RIGHT TO PRIVACY IN DIGITAL ERA IN BALANCING SECURITIES AND INDIVIDUAL LIBERTIES

Jasmine Gill
Ph.D. Scholar, Department of Laws, Panjab University, Chandigarh. Email id: kaurjasminegill@gmail.com, ORCID id: 0009-0002-5040-6941

Abstract

In the digital age, the right to privacy has become a major and divisive topic in current legal and social debates. The extraordinary advancement of digital technology has revolutionised the accumulation, storage, and utilisation of personal data, frequently testing the limits of individual privacy. Concurrently, apprehensions regarding national security, cybercrime, and terrorism have prompted governments and organisations to adopt comprehensive surveillance techniques and data gathering practices, engendering a precarious balance between safeguarding public security and preserving individual liberties. The digital age presents a dual challenge: protecting privacy rights while fulfilling the legitimate demand for security in a connected world. Advanced digital innovations offer tremendous possibilities for progress, yet they also spark serious concerns about potential misuse, mishandling of personal record, and heightened surveillance capabilities. This situation highlights the intricate relationship between privacy and security, especially as governments and corporations traverse the legal and ethical limits of personal data utilisation.

Keywords: Right to Privacy, Digital Era, Balancing Securities, Liberties

1. Introduction

Despite being implied in the Indian Constitution, the right to privacy has become more widely acknowledged and important Within today's technology-driven environment. A Quick development of digital tools, The expansion of online connectivity, and the pervasive use of data-driven services have completely changed how people engage with the outside world. But there are also previously unheard-of difficulties with regard to privacy, monitoring, and personal liberties brought about by this digital revolution. Debates concerning the sufficiency and efficacy of the judicial system protecting the entitlement to privacy in India have been triggered by these difficulties. 1

The COVID-19 epidemic has heightened questions about the gathering, handling, and storage of private data, the emergence of government initiatives such as Aadhaar and Digital India, and the increasing dependence on digital platforms. Although the goals of these programs are to enhance governance and spur economic growth, they have brought up serious concerns about

[1] Gaana N, "Right To Privacy in The Digital Period: A Study With Indian Context*," Journal of Legal Research and Juridical Sciences*, Vol. 3 Issue 2 (2019).

possible data misuse, privacy violations, and a lack of robust regulatory monitoring.2 This examines the regulatory framework governing Indian law that protects individual's right to security in the digital era, with a focus on key laws, landmark court decisions, and recent policy measures, including the 2023 legislation on personal data protection. It also evaluates whether these mechanisms effectively address privacy challenges while balancing competing priorities like national security, societal interests, and economic growth.

2. Constitutional of India, 1950

2.1 Right to Privacy under Article 213

The right to privacy was explicitly acknowledged as a basic right under article 21 in the pivotal decision of Justice K.S. Puttaswamy (Retd.) v. Union of India Judicial (2017) significantly expanded the scope of Article 21. India's apex judicial body highlighted that the essence of Inherent worth and autonomy, central to life and liberty, is safeguarded through the protection of privacy:

- Personal Autonomy: Individuals have the right to make choices about their personal lives, including decisions about family, marriage, reproductive rights, and sexual orientation.
- Data Protection: Citizens possess the right to safeguard their private information from unauthorised access and use.
- Private Spaces: People are entitled to live their private lives without undue intervention from the state or other parties.
- Freedom of Thought: Privacy extends to protecting one's thoughts, beliefs, and expressions.4

2.2 Article 19(1)(a): The protection of free expression under this article encompasses digital interactions and indirectly reinforces the individual's control over their personal information. 5

[2] Himanshu Tripathi, "Right to Privacy in the Digital Age: Constitutional Implications in India," *Acclaims* Volume 32 (May 2024).
[3] Constitutional of India, 1950, art.21.
[4] Kamshad Mohsin, Zainab Khan, "Right to Privacy in Digital Era," *SSRN Electronic Journal* (2020).
[5] Constitutional of India, 1950, art.19(1)(a).

1. Freedom to Access and Share Information: Citizens need access to information for meaningful participation in a democracy. This includes accessing data online and expressing their views via digital platforms like social media.
2. Chilling Effect on Free Expression: Without robust informational privacy protections, individuals may hesitate to share opinions, fearing their personal data might be misused or tracked.
3. Right to Anonymity: Expressing oneself anonymously is part of an individual's freedom to express opinions and ideas. The absence of informational privacy protections can compromise anonymity, deterring individuals from voicing dissent or controversial opinions.

