse, thus undermining their fundamental freedoms.

2.4.2 Supreme Court's Ruling

By a unanimous decision of a nine-judge bench, the Supreme Court declared the right to privacy to be a fundamental right under Article 21 of the Indian Constitution. This judgment overruled the earlier decisions in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963), which had refused to recognize privacy as a constitutional right.

The Court held that privacy is an essential ingredient of the right to life and personal liberty; it ensures dignity, autonomy, and the meaningful exercise of other fundamental rights, including freedom of speech and equality. On a broader aspect, privacy meant personal autonomy, dignity, informational privacy, and the sanctity of intimate spaces and relationships.

To justify any state action invading privacy, the Court laid down a tripartite framework: legality, necessity, and proportionality. State actions must have a clear legal basis, serve a legitimate public purpose, and be the least restrictive means of achieving the objective. The Court also drew heavily from international jurisprudence, invoking the decisions of the European Court of Human Rights and the U.S. Supreme Court to emphasize privacy as a universal human right.

2.4.3 Implications of the Judgment

The Puttaswamy judgment was a watershed in the history of privacy rights in India, changing the constitutional discourse. By finding privacy to be a fundamental right, the Court has provided a legal basis to challenge issues of surveillance, data protection, and personal autonomy. It made privacy an integral part of personal liberty and human dignity rather than an afterthought.

This led to a significant change in policy, such as the formulation of the Digital Personal Data Protection Act[12], 2023. The law tries to protect personal data in the digital era by setting principles on the collection, processing, and storage of data based on principles such as consent, transparency, and accountability. With this judgment, India has been brought at par with international jurisdictions like the General Data Protection Regulation of the European Union, therefore underlining the global significance of privacy.

Socially, the Puttaswamy judgment gave people the power to challenge violations of their privacy by both the government and private entities. It raised public awareness about privacy as a key right, especially in an increasingly digital world. This judgment also influenced later cases. For example, in Navtej Singh Johar v. Union of India[13] (2018), the Court decriminalized homosexuality, recognizing sexual orientation as an important part of privacy and dignity. Similarly, in Joseph Shine v. Union of India[14] (2018), the Court struck down adultery laws, protecting personal relationships and intimate decisions under the right to privacy.

While the judgment was a milestone in constitutional law, it also highlighted challenges, such as balancing privacy with national security. Surveillance laws, like those under the Information Technology Act[15], 2000, and the Indian Telegraph Act[16], 1885, still lack proper oversight and remain open to misuse. There is also ongoing debate about whether the Digital Personal Data Protection Act, 2023, is strong enough to address modern privacy concerns.

The Puttaswamy judgment is a landmark in the constitutional history of India. In the sense that it elevated privacy to the status of a fundamental right, it triggered a broader discourse on autonomy, dignity, and freedom in a fast-changing world. Its impact continues to shape legal and societal developments, reinforcing privacy as a key pillar of human liberty and democracy.

3. Legislative Developments Post-Puttaswamy

3.1 **The Digital Personal Data Protection Act, 2023**

3.1.1 **Overview of the Act**

[12] Digital Personal Data Protection Act, (2023).
[13] . Anonymus, Navtej Singh Johar vs Union Of India Ministry Of Law (2018).
[14] Chief Justice, Joseph Shine vs Union Of India (2018).
[15] Information Technology Act, (2000).
[16] Indian Telegraph Act, (1885).

The **Digital Personal Data Protection Act, 2023** aims to protect personal data in India. It sets out guidelines for the collection, processing, and storage of data, emphasizing the need for user consent before data is gathered. The Act ensures that individuals have their own control over their data, granting them the rights to access, correct, and delete it. It mandates organizations to take responsibility for securing personal data and reporting breaches, and establishes a Data Protection Authority to oversee compliance. Additionally, the Act regulates cross-border data transfers and introduces special provisions for sensitive data.

