IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, November 2025
Impact Factor: 7.67

Analytical Study of Legal Framework for Data Protection and Data Privacy in India

A. Rekha[1] and Dr. Sanjaya Chaudhary[2]
[1]Research Scholar, Law Department,
[2]Professor and Head, Law Department
Bhagwant University, Ajmer, Rajasthan

Abstract: *Globally, privacy has become a fundamental human right, and the Indian Constitution recognizes it as such under Article 21. As society digitizes, along with technological advancements, safeguarding personal data and privacy has become increasingly difficult. In India, privacy rights have been acknowledged through judicial interpretations and legislative measures, such as the Information Technology Act and the proposed Digital Personal Data Protection Bill, but comprehensive protection against data misuse and breaches remains a challenge. In this paper, we examine the evolution of privacy as a legal right in India, analyze the existing legal framework, and discuss its limitations. The study compares India\'s approach to data protection with international standards such as the European Union\'s General Data Protection Regulation (GDPR).*

Keywords: Privacy, safeguarding; framework; Digital

I. INTRODUCTION

In the 1890 seminal article, Samuel Warren and Louis Brandeis (later Supreme Court judge), coined the phrase, the 'right to be let alone' as defining privacy. This was in response to the technology of times – the newspapers – violating privacy of influential people by printing stories about them. However, it was only in the 1940s that 'Privacy' was internationally regarded as a fundamental civil liberty.

This paper aims to critically assess the information duties set out in the General Data Protection Regulation (GDPR) and national adaptations when the purpose of processing is scientific research. Due to the peculiarities of the legal regime applicable to the research context, information about the processing plays a crucial role for data subjects. However, the analysis points out that the information obligations (also known as mandated disclosures) introduced in the GDPR are not entirely satisfying and present some flaws. In the dynamic landscape of the digital era, the emergence of advanced data collection and processing technologies has necessitated the development of comprehensive legal frameworks to protect individual privacy rights. In Europe, enacting the General Data Protection Regulation (GDPR) in 2018 marked a significant milestone, establishing an EU standard for data protection and ethical compliance (ICO 2018). Historically, India's approach to data protection has historically been shaped by its unique societal dynamics and global technological advancements. In the early stages, data privacy measures in India were fragmented, relying primarily on sector-specific guidelines and existing legal provisions, such as the Information Technology Act, 2000. These measures, while addressing some concerns, lacked the coherence and depth required to deal with the complexities of modern digital ecosystems.

Privacy as a Fundamental Human Right

• Privacy is globally recognized under Article 12 of the Universal Declaration of Huma n Rights and other international covenants (ICCPR, ICPRAMW, IJNCRC).
• It includes the right to be left alone, bodily privacy, family life, sexual orientation, and pr ivate communications.
• However, it excludes public records and data of public interest.
• With digital growth, privacy is increasingly threatened by cybercrimes, data misuse, an d third-party access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 6, November 2025 Impact Factor: 7.67

The growing necessity for effective data protection frameworks is underscored by the unprecedented volume of personal information exchanged online. As individuals engage with various digital platforms— ranging from e-commerce websites and social networks to digital payment systems—the risks of data breaches, unauthorized access, and misuse of personal information have become increasingly prominent. High-profile incidents of data theft and cyberattacks have further highlighted the vulnerabilities in existing systems and the urgent need for a robust regulatory framework. Moreover, organizations are under greater scrutiny regarding their data collection, storage, and usage practices. Businesses, both domestic and international, are recognizing that robust data protection policies are not merely compliance requirements but essential components of ethical and sustainable operations. Failure to implement adequate safeguards can lead to reputational damage, financial penalties, and erosion of consumer trust.

Objectives of GDPR

• Universal Applicability: GDPR applies to all organizations processing the personal data of individuals in the EU, regardless of the organization's physical location. Even websites outside the EU that attract European visitors or monitor their behavior are subject to GDPR.
• Strengthening Consumer Rights: Ensures that consumers are informed about how their data is collected, used, and shared. Provides rights such as data access, rectification, erasure (the "right to be forgotten"), and portability.
• Consent and Transparency: Requires explicit, informed consent from individuals before collecting or processing their data. Companies must use clear and straightforward language in privacy policies to avoid confusion or misrepresentation.
• Accountability Measures for Organizations: Mandates companies to notify individuals promptly about data breaches that compromise their personal information.