2.3 Article 14: Guarantees equality before the law, relevant in addressing discriminatory practices in privacy violations. 6

1. Preventing Discrimination in Data Collection and Usage: Governments and private entities collect vast amounts of data. Article 14 ensures that data collection and processing practices do not target or discriminate against individuals based on gender, religion, caste, socioeconomic status, or other factors.
2. Addressing Digital Divide and Privacy Inequality: Access to privacy-enhancing technologies and digital literacy varies across regions and socioeconomic classes. Unequal access to these resources can lead to privacy violations for marginalized communities.
3. Discriminatory Surveillance Practices: Mass surveillance programs can disproportionately target specific communities, violating their right to equality.
4. Privacy in Employment and Workplace Practices: Employers may monitor employees differently based on gender, class, or position. Such discriminatory practices in workplace surveillance violate the equality principle under Article 14.
5. Algorithmic Bias and Data Privacy: Algorithms used in decision-making (e.g., for credit scoring, hiring, or law enforcement) may reflect biases that result in discriminatory outcomes.7

[6] Constitutional of India, 1950, art.14.
[7] Yamak Sharma, "The Right to Privacy and Digital Era in India," *White Black Legal,* Volume: 2, Issue: 16 (2024).

2.4 Regulatory Landscape: India's IT Act, 2000

This legislation underpins India's digital legal infrastructure through its emphasis on protecting individual privacy and ensuring data security:

2.5 Section 43A: Obligates corporate bodies to safeguard sensitive private information and compensate individuals for negligence

Under Section 43A of India's principal cyber law, organizations are held accountable for securing sensitive user information and are liable to pay damages in cases of negligent handling. Introduced in response to mounting worries about data breaches and privacy violations in the digital sphere, this section came under the Information Technology (Amendment) Act, 2008.[8]

1. Obligation to Protect Sensitive Personal Data: Organisations that manage, process, or retain sensitive personal information are legally required to adopt appropriate security measures and protocols to protect that information.
2. Definition of Sensitive Personal Data:

   Section 43A omits a direct definition of *sensitive personal data*; however, the interpretation is supplied by the 2011 IT Rules on Reasonable Security Practices, which enumerate the types of personal information classified as sensitive. Following terms are included:

   - Passwords
   - Financial personal data (e.g., bank account related details etc.)
   - Health data
   - Biometric data
   - Sexual orientation
   - Any information received under confidentiality agreements
3. Reasonable Security Practices: Corporate bodies must adopt security practices consistent with international standards or industry best practices, as prescribed in their privacy policy or other agreements with customers.

[8] Information Technology Act, 2000, s.43A.

2.6 Section 72: Penalizes unauthorized disclosure of personal information by service providers. 9

1. Unauthorized Access and Disclosure: This section penalizes individuals or service providers who have: Gained access to any personal information through their official capacity or due to a legal agreement.
2. Applicability: It applies to service providers, intermediaries, and individuals entrusted with personal data during their professional duties.
3. Punishment: Section 72 prescribes a penalty that may involve imprisonment for a term extending up to two years and/or a monetary fine not exceeding ₹1 lakh.

2.7 Section 66E: Prohibits capturing, publishing, or transmitting private images without consent. 10

1. Prohibited Actions: Photographing an individual's private area without their consent. Disseminating or sending such photos electronically without permission.
2. Private Area Definition: The term "private area" refers to parts of the human body that are covered with clothing and are not intended to be visible to the public.
3. Consent Requirement: Explicit consent is necessary to capture or share such images. Lack of consent constitutes a violation under this section.
4. Punishment: Section 66E prescribes a penalty that may involve imprisonment for a term extending up to three years and/or a fine not exceeding ₹2 lakh.

2.8 Section 69, Government is legally empowered to access, supervise, or decode data if it serves purposes related to national safety or public order. 11

1. Powers Granted: Relevant governmental bodies at the national or regional level may instruct designated agencies to access or surveil data that is being sent, received, or maintained on digital platforms or electronic systems. They are also authorized to decrypt such information when required.
2. Responsibilities of Intermediaries and Providers of services:

[9] Information Technology Act, 2000, s.72.
[10] Information Technology Act, 2000, s.66R.
[11] Information Technology Act, 2000, s.69.