3.1.2 **Key Provisions of the Act**

The **Digital Personal Data Protection Act, 2023** includes provisions to safeguard individuals' privacy and regulate data processing. It grants data subjects rights such as informed consent, access, correction, erasure, data portability, and the ability to object to data processing. Organizations must adhere to obligations like purpose limitation, data minimization, and ensuring data security, and must notify individuals in case of breaches. The Act emphasizes transparency, requiring organizations to disclose how and why data is collected. It also establishes a **Data Protection Authority** to oversee compliance, address complaints, and enforce penalties for violations, ensuring privacy rights are protected.

3.1.3 **Impact on Privacy Rights**

The **Digital Personal Data Protection Act, 2023** strengthens privacy rights in India by giving individuals greater control over their personal data. It requires explicit consent for data collection and allows individuals to access, correct, and delete their data. The Act also ensures transparency in data processing, with organizations obligated to inform individuals about data usage. In case of data breaches, individuals can seek redress through a dedicated Data Protection Authority, which enforces compliance and addresses complaints. Additionally, special protections are provided for sensitive data and vulnerable groups, like children.

3.2 **Other Relevant Legislation**

3.2.1 **Information Technology Act, 2000**

The Information Technology Act, 2000 (IT Act) addresses cybercrime, electronic commerce, and data protection in India. It criminalizes offenses such as hacking, identity theft, cyberstalking, and data breaches, with penalties including fines and imprisonment. The Act also supports electronic commerce by recognizing digital signatures and electronic contracts, ensuring the legality of online transactions. It mandates organizations to implement security

practices to protect sensitive personal data and imposes penalties for data breaches. Additionally, the Act holds intermediaries accountable for illegal content on their platforms and establishes the Indian Computer Emergency Response Team (CERT-In) to enhance cybersecurity.

3.2.2 **Right to Information Act, 2005**

The **Right to Information Act, 2005** (RTI Act) promotes transparency and accountability in governance by allowing citizens to access information held by public authorities. While it empowers individuals to scrutinize government activities, it also respects privacy rights by including exemptions for personal information, third-party data, and matters related to national security. The Act balances the public's right to know with the need to protect personal privacy, ensuring that sensitive details, such as medical records or personal family matters, are not disclosed unless in the public interest. Courts also play a role in ensuring this balance is maintained.

4. Challenges in Implementing Privacy Rights

4.1 Lack of Awareness and Education

4.1.1 Public Ignorance of Privacy Rights

One of the biggest difficulties in enforcing privacy rights is the general ignorance among people. Most citizens are unaware of their legal rights and what the law says regarding intrusions into their private lives. The ignorance is rather very disturbing in the digital era, where personal information is being collected, shared, and even monetized without clear consent. Without proper knowledge of their rights, people would not know or be able to challenge most of the violations.[17]

4.1.2 Complexity of Legal Language

The other impediment to awareness is the complex and technical language of the privacy policies, terms-of-service agreements, and legal frameworks. These documents are often too dense for the average user to read and understand, therefore leading to uninformed consent to

[17] Tanvi Garg & Navid Kagalwalla, Challenges of Implementing Privacy Policies Across the Globe, in Data Protection and Privacy in Healthcare 212 (2021), https://doi.org/10.1201/9781003048848-12 (last visited Jan 9, 2025).

data collection practices. [18]This lack of clarity widens the gap between legal protection and practical enforcement of privacy rights.

4.1.3 Need for Privacy Education

To this end, educational initiatives are important. Privacy literacy should be incorporated into the school curriculum to educate students on digital safety, data protection, and their rights under privacy laws. Community-driven campaigns can also raise awareness among adults about data security and empower them to exercise their rights. Governments, NGOs, and private organizations must collaborate in promoting understanding and accessibility of privacy laws.[19]

4.2 Enforcement Mechanisms

4.2.1 Importance of Strong Oversight

Effective enforcement mechanisms are the backbone of any successful privacy law. Without proper oversight, even the strongest legislative frameworks risk becoming ineffective. Robust mechanisms ensure compliance, address violations, and provide remedies for affected individuals.

