IJMRRS

International Journal for Multidisciplinary
Research, Review and Studies

ISSN: 3049-124X (Online)

VOLUME 2 - ISSUE 2

2024

Right To Privacy Issues and Challenges in Digital Era

Author: Sushant Pal, Student of BA.LLB(Hons.) at Amity University Lucknow.
Co-author: Mr. Praful Saran, Assistant Professor at Amity University Lucknow

ABSTRACT

The digital revolution has profoundly altered modes of communication, information access, and transactional activities, while simultaneously introducing significant threats to personal privacy. This research critically examines the multifaceted challenges to privacy in the digital environment, emphasizing legal, technological, and ethical dimensions. The widespread collection of personal data by state actors, private corporations, and other entities has rendered individuals increasingly vulnerable to data breaches and unauthorized exploitation of their information. The study assesses the sufficiency of existing legal frameworks in ensuring privacy protection, investigates the dual role of technology in both compromising and safeguarding privacy, and scrutinizes the ethical ramifications of pervasive data surveillance practices. Additionally, it explores the ongoing tension between national security imperatives and the protection of individual privacy rights. In response to these concerns, the research advocates for the adoption of more robust data protection legislation, the promotion of comprehensive digital literacy programs, and the innovation of privacy-preserving technologies. Through an analysis of case studies and relevant legal precedents, this study aspires to provide a nuanced and holistic understanding of privacy challenges in the digital age, while proposing concrete measures to enhance the protection of personal information in an increasingly interconnected global society.

Keywords: Privacy, Data Protection, Digital Era, Surveillance, Fundamental Rights, DPDP Act 2023, Article 21, Cybersecurity, Data Breaches, Right to Privacy

INTRODUCTION

Over time, human dependence on technology has grown significantly, driving rapid advancements in the technological sphere. While these developments have undoubtedly benefited humanity in numerous ways, they have also introduced several drawbacks, such as fraud, scams, and harassment. A key concern arises from the continuous collection and processing of user data, which often results in mishandling and unauthorized dissemination to fraudulent websites, commercial enterprises, intelligence agencies, and state authorities. Such practices lead to serious breaches of privacy, making privacy protection one of the most pressing challenges of the modern age. This research seeks to explore the historical evolution of the right to privacy, examine the contemporary challenges it faces, propose potential solutions, and trace the journey of the right to privacy's recognition as a fundamental right.

A Detailed Examination of the Evolution of the Right to Privacy

Although humans are often described as social beings, there remains a sphere of each individual's life that one wishes to keep private and undisclosed. The word "private" is rooted in the Latin term privatus, which signifies secrets or personal matters. It is important to recognize that while the notion of privacy is ancient, its formal acknowledgment as a legal right is relatively modern. Privacy, in essence, relates to a person's sense of ownership over personal information they choose not to share.[1]

A groundbreaking article authored by Samuel D. Warren and Louis Brandeis, published in the *Harvard Law Review*[2] in 1890, was among the first to formally address the right to privacy. They proposed the creation of a new legal remedy for invasions of privacy. Celebrated jurist and then-Dean of Harvard Law School, Roscoe Pound, praised the article, noting that it "added a new chapter to our law."

On the international front, privacy has been recognized as a fundamental human right, forming the foundation for the protection of various other rights. It is explicitly acknowledged in major international instruments such as the Universal Declaration of Human Rights (UDHR), 1948, and the International Covenant on Civil and Political Rights (ICCPR) under Articles 12 and 17, respectively.

In the Indian context, the right to privacy was not explicitly enshrined in Part III of the Constitution and was not originally recognized as a fundamental right. In 1954, the Supreme Court, in the landmark case of M.P. Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors.[3], ruled that while the right to privacy was a basic right, it was not absolute, particularly concerning the constitutionality of search and seizure operations.It was only towards the end of the 20th century that the right to privacy began receiving clearer recognition as a distinct right. A significant development occurred in People's Union for Civil Liberties (PUCL) v. Union of India[4], where the Supreme Court unequivocally held that telephone tapping constituted a violation of an individual's privacy, as telephonic conversations fall within the realm of private communication.