- Suppliers of services, intermediaries, and persons in charge of computer resources are required to:

  Designated entities are obligated to provide technical assistance to governmental authorities in accessing, overseeing, or decoding electronic communications or data. Failure to comply with these obligations may result in imprisonment for a term of up to seven years, along with financial penalties.

3. Safeguards:
   - Orders for interception, monitoring, or decryption can only be issued by:
     - Authorized government officials at the central or state level.
     - Following due process as outlined in rules framed under the IT Act.

2.9 Section 69A: Governmental Power to Restrict Digital Access[12]

Section 69A empowers government officials to order online platforms and service providers to block certain content or apps if it poses a threat to national security. This legal measure is often applied to ensure the protection of the country's sovereign rights, internal and external security, peaceful foreign affairs, social harmony, and to stop any acts that could lead to serious legal infractions. Upon the issuance of such an order, intermediaries are legally mandated to adhere and limit access to the designated content or sites. This clause has been prominently utilised in instances such as prohibiting mobile applications considered detrimental to India's national interests.

2.10 Section 79: Provides a safe harbour to intermediaries like social media platforms but holds them accountable for non-compliance. 13

This section explains a "safe harbour" to intermediaries, including social networking platforms, e-commerce websites, and web hosting services, shielding them from liability for third-party content. This indicates that intermediaries are not legally accountable for user-generated information, data, or communications conveyed via their platforms, provided they do not start, alter, or choose the recipient of such content. This protection is not unconditional. If an intermediary contributes to content creation or fails to act on illegal content after official notification, it is no longer protected from liability.

[12] Information Technology Act, 2000, s.69A.
[13] Information Technology Act, 2000, s.79.

To maintain safe harbour protection, intermediaries must meet specific requirements, including preventing users from disseminating illegal information such as obscene, defamatory, or dangerous material. They must exercise due diligence as mandated by the 2021 rules governing intermediaries and digital media ethics under the framework of India's IT regulations. This encompasses notifying users regarding content limitations, designating grievance officers to handle user complaints, and collaborating with law enforcement agencies during enquiries. These clauses seek to reconcile the autonomy of internet platforms with their accountability and obligation to mitigate the dissemination of illegal or detrimental content.

3. New Legal Framework for Data Privacy (2023)

The 2023 enactment of India's data protection law reflects a legislative shift towards empowering individuals with greater control over their digital personal information Sections 2 and 3 of the 2023 data protection legislation outline its scope and key definitions. The law applies to the handling of digital personal data within Indian territory, irrespective of the data's origin, and extends to both domestic and international entities engaged in offering goods or services in India. It defines essential terms such as the *Data Principal*, referring to the individual whose data is processed, and the *Data Fiduciary*, denoting the party responsible for such processing. Consent is characterised as a voluntary, informed, clear, and specific agreement given by the Data Principal.

Rights of Data Principals: Section 11 ensures their access to information regarding the manner in which their personal data is handled. 14 Section 12 allows individuals to seek correction of inaccurate data and deletion of data that is outdated or no longer relevant.15 Under Section 13 individual have the right to file complaint, Data Principals can lodge complaints with the Data Fiduciary or escalate them to the Data Protection Board if unresolved.16 The provision in Section 14 grants individuals the ability to retrieve their personal data and transfer it across different processing entities, ensuring greater control over their digital information.[17]

Obligations of Data Fiduciaries: Sections 4 through 10 of the Digital Personal Data Protection Act, 2023, set out essential obligations for entities handling personal data.

[14] Digital Personal Data Protection Act, 2023, s.11.
[15] Digital Personal Data Protection Act, 2023, s.12.
[16] Digital Personal Data Protection Act, 2023, s.13.
[17] Digital Personal Data Protection Act, 2023, s.14.

- Section 4 establishes the principle of purpose limitation, requiring that data be processed solely for clearly defined and legitimate objectives.[18]
- Section 5 reinforces data minimization by mandating that only the data strictly necessary to achieve the intended objective be collected and used.[19]
- Section 6 provides that processing activities must be grounded in lawful bases, which may include the individual's consent, compliance with legal duties, or actions carried out in the public interest. [20]
- In line with this, Section 7 outlines the requirements for valid consent, which must be specific, informed, and voluntary, while Additionally providing data subjects with the ability to rescind their consent at any point.[21]
- Section 9 addresses data retention, directing that personal data be discarded once its relevance to the processing purpose has ceased.
- Lastly, Section 10 imposes a duty on Data Fiduciaries to implement adequate technical and organizational safeguards to prevent data breaches, unauthorized disclosures, or loss of information.