4.2.2 Role of Data Protection Authority (DPA)

Establishment of the DPA under the Digital Personal Data Protection Act, 2023, is a significant step. However, its success depends on various factors: firstly, the DPA needs sufficient resources, including funds, infrastructure, and skilled personnel, to monitor the compliance of entities and investigate any violations. Secondly, it should operate autonomously, uncontrolled by any political or corporate influence, for earning public trust.[20] Lastly, the DPA has to be accessible; meaning that it has to provide channels through which people can report violations of privacy and seek redress without bureaucratic hurdles.

4.2.3 Building Public Trust

Public trust in enforcement bodies like the DPA is crucial for their effectiveness. Transparent processes, timely investigations, and visible actions against violators can instill confidence in

[18] Normann Witzleb et al., Emerging Challenges in Privacy Law: Comparative Perspectives (2014).
[19] Nigel Waters, Responding to New Challenges to Privacy through Law Reform: A Privacy Advocate's Perspective, in Emerging Challenges in Privacy Law 45 (2014), https://doi.org/10.1017/cbo9781107300491.005 (last visited Jan 9, 2025).
[20] T. Raab, New Form of Establishment for Federal Data Protection Authority as Completely Independent Authority, 2 European Data Protection Law Review 112 (2016).

the system. Trust encourages compliance from organizations and empowers individuals to use enforcement mechanisms when their privacy is violated.

4.3 Technological Challenges

4.3.1 Speedy Technological Development

The fast pace of technological innovation poses significant challenges to privacy rights. Technologies like artificial intelligence (AI)[21], big data analytics, and the Internet of Things (IoT) collect and process vast amounts of personal data, often in ways that existing legal frameworks cannot adequately address. These advancements outpace legislation, creating gaps in privacy protection.

4.3.2 AI and Big Data Risks

AI and big data analytics typically rely on vast datasets that involve personal and sensitive information. The result can be unintended privacy violations through, for example, bias in algorithms or profiling of individuals without their knowledge. A lack of transparency in how these AI systems operate further complicates accountability.

4.3.3 IoT and Data Security

The IoT devices, such as smart home appliances and wearable technologies, have introduced new vulnerabilities. These devices collect huge data from users, but most of them do not have strong security measures in place and are thus exposed to hacking and unauthorized access; this poses huge threats to individual privacy.

4.3.4 Adapting Legal Frameworks

In order to deal with these challenges, legal frameworks will have to change. There is a need to strengthen data protection laws and include provisions for emerging technologies. Promoting privacy-enhancing technologies—like encryption and anonymization—may provide further protection. International cooperation will also be necessary in establishing global standards for data governance, as data flows across borders, making enforcement difficult.

5. Privacy Violation Case Studies

[21] Dara Hallinan, Ronald Leenes & Paul De Hert, Data Protection and Privacy, Volume 13: Data Protection and Artificial Intelligence (2021).

5.1 Case Study: Cambridge Analytica Scandal[22]

5.1.1 Background of the Scandal

The Cambridge Analytica scandal emerged in 2018 as one of the most significant privacy violations in the digital age. Political consulting firm Cambridge Analytica harvested personal data from millions of Facebook users without their consent, using it to influence key political events such as the 2016 U.S. presidential election and the Brexit referendum.

5.1.2 Method of Data Harvesting

Cambridge Analytica harvested the data through a third-party app, a harmless-looking personality quiz. While just 270,000 users took the quiz, the app was able to use Facebook's data-sharing policies to harvest information about their friends. In this way, it managed to gain possession of the personal data of more than 87 million users without authorization, including very sensitive information such as political preferences, social connections, and even browsing habits.[23]

5.1.3 Implications and Criticism

The scandal brought to light massive failures in data protection practices and a lack of transparency by Facebook in how user data was used. It exposed how platforms can use personal data for purposes other than those users have consented to—such as targeted advertising and political campaigns. Facebook faced global outrage and was fined $5 billion by the U.S. Federal Trade Commission for its role in the privacy breach.

