INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 14

2025

# Strengthening the Legal Frameworks of Data Piracy and Cybersecurity in Digital Era

Bharat P. and Jyotirmoy Banerjee

**Recommended Citation**
Bharat P. and Jyotirmoy Banerjee, *Strengthening the Legal Frameworks of Data Piracy and Cybersecurity in Digital Era*, 4 IJHRLR 187-199 (2025).
Available at www.humanrightlawreview.in/archives/.

# Strengthening the Legal Frameworks of Data Piracy and Cybersecurity in Digital Era

Bharat P. and Jyotirmoy Banerjee

*LLM Student, Amity Law School, Amity University, Bengaluru*
*Assistant Professor, Amity Law School, Amity University, Bengaluru*

| Manuscript Received | Manuscript Accepted | Manuscript Published |
|---|---|---|
| 04 Jan. 2025 | 06 Jan. 2025 | 08 Jan. 2025 |

## ABSTRACT

*In today's digital landscape, the need for a robust policy and legal framework for data protection in India has become increasingly critical. The swift advancements in technology and the widespread embrace of digital platforms have led to an unprecedented surge in the creation, collection, processing, and sharing of personal data. This rising trend has sparked serious concerns about privacy, security, and the potential for mishandling personal information. As India undergoes rapid digitization and the growth of its digital economy, safeguarding personal data emerges as a top priority. In a striking indication of the challenges faced, over 740,000 cybercrime incidents were reported to the Indian Cyber Crime Coordination Centre (I4C) in the first four months of 2024, with approximately 85% of these incidents related to online financial fraud. This study aims to utilize a doctrinal research methodology to examine the existing laws, regulations, and policies in India pertaining to data security and privacy. This article provides a comprehensive overview of India's journey in cybersecurity and data privacy, tracing its evolution from the establishment of the Information Technology Act in 2000 to the recent enactment of the Digital Personal Data Protection Act in 2023. By exploring significant legislative milestones, committee formations, and judicial actions, it underscores India's dedication to strengthening its cybersecurity infrastructure. The research focuses on the crucial need for a well- defined data protection framework that not only safeguards individual privacy rights but also builds user trust and stimulates innovation within the digital landscape. Employing an analytical and qualitative approach, the article draws upon various*

*sources, both primary and secondary, offering a descriptive analysis that specifically examines cybersecurity in the banking sector. Given the rising threats in our increasingly digital world, it contributes valuable insights into pressing issues such as deep fakes, as well as evaluating the existing security frameworks and innovative solutions for protecting digital assets. By highlighting the essential connections among technology, governance, and legal standards, the article emphasizes the urgent necessity for robust cybersecurity measures to protect both citizens and governmental interests. Additionally, this research outlines recommendations aimed at improving data security and privacy in India. These suggestions are crafted to adapt to the continuously changing technological landscape and the emerging legal frameworks. It is crucial for policymakers, legislators, and stakeholders to acknowledge the importance of developing a comprehensive and resilient system that not only defends personal data but also cultivates a secure and reliable digital environment for both individuals and businesses.*

**KEYWORDS**

*Data Piracy, Cybersecurity, Artificial Intelligence, GDPR, Policymakers, Legislators, Data Protection.*

## INTRODUCTION

In today's world, where technology is advancing at an unprecedented rate, the importance of digital privacy and data protection has become incredibly critical. As our daily lives become more closely connected with digital platforms, it is essential to protect personal information from unauthorized access and potential misuse. This raises a fundamental inquiry about the effectiveness of existing legal frameworks in India and their ability to tackle the complex challenges posed by the fast-evolving landscape of digital privacy and data protection. With the rapid pace of technological change, there are growing concerns regarding whether current legal measures are sufficient to safeguard individual privacy and adequately govern the use of personal data.[1]

This study explores the complex challenges and opportunities present in India's digital ecosystem, aiming to improve our understanding of the legal landscape. It seeks to contribute to the development of a stronger framework for digital privacy and data protection in light of The Digital Personal Data Protection Act,