4. Special Provisions for Significant Data Fiduciaries

Sections 17 and 18 of the act introduce a risk-based classification system and impose enhanced responsibilities on certain entities. Entities that process large volumes of personal information or present elevated risks to individual privacy are classified under a special category of data handlers with heightened responsibilities. These organizations must adhere to enhanced regulatory obligations, including the regular evaluation of privacy-related risks through structured assessments. Moreover, they are required to appoint a dedicated officer responsible for ensuring compliance with data management standards and applicable legal frameworks. To promote greater accountability and operational transparency, such entities must also keep comprehensive documentation of their data processing activities via systematic audit logs.

4.1 Cross-Border Data Transfers

[18] Digital Personal Data Protection Act, 2023, s.4.
[19] Digital Personal Data Protection Act, 2023, s.5.
[20] Digital Personal Data Protection Act, 2023, s.6.
[21] Digital Personal Data Protection Act, 2023, s.7.

Section 15 addresses cross-border movement of individual data. It allows personal information to be moved outside India to specific countries or regions, provided they are officially designated by the Government of India. This designation is reflecting on an assessment of receiving jurisdiction's commitment to data protection and its adequacy in ensuring privacy safeguards comparable to Indian standards.

4.2 Data Protection Board (DPB)

- Section 19: Establishment
    - Constitutes the Data Protection Board of India, responsible for:
        - Grievance redressal.
        - Ensuring compliance with the Act.
        - Imposing penalties for non-compliance.
- Section 20: Powers
    - The DPB can summon individuals, inspect data processing systems, and issue binding orders.22

4.3 Penalties for Non-Compliance

- Section 25: Financial Penalties
    - Imposes strict penalties for violations, including:
        - Up to ₹250 crore for failing to prevent a data breach.
        - Up to ₹200 crore for non-compliance with Data Principal rights.
- Section 26: Recovery Mechanism
    - The penalties can be recovered as arrears of land revenue if unpaid.

4.4 Telegraph Act, 1885

- Section 4: Exclusive Privilege of the Government: The central government holds exclusive rights to establish, maintain, and regulate telecommunication systems within

[22] Himanshu Tripathi, "Right to Privacy in the Digital Age: Constitutional Implications in India," *Pen Acclaims* (2024).

India. Private players can operate telecom services only with a license granted by the government.[23]

- Section 5(2): Interception of Messages
    - Empowers the central or state government to intercept messages in the following circumstances:
        - In furtherance of national defence and public safety.
        - To safeguard public peace and social harmony.
        - To prevent incitement of offenses.
        - During emergencies.
    - This section forms the legal basis for government surveillance programs.
- Section 7: Rules and Regulations
    - Allows the government to make rules regulating telecommunication services.
    - Includes the authority to prescribe conditions for granting licenses, equipment usage, and fee structures.[24]
- Section 10: Right of Way
    - Grants the government powers to place and maintain telegraph lines on private or public property, subject to compensation for damages.
- Section 20: Misuse of Telegraph Lines
    - Penalizes unauthorized use of telegraph lines with fines or imprisonment.
- Section 25: Damage to Telegraph Lines
    - Penalizes willful destruction or interference with telegraph lines.
- Section 26: Telegraph Fraud
    - Penalizes fraud in using telegraph services, including unauthorized access or tampering.

[23] Telegraph Act, 1885, s.4
[24] Meenakshi Bains, "Right to Privacy in the Digital Era," *Amity International Journal of Law and Multidisciplinary Studies,* Volume: II, Issue: III (2018).

5. Credit Information Companies (Regulation) Act, 2005

1. Objective of the Act

- To oversee the operations of credit information entities and promote transparency and accountability in how credit-related data is gathered, handled, and disclosed.[25]
- To facilitate the smooth operation of the credit system by providing accurate and reliable credit data.
- To safeguard the privacy and confidentiality of credit-related information.