5.1.4 Lessons and Reforms

The Cambridge Analytica case was a wake-up call for stronger data protection laws and greater accountability of companies handling personal data. It prompted the creation of more stringent regulations, such as the European Union's General Data Protection Regulation (GDPR)[24], which sets rigid guidelines for data collection, processing, and storage. The case is

[22] Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times, Apr. 4, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (last visited Jan 9, 2025).
[23] Christopher Wylie, Mindf*ck: Inside Cambridge Analytica's Plot to Break the World (2019).
[24] Asena Yildirimer, Surveillance Society in the Age of Information: The Facebook Cambridge Analytica Scandal Enformasyon Çağinda Gözetim Toplumu: Facebook Cambridge Analytica Skandali, 6 Electronic Journal of New Media 104 (2017).

a warning about how personal data can be misused in the digital age and how strong privacy safeguards are necessary.

5.2 Case Study: Aadhaar Data Breaches

5.2.1 Background of Aadhaar

The Indian government launched the Aadhaar system to standardize service delivery by assigning a unique 12-digit identification number to every citizen, linked with their biometric and demographic data. On the other hand, although it has been argued that Aadhaar improved the efficiency of welfare distribution, severe criticism arose due to privacy violations and data security issues.[25]

5.2.2 Reports of Data Breaches

Ever since Aadhaar's inception, there have been reports of its data breaches. In 2018, an investigation by The Tribune found that unauthorized access to the Aadhaar database was being sold for as low as ₹500, allowing individuals to access personal details of citizens, including their names, addresses, phone numbers, and Aadhaar numbers. Another serious breach involved government websites inadvertently showing sensitive information of millions of citizens.[26]

5.2.3 Risks of Biometric Data Compromise

One of the most concerning aspects of these breaches is the vulnerability of biometric data, namely, fingerprints and iris scans that are central to the Aadhaar system. In contrast to passwords, biometric data cannot be changed if it gets compromised, and hence, the breach of such kind of data is all the more worrisome. Critics have pointed to weak encryption and security protocols as major flaws in Aadhaar's data protection measures.

5.2.4 Legal and Policy Implications

The breaches thus brought very serious questions regarding the ability of the government to protect the citizens' data. In the case of Justice K.S. Puttaswamy v. Union of India (2018), by which the Supreme Court upheld the constitutionality of Aadhaar but limited its mandatory

[25] Anjana Sasi, Decoding the Indian Data Governance Model: Relooking at Aadhaar, (2024), https://doi.org/10.2139/ssrn.5022202 (last visited Jan 9, 2025).
[26] digiALERT, Aadhaar Data Breach: An In-Depth Analysis of One of India’s Most Pervasive Data Breaches, Nov. 23, 2023, https://www.linkedin.com/pulse/aadhaar-data-breach-in-depth-analysis-one-indias-most-pervasive-iywzc/ (last visited Jan 9, 2025).

use to welfare schemes, the Court prohibited the requirement of Aadhaar for private services, including bank accounts or mobile connections. That is why the urgent need was felt to bring about effective laws of data protection through the promulgation of the Digital Personal Data Protection Act, 2023.

5.3 Case Study: Surveillance in Jammu and Kashmir[27]

5.3.1. Deployment of surveillance technologies

Jammu and Kashmir, a region that has been marked by political unrest, has seen an expansive deployment of surveillance technologies. The government has used tools like drones, CCTV cameras, internet monitoring, and phone tapping, citing national security as the primary justification.

5.3.2 Monitoring of Digital Communications

The most concerning aspect of surveillance in the region relates to the monitoring of internet and mobile communications.[28] The government has, at times, shutdown the internet and monitored online activities to prevent the spread of false information. Security agencies have reportedly monitored social media accounts, emails, and private messages, often without judicial oversight.[29]

5.3.3 Use of Advanced Technologies

The region has also witnessed an increase in the use of facial recognition systems and drones to monitor public gatherings, movements, and activities. Such practices have stoked fears of mass surveillance and erosion of individual freedoms.