2023. The importance of this research goes beyond academic inquiry; it carries significant practical implications for real-world stakeholders. Policymakers can utilize the informed recommendations to strengthen legislative frameworks, businesses can adjust their strategies to stay compliant with changing regulations, and individuals will gain clarity and empowerment in advocating for their digital rights.[3]

In conducting this research, the aim is not just to assess the current landscape but also to actively engage in the ongoing conversation about the challenges we face in the digital age. This research is designed to offer meaningful insights that can help policymakers, businesses, and individuals find a careful balance between advancing technological innovation and safeguarding personal privacy in our increasingly digital world.[1]

## CONCEPT OF DATA PROTECTION AND DATA PRIVACY

### *What is Data Privacy?*

Data privacy is essential in safeguarding personal information, ensuring that individuals have command over the collection, processing, storage, and sharing of their data. It highlights the individual's right to maintain the confidentiality and security of their information, thereby restricting unauthorized access and use. The term "data privacy" primarily pertains to the management of sensitive personal data, known as personally identifiable information (PII). This encompasses vital data points such as social security numbers, health records, and financial information, including bank accounts and credit card details.[2]

In a corporate environment, data privacy extends beyond just the PII of employees and customers. It can also entail the protection of confidential research, development data, and financial insights. India, with its massive population and dynamic digital landscape, is at the vanguard of technological progress. The swift expansion and accessibility of data have significantly altered governmental operations, enhancing public services and promoting unprecedented innovation for its citizens.[3]

The discussion surrounding data security encompasses two critical dimensions: data privacy and data protection. Data privacy refers to the parameters dictating when, how, and to what degree personal consumer information can be shared and disclosed to others. This includes sensitive details such as name, address, ethnicity, phone number, marital status, and more. In light of the escalating internet usage over the years, the necessity for robust data privacy regulations has never been more pressing.[2]

Conversely, data protection involves the legal measures established to guard data against loss, damage, or corruption. With the exponential growth of data collection, safeguarding this information from unauthorized access has emerged as a significant concern. As researchers and policymakers delve into these issues, finding effective solutions is critical to ensuring consumer trust and safety in the digital realm.[4]

## WHY IS DATA PRIVACY IMPORTANT?

- ***Protection against identity theft and fraud***

The sharing of personal information poses significant risks, particularly related to identity theft and financial fraud. Identity theft occurs when cybercriminals illicitly obtain sensitive personal data with the intent to misuse it, potentially draining bank accounts or creating fraudulent social media profiles to access or manipulate accounts maliciously.[5]

- ***Protection against discrimination:***

Personal data can be leveraged in ways that contribute to discrimination based on attributes such as race, religion, or political beliefs. This misuse can create societal and political instabilities, compromising the social fabric of a nation.[5]

- ***Transparency and accountability:***

Major digital platforms and mobile applications often collect vast amounts of user data to enhance user experiences, provide targeted advertising, and optimize services. However, they frequently lack transparency regarding how this data is utilized. Additionally, while location-based services can improve navigation and offer personalized recommendations, they also track users' movements, which can infringe upon their privacy.[5]

- ***Protection against Government Surveillance:***

Government surveillance can significantly threaten individual privacy by compromising the core principles of consent, transparency, and proportionality. This intrusion often results in a chilling effect on free expression and association; individuals may be apprehensive about voicing dissenting opinions or participating in lawful activities that authorities might view as threatening. A notable illustration of this is the 2013 revelations by Edward Snowden, which brought to light the mass surveillance operations of the U.S. National Security

Agency (NSA). Programs like PRISM collected extensive data from leading technology companies and amassed metadata on millions of Verizon customers' phone calls. These disclosures underscore the alarming capacity of governments to monitor citizens' communications without their awareness, prompting serious concerns about widespread violations of privacy on a global scale.[5]

## HOW GOVERNMENT DEPARTMENT'S DATA IS STORED IN INDIA?

In India, government departments are increasingly leveraging cloud storage services provided by authorized private companies to handle vast amounts of data. Cloud computing offers the flexibility to rent software, storage, and servers as needed, avoiding the capital expenditure associated with setting up a complete infrastructure. The Ministry of Electronics and Information Technology (MEITY) has partnered with 11 private companies to supply these cloud computing services, enabling government entities to adjust their IT infrastructure according to demand, even for brief periods. This adaptability supports the rapid deployment of online services.[6]