---

[1] Julie E. Cohen, What Privacy Is For, 126 HARV. L. REV. 1904 (2013)
[2] Samuel D. Warren; Louis D. Brandeis, The Right to Privacy, Vol.4, 193, 196 (1890).
[3] M.P Sharma & Ors. V. Satish Chandra, DM Delhi & Ors. MANU/SC/0139/1978
[4] PUCL vs Union of India MANU/SC/1239/1998

Right to Privacy: Issues and Strategic Solutions

The digitalisation era has brought forth serious challenges to the protection of the right to privacy. Some of the key concerns are outlined below:

Data Breaches:

A major threat to privacy today is the occurrence of data breaches, which negatively impact both individuals and large-scale businesses. In simple terms, a data breach involves the unauthorized exposure of confidential personal information to third parties, who often exploit this data for malicious purposes. Such breaches may result from internal actors within an organization or external attackers. It is important to note that not all breaches are intentional; some occur accidentally. With increasing digital dependency, data breaches have emerged as a persistent and growing threat.

According to various biannual surveys, India's rising reliance on digital platforms such as the Unified Payments Interface (UPI), Aadhaar, and Open Network indicates a heightened dependence on technology. In India alone, reported data breaches increased significantly from 447 incidents to 1200 incidents in 2022.

One of the most significant breaches, termed the "Mother of All Breaches," occurred in January 2024, where over 26 billion records, primarily comprising usernames and passwords from platforms like Twitter, Adobe, Canva, LinkedIn, and Dropbox, were leaked.

Corporate and Government Surveillance:

The right to privacy is increasingly threatened by the constant surveillance activities conducted by governments and private corporations. Beyond surveillance, concerns also extend to data collection practices, the intended use of collected data, and the lack of robust security measures, often leading to unauthorized intrusions that compromise communication channels and decrypt sensitive data.

Government initiatives such as the National Intelligence Grid (NATGRID), the Centralised Monitoring System (CMS), and the Network Traffic Analysis (NETRA) have been developed to strengthen national security and counter terrorism. However, these surveillance mechanisms have

come under scrutiny for allegedly allowing authorities to access and analyze personal citizen data, thus raising serious alarms about privacy infringement.

This issue was also brought before the Hon'ble Delhi High Court and later escalated to the Supreme Court through a writ petition filed in CPIL & Anr. v. Union of India & Others.

Social Media Information Policies:

Various social media platforms and e-commerce websites routinely gather user information, including location data, browsing habits, and platform activities, often sharing such data with third-party entities.

A notable incident illustrating these concerns is the Facebook–Cambridge Analytica scandal[5], where personal data of millions of Facebook users was harvested and misused to influence voter behavior during the U.S. elections. This became one of Facebook's most significant crises, ultimately leading to Meta (Facebook's parent company) paying $725 million to settle the ensuing legal claims.

Another alarming case involved Amazon's Alexa devices, where reports alleged that contractors and third parties had access to users' recorded conversations. These recordings were used to train artificial intelligence (AI) systems, causing widespread concern about potential violations of user privacy.

Corporate Accountability:

Private sector entities have often come under criticism for violating user privacy, particularly through vague and lengthy agreement policies. Frequently, users are not clearly informed about the nature of their consent, as few have the time or inclination to read through extensive policy documents in today's fast-paced world. This lack of transparency enables the monetization of personal data, which is often shared with third parties—a practice that has become alarmingly widespread.

[5] Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times (April 4, 2018) https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

In a recent incident from June 2024, a hacker known as “xenGen” claimed to have obtained sensitive personal information—including mobile numbers, addresses, and Aadhaar IDs—of 375 million Indians, allegedly sourced from Airtel India’s database. The hacker reportedly offered this data for sale on a hacking forum for $50,000. Airtel, however, categorically denied the allegations, describing them as a “short and desperate attempt to tarnish Airtel’s reputation.”

Lack of Infrastructure and Institutional Capacity:

Vital infrastructures such as biometric and financial databases play a crucial role in data management. However, breaches in such systems have led to serious violations of privacy. These failures often stem from outdated technologies that cannot withstand modern cyber threats, inadequate security protocols, or a single point of failure that compromises entire centralized systems.

The rapid technological boom has also led to the emergence of numerous startups and small enterprises. The sheer volume of such businesses makes it difficult for regulatory bodies to effectively enforce privacy standards. Moreover, limited financial resources often prevent these businesses from hiring cybersecurity experts, forcing them to rely on outdated or insufficient security measures.

A significant breach occurred in 2018 involving India’s Aadhaar system, where biometric data—including fingerprint scans and iris images—of millions of Indians were leaked. Investigations revealed that this sensitive information was sold to unauthorized individuals for as little as ₹500.