2. Applicability

- Applicable to all credit information companies, their members (banks, financial institutions, etc.), and users of credit information (e.g., lenders).[26]
- Section 3: Mandatory Registration
    - CICs must obtain a certificate of registration from the Reserve Bank of India (RBI) to operate.
    - RBI has the authority to regulate and supervise these companies.
- Section 4: Conditions for Registration
    - The RBI may impose conditions for granting registration, including capital adequacy, infrastructure, and security measures. [27]
- Section 14: Functions of CICs
    - CICs are authorized to collect, process, and disseminate credit information to their members.
    - Information includes loan histories, repayment records, defaults, and other financial data.
- Section 15: Obligation of Members

  It is mandatory for banks, financial institutions, and associated participants to routinely furnish credit information that is accurate and reliable to CICs.

[25] Credit Information Companies (Regulation) Act, 2005.
[26] Gaana N, "Right to Privacy in the Digital Period: A Study with Indian Context," *Journal of Legal Research and Juridical Sciences* (2024).
[27] Ayushman Patnaik and Harshit Arora, "The Right To Privacy In The Digital Age: How Technology Is Impacting Privacy On Social Media," *Indian Journal of Integrated Research in Law* Volume III Issue III (2018).

Section 16: Sharing of Credit Information

- CICs can share credit data only with authorized users (e.g., lenders) and cannot disclose it to unauthorized parties.

- Section 19: Protection of Information
  - Ensures confidentiality and restricts the misuse of credit information.
  - Any breach of confidentiality can result in penalties.
- Section 20: Right to Access and Correct Information
  - Individuals and organizations are entitled to review their credit records and seek rectification in case of any discrepancies.

Regulation by RBI

- Section 13: Powers of RBI
  - RBI is the regulatory authority and oversees the functioning of CICs.
  - RBI can issue directions, inspect records, and revoke the registration of CICs in case of violations. 28

Dispute Resolution

- Section 21: Disputes Between CICs and Members
  - Disputes between CICs and their members (e.g., banks) can be referred to the RBI for resolution.
- Section 22: Disputes with Individuals
  - Individuals can lodge complaints with the CICs if they find errors in their credit reports. CICs are obligated to resolve these disputes promptly.29

Penalties

- Section 23: Penalty for Non-Compliance

[28] Poonam Rawat and Shreyes Aggarwal, "Right to Privacy And Data Protection Issues In India," *IJCRT*, Volume 8, Issue 8 (August 2020).
[29] Rohit Saini, "The Right to Privacy in the Age of Digital Technology: A Study with Indian Context," *International Journal of Advanced Legal Research*, Volume: 3, Issue: 3 (2023).

  - CICs and their affiliates can incur sanctions for violating regulatory requirements or disseminating false or misleading information.

- Section 24: Offenses by Companies
  - Any violation by a company can result in fines or imprisonment of responsible individuals.

6. Conclusion

In the contemporary digital era, Privacy has increasingly been recognised as a critical and highly contested issue, particularly in the Indian context, where rapid technological advancement and widespread digitisation have significantly transformed societal structures. With individuals increasingly reliant on digital platforms for essential activities such as communication, commerce, education, and healthcare, personal data has evolved into a valuable and vulnerable asset. This growing digital dependency has amplified the risk of data misuse, unauthorised surveillance, and exploitation, thereby necessitating the development of a robust legal framework to uphold individual rights and freedoms.

A landmark judicial pronouncement by India's highest judicial authority reaffirmed that privacy constitutes an essential constitutional guarantee, intrinsically linked to the broader principles of life, dignity, and individual freedom as enshrined within the nation's supreme legal document. This decision marked a pivotal moment in Indian constitutional jurisprudence, establishing a foundational precedent for addressing privacy concerns in the digital age. It acknowledged the multifaceted challenges introduced by emerging technologies and the broad use of individual data across state bodies and commercial organisations.

In response, there has been a gradual evolution of the legal and regulatory landscape aimed at enhancing data protection and ensuring accountability among entities that process personal information. Earlier statutes helped establish initial measures against online threats and data compromise, but lacked the breadth needed to manage evolving issues concerning the control, sharing, and protection of personal data. Consequently, newer legislative developments have been introduced, specifically designed to provide comprehensive protection of personal data and to establish mechanisms for transparency, user rights, and institutional accountability in digital governance.