5.3.4 Privacy vs. National Security

While the state has a legitimate interest in maintaining law and order, the lack of transparency and accountability in surveillance practices has attracted widespread criticism. The judgment in Justice K.S. Puttaswamy v. Union of India reiterated that any state action infringing on

[27] Khalid Bashir et al., Measles Surveillance in Kashmir: A Mixed Methods Study, 66 Indian journal of public health 251 (2022).
[28] Ht Correspondent, Drone Surveillance by J&K Police Raises Privacy Concerns for Citizens, Hindustan Times, Sep. 25, 2022, https://www.hindustantimes.com/cities/chandigarh-news/drone-surveillance-by-j-k-police-raises-privacy-concerns-for-citizens-101664046208644.html (last visited Jan 9, 2025).
[29] Sabine Kurtenbach Dr., Digital Surveillance and the Threat to Civil Liberties in India, Giga Hamburg, https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india (last visited Jan 4, 2025).

privacy must satisfy the principles of legality, necessity, and proportionality. These principles are generally ignored in Jammu and Kashmir, where national security is trotted out as a blanket justification.

5.3.5 Need for Regulatory Oversight

The surveillance practices in Jammu and Kashmir bring into sharp focus the need for comprehensive surveillance laws in India. These laws must balance national security with individual privacy, ensuring transparency, proportionality, and judicial oversight. Without such safeguards, these measures are at risk of undermining civil liberties and public trust.

6. Conclusion

The right to privacy in India has undergone a remarkable transformation, evolving from a concept largely ignored in the Constitution to a fundamental right enshrined under Article 21. This journey, shaped by judicial interpretations and societal needs, highlights the growing recognition of privacy as essential to personal dignity, autonomy, and freedom in a democratic society.

The landmark *Justice K.S. Puttaswamy v. Union of India (2017)* judgment firmly established privacy as a cornerstone of constitutional rights, influencing legislative reforms like the Digital Personal Data Protection Act, 2023. These advancements demonstrate India's commitment to addressing privacy concerns in an increasingly digital world. However, challenges remain, including public ignorance about privacy rights, the complexity of legal frameworks, and the rapid evolution of technologies like AI and IoT, which complicate the protection of personal data.[30]

Case studies such as the Cambridge Analytica scandal, Aadhaar data breaches, and surveillance in Jammu and Kashmir underscore the urgent need for stronger enforcement mechanisms, transparency, and accountability.[31] While balancing privacy with national security and public interest remains a complex issue, adherence to principles like proportionality, necessity, and legality can ensure privacy rights are not unduly compromised.

[30] Jan Baumbach, To Share or Not to Share? Privacy-Preserving AI in Medicine, in To share or not to share? Privacy-preserving AI in medicine (2024), https://doi.org/10.58647/rexpo.24000035.v1 (last visited Jan 9, 2025).
[31] Veena T. N. & Avishek Chakraborty, Securing Data Privacy, Preserving Trade Secrets: India Tech, in Proceedings of the 2nd Pamir Transboundary Conference for Sustainable Societies 608 (2023), https://doi.org/10.5220/0012907500003882 (last visited Jan 9, 2025).

In conclusion, privacy is more than a legal right; it is fundamental to human dignity and democratic governance. As India continues to navigate the challenges of the digital age, sustained efforts in education, robust regulatory mechanisms, and adaptive legal frameworks will be critical. Protecting privacy is essential not only for individual freedom but also for fostering trust, innovation, and a just society.[32] The recognition of privacy as a fundamental right marks a pivotal moment, but its effective implementation will determine its true impact in safeguarding citizens' rights in the years to come.

[32] Vaishanvi Anand, A Comprehensive Analysis on Right to Privacy in the Digital Age under the Ambit of Data Privacy Laws in India, 12 International Journal of Science and Research (IJSR) 1802 (2023).