Need for Data Protection Regulations

In response to these challenges, the Indian government introduced the Personal Data Protection Bill, which seeks to establish a comprehensive legal framework for data protection. The Bill aims to regulate the processing of personal data by public and private entities, ensure accountability, and empower individuals with greater control over their personal information.
• Data protection laws aim to limit unauthorized collection, storage, and sharing of persona l information.
• In India, comprehensive data protection legislation is still evolving.
• Existing legal protections stem from:
• The Constitution of India (Article 21)
• Information Technology (IT) Act, 2000
• Indian Contract Act, 1872
• Intellectual Property Laws
• Credit Information Companies Regulation Act (CICRA), 2015

Judicial Recognition of the Right to Privacy in India

Beyond legislative measures, the Bill also envisions the establishment of a Data Protection Authority (DPA) to oversee compliance, address grievances, and enforce penalties for violations. This institutional mechanism is expected to strengthen enforcement and ensure that data protection norms are consistently upheld. While the introduction of the Personal Data Protection Bill is a significant step forward, its implementation will pose challenges. Striking a balance between individual privacy rights and the legitimate needs of businesses and governments for data access is a complex task. Additionally, ensuring the Bill's provisions are effectively enforced across India's diverse socio-economic landscape will require significant investment in awareness, infrastructure, and capacity-building.
• Initially, the right to privacy was not considered a fundamental right.
• MP Sharma v. Satish Chandra and Kharak Singh v. State of UP did not affirm it.
• Later judgments began to recognize it:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 6, November 2025 Impact Factor: 7.67

• Govind v. State of MP, Malak Singh v. Punjab & Haryana, R. Rajagopalan v. TN, and PUCL v. Uni on of India broadened the understanding of privacy.
• In 2017, K.S. Puttaswamy v. Union of India, a 9-judge bench declared the Right to Privacy as a Fun damental Right, embedded in Article 21 of the Constitution.

Major Privacy-Related Cases in India

A. Aadhaar Case

• Aadhaar collects biometric and demographic data.
• Concerns: privacy breaches, misuse of data by private agencies, absence of safeguards.
• Supreme Court upheld the Aadhaar Act (majority 4:1) but struck down sections allowin g private access to Aadhaar data.
• Justice Chandrachud dissented, calling the Act unconstitutional as a Money Bill.

B. Section 377 IPC

• Dealt with criminalization of homosexuality.
• In 2018, the SC struck down parts of Section 377, affirming that consensual sexual activity b etween adults is protected by the Right to Privacy.
• Existing Legal Framework for Data Protection in India

Constitutional Protection

• Article 21 (Right to Life) now includes Right to Privacy post-Puttaswamy.
• Subject to reasonable restrictions under Article 19(2) for public interest.

Statutory Protections

IT Act, 2000 (Amended in 2008)

1. Sections 43A, 65, 66, 69A deal with unauthorized data access, cybercrime, and governme nt surveillance.
2. Establishes corporate liability for data leaks.

IPC (Indian Penal Code), 1860

Addresses privacy breaches indirectly through criminal misappropriation and trust violations.

Intellectual Property Laws

Protects data compiled using significant effort under copyright law.

CICRA, 2015

Regulates credit-related personal information and holds entities accountable.

Indian Contract Act, 1872

Allows inclusion of confidentiality clauses in contracts to prevent unauthorized disclosure.

II. CONCLUSION

India's evolving data protection and privacy laws mark significant progress in safeguarding indivi dual rights in the digital era. However, the current framework, while foundational, needs refineme nt to address emerging challenges, including rapid technological advancements, cross-border data flows, and growing cyber threats. Strengthening enforcement mechanisms, fostering public aware ness, and enhancing international cooperation are critical steps forward. The adequacy of India's l aws is a work in progress, with much scope for improvement. Legislators must prioritize creating adaptable and comprehensive policies, organizations must adopt robust datagovernance practices,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 6, November 2025 Impact Factor: 7.67

and individuals must remain vigilant about their digital rights. A collective effort is essential to en sure that India builds a resilient and ethically sound data protection ecosystem that upholds privac y while fostering innovation.

REFERENCES

[1] (DataProtectionLaws, n.d.)
[2] (Finology, n.d.)
[3] (Legal500, n.d.)
[4] (CNBC, n.d.)
[5] (ResearchGate, n.d.)
[6] (https://pwonlyias.com/current-affairs/cybercrime-in-india/#ncrb-data-on-cyber-crimes-inindi a, n.d.)
[7] (MckinseyandCo, n.d.)
[8](https://www.india-briefing.com/doingbusiness-guide/india/sector-insights/indiadigital-transfo rmation, n.d.)
[9] (IAPP, n.d.)
[10] (https://emildai.eu/dpdpa-2023-vs-gdpr-acomparative-analysis-of-indias-eus-dataprivacy-law s/, n.d.)
[11] (MondaqLaw, n.d.)