The cloud computing guidelines are based on the MeghRaj Policy, which outlines a strategic framework for the adoption of cloud services within the government. The primary objective of this policy is to establish a cohesive Government Cloud (GI Cloud) environment, designed to be accessible by various government tiers, including central and state departments, districts, and municipalities. This initiative is geared towards enhancing Information and Communication Technology (ICT) services across government organizations efficiently and effectively.[7]

## EVOLVING THREATS TO DIGITAL PRIVACY IN INDIA:

The wave of digitalization in India has initiated significant transformations, with technologies such as Aadhaar, e-Governance, and digital payment systems like UPI fundamentally reshaping government operations. These advancements have prompted government organizations to adopt digital transformation strategies aimed at improving public services, optimizing operations, and fostering citizen engagement. While the digitization of various government services holds the potential for increased efficiency, it also raises critical concerns regarding the security and privacy of citizens' data, highlighting the risk of misuse and potential infringement on privacy rights.[6]

Several evolving threats to digital privacy in India warrant

attention:

1. The increasing frequency of cyberattacks exposes sensitive data, leading to serious privacy concerns.

2. he rapid growth of online transactions introduces vulnerabilities, making personal and financial information susceptible to unauthorized access and fraud.

3. Compliance with data localization laws poses difficulties for businesses and may hinder cross-border data flow, complicating the protection of personal data.

4. A general unawareness among citizens regarding digital security practices can exacerbate the risks associated with online activities.

5. As new technologies evolve, they present unique privacy challenges that necessitate constant vigilance and adaptation from regulatory frameworks to safeguard citizens' rights.

6. This evolving landscape requires ongoing research and proactive measures to protect digital privacy in India.[8]

***Balancing the Equation***

Navigating the intricacies of this field demands a comprehensive strategy that merges innovation with robust data protection measures. Below are some pivotal approaches to consider:

- Emphasizing transparency and accountability
- Implementing privacy by design principles
- Empowering individuals with control
- Ensuring security as a default standard
- Fostering collaboration and knowledge exchange

Governments have the opportunity to collaborate with one another and engage with private sector specialists to craft and execute robust data protection strategies. However, this undertaking is not without its hurdles. Resource limitations, intricate legacy systems, and various competing priorities often hinder progress. Achieving a balance between security, efficiency, and user experience is a complex task.

Nonetheless, several promising solutions are starting to take

shape:[9]

1. Innovative tools such as homomorphic encryption and secure multi-party computation facilitate the analysis of data while maintaining the confidentiality of individual information.

2. Researchers in this domain are focused on creating AI algorithms that prioritize fairness, eliminate bias, and uphold the privacy of individuals.

3. By gathering only the essential data required for specific objectives and safely discarding it post-utilization, organizations can significantly mitigate privacy concerns.

4. Establishing clear policies and procedures for data management promotes consistent and responsible handling of data across government agencies.

5. In early August 2023, the Indian Parliament enacted the Digital Personal Data Protection (DPDP) Act, marking a significant milestone as India's inaugural data protection legislation. This act creates a framework for the processing of personal data within India, applicable to data collected both online and offline, and subsequently digitized.[10]

***Whether data protection is a right?***

Data protection is recognized as a fundamental right in India, closely linked to the Right to Privacy, which encompasses the privacy of data. Without robust data protection, the essence of data privacy cannot be fully realized. Hence, data protection stands as an essential right in its own capacity.[11]

## NEED OF DATA PROTECTION IN INDIA

In an increasingly data-driven economy, corporations and large enterprises are recognizing data as a valuable asset, leading to a heightened focus on the storage, collection, and distribution of data. Consequently, there is a pressing need for robust measures to safeguard big data.