Weak Grievance Redressal Mechanisms:

Another critical shortcoming is the ineffectiveness and inaccessibility of grievance redressal systems. These mechanisms are often overly complicated, discouraging victims from seeking help. In the aforementioned cases, affected organizations typically responded slowly to cyberattacks and showed minimal accountability.

There is, therefore, a pressing need for a more robust and user-friendly redressal framework that individuals can easily access and trust.

The newly enacted Digital Personal Data Protection Act, 2023 (DPDP Act 2023)[6] addresses this issue by proposing the establishment of the Data Protection Board of India (DPB). This board will be empowered to order urgent remedial actions and recommend precautionary measures whenever a data breach occurs or is anticipated.

It is undeniable that reliance on technology has surged in recent times and is expected to escalate further as newer and more sophisticated technologies emerge. Consequently, addressing the challenges to privacy requires implementing effective solutions, outlined below:

Strengthening Security Measures:

One of the most effective strategies to safeguard personal data is the enhancement of system security protocols. This involves adopting robust encryption techniques that protect data both during transmission and while stored. Encryption ensures that information is converted into a coded format, rendering it useless if accessed by unauthorized individuals without the appropriate decryption keys. Applications like WhatsApp, Telegram, Google Drive, and Microsoft OneDrive employ such encryption methods.

Additionally, implementing Multi-Factor Authentication (MFA) adds another protective layer by requiring multiple forms of verification before granting access, thereby making unauthorized entry significantly more difficult.

Promoting Awareness and Education:

Creating awareness among the general public about cyber threats, scams, and privacy breaches is crucial. Organizations should regularly conduct training sessions for employees to keep them informed about emerging threats and corresponding preventive measures, thereby minimizing human error.

Furthermore, it is imperative for companies to maintain transparent and accurate privacy policies, ensuring users are not misled into giving consent without fully understanding its implications.

Restricting Data Collection and Sharing:

[6] Rachit Bahl, Rohan Bagai, Digital Personal Data Protection Bill, 2023 – Key Highlights, AZB & Partners (Aug 3, 2023), https://www.azbpartners.com/bank/digital-personal-data-protection-bill-2023-key-highlights/

Organizations must practice data minimization, collecting only the information that is absolutely necessary. Gathering excessive or irrelevant data not only heightens the risk of breaches but also creates additional challenges related to data storage and management. Conducting regular audits can help identify and eliminate redundant data, thus enhancing overall security.

The Digital Personal Data Protection Act, 2023 (DPDP Act 2023) introduces important concepts such as “Data Fiduciary,” “Data Processor,” and “Data Principal,” aimed at maintaining tighter control and tracking of personal information. These provisions are expected to significantly improve accountability among organizations handling sensitive data.

Appropriate Legislations:

Given the rapidly evolving nature of technology, it is essential to enact new laws and revise existing ones, with stricter regulatory frameworks. Strengthening legislation in this manner reduces organizational risks, as entities would be required to manage less personal data. This would, in turn, support organizations in maintaining better compliance.

Previously, India’s primary legal instruments for data protection were the Information Technology Act, 2000 (as amended in 2008) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, these frameworks required significant updates to address the challenges posed by the modern digital era.

Recognizing this need, India made a significant advancement by introducing and passing the Digital Personal Data Protection Act, 2023, on August 11, 2023. The initial draft of the legislation was proposed back in 2018 by the Justice Srikrishna Committee.

The newly enacted law comprehensively addresses matters related to personal data, user consent, and the roles of various parties involved. Although detailed rules and subordinate legislation under this Act are still awaited, the passage of this law marks a crucial step forward in safeguarding data and upholding the fundamental right to privacy.

Right to Privacy as an Integral Part of Article 21 of the Indian Constitution

The core essence of the Indian Constitution is embodied in Article 21, as it guarantees the right to life and personal liberty not only to Indian citizens but also to foreigners residing within the country. It serves as the foundation for all other fundamental rights and duties outlined in the Constitution. The scope of Article 21 is vast, as it encompasses the very essence of human existence — life itself.

Within its protection, several rights such as the right to health, the right to a clean environment, and access to legal aid are included. The right to life, as ensured under Article 21, has been interpreted to include the right to live with dignity, forming an inseparable part of personal liberty.