The Right to Privacy, which encompasses personal data, is recognized as a fundamental right in India. As such, the Indian government bears the responsibility of developing and enforcing legislation specifically addressing personal data protection. To effectively address the escalating threats posed by cyber-attacks, including identity theft and data breaches, it is essential to establish comprehensive legislation that incorporates stringent

penalties and a framework for redress.[10]

## EVOLUTION OF DATA PROTECTION LAWS IN INDIA

Data privacy has deep historical roots, dating back to the Semayne case of 1604, which established the notion that a person's home is their castle—a foundational belief in personal privacy. This concept continued to evolve, notably highlighted in the influential article "The Right to Privacy" by Attorney Samuel Warren and Justice Louis Brandeis. They argued that safeguarding privacy is essential to individual freedom in contemporary society.[9]

The recognition of privacy rights gained legislative acknowledgment in 1984 with the Universal Declaration of Human Rights (UDHR) in Article 12(4). Subsequently, in 1980, the Organisation for Economic Cooperation and Development (OECD) introduced guidelines to protect privacy and the transborder flow of personal data. Some countries, like Germany, began implementing data privacy laws as early as 1970. The landscape of data privacy underwent a significant transformation with the introduction of the General Data Protection Regulation (GDPR) on May 25, 2018, which set a new standard for data protection and privacy regulations worldwide.[8]

In India, the concept of privacy has long been a contentious issue within the judiciary. Various courts have approached the topic differently, with some recognizing privacy as a fundamental right, while others have refrained from acknowledging it under Article 21 of the Indian Constitution. The landmark ruling in 2017, *K.S. Puttaswamy v. Union of India*, ultimately established the right to privacy as a fundamental right protected by Article 21. Prior to this decision, there were elements addressing privacy in existing laws, such as the Information Technology Act (2000) and the Indian Penal Code (1860); however, a comprehensive, standalone law specifically focused on privacy was notably lacking. After several years of deliberation and three legislative attempts, India enacted a robust data protection and privacy law on August 9, 2023.[11]

## JUDICIAL PRONOUNCEMENTS IN INDIA

The right to privacy, now recognized as a fundamental aspect of our democracy, has not always held this status. Over the years, Indian jurisprudence has undergone significant evolution. The Supreme Court of India has played a crucial role in this journey, issuing a series of landmark rulings that have facilitated the organic development and expansion of privacy rights. This

analysis will explore the legal progression of the right to privacy over time.[11]

According to the case of *M. P. Sharma v. Satish Chandra (1954)*, earliest in India addressing the issue of the right to privacy. An eight-judge bench of the Supreme Court convened to evaluate the constitutionality of the search and seizure provisions under the Code of Criminal Procedure. In this instance, the Court did not acknowledge any legal right to privacy and determined that the actions of search and seizure did not infringe upon such a right. Given that the Indian Constitution does not include a specific provision protecting the right to privacy, it cannot be considered as being violated.[11]

In the case of *Mr. X v. Hospital Z* (1998), the court grappled with a conflict between two essential rights: the right to privacy and the right to public morality. The appellant, a patient, found that his medical conditions were publicly disclosed by the hospital. The Court upheld the right to privacy in this scenario, affirming that every individual is entitled to life and a healthy way of living under Article 21. It was noted that revealing even accurate private information can infringe on an individual's peace of mind and privacy.[10]

Such another case is that of *District Registrar and Collector, Hyderabad v. Canara Bank (2005)*, where the Hon'ble Court rules on the significance of financial privacy of an individual. It stated that the right to privacy also extends to maintaining the confidentiality of bank account details and related information as well. This decision basically widened the scope of the right to privacy and also covered the financial aspects of the right.[11]

While most courts did not explicitly acknowledge the right to privacy, India's highest court affirmed its existence in the significant ruling of *K.S. Puttaswamy v. Union of India (2018)*. In this landmark decision, rendered by a bench of nine judges, the court interpreted the right to privacy as falling under Article 21, which pertains to the right to life and liberty. By declaring that the right to privacy is fundamental to personal liberty and life itself, the Court overturned previous rulings in MP Sharma and Kharak Singh, which had maintained that privacy was not safeguarded under the Indian Constitution. The Bench stated in its judgment:[12]

- Recognizing the right to privacy does not entail amending the Constitution or granting a new freedom; instead, it is an interpretation of existing provisions. Privacy aims to

protect personal intimacies, sanctity of personal life, marriage, reproduction, sexual orientation, etc.

- Privacy also means the right to be left alone. Just because a person sets out his foot in a public place doesn't mean he surrenders all his rights to privacy. It is attached to a person, no matter where he is or goes.

- The Constitution must be interpreted liberally to allow growth and development with technological changes.

- Although the right to privacy is considered a fundamental right, it is not without limitations. Like other essential rights, it is subject to a framework of reasonable restrictions regarding its application.

- Privacy encompasses both positive and negative aspects. The negative aspect limits government actions that could infringe upon an individual's right to privacy, while the positive aspect signifies the obligation of the state to actively safeguard that right.

- Acknowledging the right to privacy as a fundamental right serves to shield individuals' personal domains from interference by both governmental and non- governmental entities. This right to privacy cannot be denied, regardless of the fact that it may affect only a small number of individuals.[11]

## CONCLUSION

The changing landscape of digital privacy within Indian Government organizations necessitates a thoughtful and comprehensive strategy. As India advances in digital transformation, it is crucial to strike a delicate balance between innovation and data security. Government bodies must not only adhere to changing regulatory standards but also cultivate an ethical and responsible approach to data usage. Moving forward, the expected advancements and updates in India's legal framework regarding data protection signify a proactive stance on tackling the challenges presented by cutting- edge technologies such as artificial intelligence and the Internet of Things. The adoption of sophisticated security technologies, alongside robust legislation, paves a promising path for safeguarding individual privacy rights while supporting the growth of the digital economy. In summary, it is evident that the evolution of data protection laws in India represents a progressive journey.

The path to achieving a balance between innovation and data

protection is an ongoing process. It demands a dynamic, adaptable, and cooperative approach from government entities, regulatory agencies, and the public. In this article, we have examined India's developing data protection laws, delving into their historical context, the important progress marked by the introduction of the Digital Personal Data Protection Act, 2023, and the challenges and implications these laws pose for businesses, individuals, and society as a whole. The legislation's progressive alignment with international standards highlights India's dedication to protecting personal data while creating an atmosphere that encourages technological growth and instills trust. As the digital realm continues to transform, so will the regulations governing data protection, requiring all involved parties to remain vigilant and adaptable.

## REFERENCES

1. "Data Protection: A Practical Guide to UK and EU Law" by Peter Carey

2. "Privacy Law Fundamentals" by Daniel J. Solove and Paul M. Schwartz

3. Pirvan, P. (2023). Safeguarding the Digital Frontier: An Overview of India's Privacy Rights and Digital Data Protection Bill 2023. DOI: 10.1732/IJLMH.25766

4. "The Personal Data Protection Bill, 2019: A Critical Appraisal" edited by Rahul Matthan and Anirudh Burman

5. "Cybersecurity in India: A Framework for National Security" by Balsing Rajput "The IT Act and Digital Policy: A Citizen's Guide to Digital Law and Rights in India" by Rohini Lakshané and Vanya Rakesh

6. Srinivasan, S., Sinha, V., Modi, S. (2023). Drafting a Pro-Antitrust and Data Protection Regulatory Framework. https://doi.org/10.55763/ippr.2023.04.05.003

7. Cook, A. V., Mariani, J., Kishnani, P., & Harr, C. (2019). How to begin regulating a digitalreality world.Deloitte Insights. Retrievedfrom (25.02. 2020): https://www2.deloitte.com/us/en/insights/industry/publicsector/regulating- digitalreality-augmented-spaces. html.

8. Information Technology (Amendment) Act, 2008 7- Personal Data Protection Act, 2023

9. Shruti Devan. K, An Analysis on Data Protection in India,

2-5, Indian Journal of Integrated Research in Law, Volume II Issue II, ISSN: 2583-0538, 2021.

10. Navmi Joshi, Dr. Monica Kharola, Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence, 59-60, International Journal of Law and Policy | Volume: 2 Issue: 4, IRSHAD, 2024.

11. Information Technology Act, 2000, No.21, Acts of Parliament, 2000 (India).

12. AI or Artificial Intelligence: A New Challenge for the Competition System in India, Legal Services India, https://www.legalserviceindia.com/legal/article-6978-ai-or-artificial-intelligencea-new-challenge-for-the-competition-system-in-india.html, (last seen on August 25, 2024)