The concept of liberty under this provision emphasizes an individual's authority over their own life, guaranteeing privacy and personal autonomy free from unwarranted interference. This principle was strongly upheld in the landmark case Maneka Gandhi v. Union of India (1978)[7].

Another significant case affirming the right to privacy was Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.[8], where a crucial question was raised: whether the right to privacy qualifies as a fundamental right. A nine-judge bench unanimously declared that privacy is indeed a fundamental right under the Indian Constitution. The Court emphasized that privacy is integral to the freedoms protected under fundamental rights and is an essential component of dignity, personal autonomy, and liberty.

The judgment also addressed concerns surrounding the Aadhaar database, particularly the collection and use of citizens' biometric information. Applying the Doctrine of Proportionality, the Court weighed the necessity and extent of state intrusion into individual privacy. Furthermore, the verdict overruled previous decisions in M.P. Sharma and Kharak Singh, which had failed to acknowledge the right to privacy as a constitutionally protected fundamental right.

The connection between the right to privacy and Article 21 has been a subject of considerable debate. To address this, the Supreme Court, on several occasions, has clarified that any legislation or policy that infringes upon an individual's right to privacy must pass a strict four-fold test of

[7] Maneka Gandhi v. UOI MANU /SC/0062/1976
[8] K.S. Puttaswamy (Retd.) & Anr. v. UOI & Ors. MANU/SC/0911/2017

proportionality and reasonableness. This framework, articulated in the case of Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., consists of the following stages:

- (a) The restrictive measure must pursue a legitimate objective (legitimate goal stage);
- (b) The measure must be an appropriate means to achieve the intended purpose (suitability or rational connection stage);
- (c) There should be no less restrictive alternative that would achieve the same objective with equal effectiveness (necessity stage);
- (d) The measure should not impose a disproportionate burden on the individual concerned (balancing stage).[9]

Following this landmark ruling, the right to privacy was firmly established as a statutory right. Consequently, any breach of this right now constitutes a violation of Article 21 of the Constitution.

[9] Aditya AK, Proportionality Test for Aadhaar: The Supreme Court's two approaches, Bar and Bench (Sep, 26, 2018, 8:08 pm)

CONCLUSION

The recognition of the right to privacy as a constitutional right marks a significant milestone in legal history, and much of the credit for this achievement is attributed to the insightful and progressive thinking of the judiciary. This ruling affirms the crucial role of courts in safeguarding justice and the rights of citizens. It reinforces the idea that laws evolve in response to the changing needs and dynamics of society, ensuring that they remain relevant and effective in addressing contemporary challenges.

However, the advancement of technology, while offering numerous benefits, also introduces serious concerns about security—particularly when it comes to the protection of individuals' privacy. The rapid pace of technological development presents various risks, including potential violations of personal privacy, data breaches, and cyber threats that undermine the safety of individuals and communities at large. These challenges highlight the complexities of maintaining privacy in the digital age.

In response to these growing concerns, India has made considerable strides with the enactment of the Digital Personal Data Protection Act (DPDP Act 2023). This legislation represents a pivotal step by the Indian government towards strengthening data protection laws and ensuring that citizens' personal information is better safeguarded. The DPDP Act 2023 is a crucial initiative aimed at restoring and bolstering public trust in data privacy regulations, reflecting the nation's commitment to addressing privacy challenges in the digital era.

This legal development not only aligns India with global privacy standards but also serves as a demonstration of the government's proactive approach in protecting the fundamental rights of its citizens in an increasingly digitized world.

REFERENCE

Books & Articles

1. Julie E. Cohen, What Privacy Is For, 126 Harvard Law Review 1904 (2013).

2. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 193 (1890).

Cases

3. M.P. Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors., AIR 1954 SC 300.

4. People's Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568.

5. Maneka Gandhi v. Union of India, AIR 1978 SC 597.

6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Statutes & Legal Documents

7. Constitution of India, Article 21.

8. Information Technology Act, 2000.

9. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

10. Digital Personal Data Protection Act, 2023.

11. Universal Declaration of Human Rights, 1948.

12. International Covenant on Civil and Political Rights, 1966.

Web Sources / Reports

13. Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times (Apr. 4, 2018).

14. Rachit Bahl & Rohan Bagai, Digital Personal Data Protection Bill, 2023 – Key Highlights, AZB & Partners (Aug. 3, 2023).

15. Aditya A.K., Proportionality Test for Aadhaar: The Supreme Court's Two Approaches, Bar & Bench (Sept. 26, 2018).