INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION IN DIGITAL ERA: A CRITICAL ANALYSIS WITH SPECIAL REFERENCES OF DATA PROTECTION ACT, 2023

AUTHOR - MR. MD JIYAUDDIN & DR. SUNITA BANERJEE, ASSISTANT PROFESSORS OF LAW, VEL TECH RANGARAJAN DR SAGUNTHALA R & D INSTITUTE OF SCIENCE AND TECHNOLOGY, IMDJIYAUDDIN@GMAIL.COM

, **BEST CITATION -** MR. MD JIYAUDDIN & DR. SUNITA BANERJEE, DATA PROTECTION IN DIGITAL ERA: A CRITICAL ANALYSIS WITH SPECIAL REFERENCES OF DATA PROTECTION ACT, 2023, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (1) OF 2025, PG. 82-90, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

In an era marked by unparalleled digital data expansion and technological change, securing personal data has become a top priority for individuals, organisations, and governments throughout the world. The impact of social media on people's right to privacy has sparked considerable controversy. The importance of data protection has risen dramatically over the last several decades, reaching previously inconceivable heights as a result of global digitalisation, including India. The concept of "privacy" dates back to the dawn of human civilisation. However, comprehending privacy may be difficult. There is no commonly agreed definition of "privacy" among scholars since the term changes alongside society. The term "right to privacy" has developed to cover rights such as the right to be alone or to be anonymous, which have emerged throughout human history. Protecting this freedom is critical in today's world, given the proliferation of digital media. The implementation of the Digital Personal Data Protection Act, 2023, is significant in that it defines rules for the authorised handling of personal data, giving power and protecting individuals' rights. The DPDP Act's main goal is to increase the accountability and responsibility of organisations that operate inside Indian borders, such as internet companies, mobile applications, and companies that collect, store, and alter citizen data. Emphasising the 'Right to Privacy,' this law seeks to make sure that these organisations are transparent and answerable for how they handle personal information, therefore prioritising individual rights to privacy and data protection. Thus, examining the Digital Data Protection Act 2023 from a privacy perspective is pertinent.

Key Words: Digital data expansion, Technological change, Right to privacy, Unparalleled, Accountability and Responsibility

INTRODUCTION

In a time when digital information is constantly being exchanged and technology is constantly evolving, safeguarding personal information has become a major concern for people, businesses, and governments worldwide. In addition to changing how we communicate, work, and live our lives, the rapid growth of social media, e-commerce, and digital transactions has brought attention to the urgent need for strict privacy and data security regulations. The growing dangers to people's digital privacy and security highlight the urgent necessity to operationalise the Digital Personal Data Protection Act (DPDPA), 2023. The techniques and scope of cyberattacks are evolving along with technology, making people and organisations more susceptible to identity theft, data breaches, and spying. To create precise rules, regulations, and enforcement procedures to protect personal data, guarantee openness in data handling procedures, and hold organisations responsible for any breaches in cybersecurity protocols, comprehensive, strong, and rights-respecting data protection

legislation is necessary. Concerning gaps and weaknesses are shown by the DPDPA, 2023's shortcomings in protecting data privacy and enabling data principals in the case of a breach, as well as the dire condition of cybersecurity in the nation at the moment. Issues including inadequate funding, antiquated infrastructure, and a lack of qualified personnel continue to exist despite attempts to strengthen cybersecurity measures, such as the creation of specialised organisations and programs. There are significant questions regarding the accountability of an organisation whose actions or inaction have an impact on the nation's cyber security and individual privacy situation given that the Indian Computer Emergency Response Team (CERT-In), the nodal authority tasked with monitoring data breaches, was exempted from the Right to Information (RTI) Act, 2005 in 2023. This action is undoubtedly not in the public interest as it dilutes an Act intended to empower the people, so weakening their rights. However, critical concerns like data ownership are unclear, and there is a lack of a well-articulated access control system. This is due to the fact that most initiatives have public-private partnerships, which entail private entities gathering, analysing, and preserving vast volumes of data. This raises data security concerns in terms of data protection. As a result, the paper attempts to assess how the Act redefines the boundaries of data protection and privacy issues in India.

OBJECT AND APPLICABILITY OF THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023

- The fundamental goal of the Act is to create a comprehensive framework for the protection and processing of personal data.
- The Act provides for the processing of digital Personal Data in a manner that recognises both the rights of the individuals to protect their Personal Data and the need to process such Personal Data for lawful purposes and matters connected therewith or incidental thereto.
- The Act shall apply to the processing of Personal Data in India, including both online and digitised offline data, as well as the processing of such data outside India in connection with the provision of products or services in India.
- The Act also provides the groundwork for a number of additional legislations, including the Digital India Act and other industry-specific privacy and data protection rules, to help India accelerate the adoption of Artificial Intelligence (AI) and other future technologies while protecting personal data. The Act may also benefit Indian enterprises in improving engagement with other businesses situated worldwide under reciprocal arrangements while preserving personal data.

DEFINITION OF DATA

Section 2(h) of the Digital Personal Data Protection Act (2023) "Data" refers to a representation of information, facts, thoughts, views, or instructions in a format that allows humans or computers to communicate, interpret, or process it. Section 2(n) defines "digital personal data" as personal data in digital form, whereas section 2(t) defines "personal data" as any data about an individual that may be identified by or in connection to such data. 2(u) defines "personal data breach" includes any unauthorised processing of personal data or unintentional disclosure, acquisition, sharing, use, modification, destruction, or loss of access to personal data, which undermines the confidentiality, integrity, or availability of personal data.

Section 2(1)(o) of the Information Technology Act, 2000 defines "data" as "a representation of information, knowledge, facts, concepts, or instructions that are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards). The Digital Locker Authority's electronic consent framework defines 'data' as "any electronic information maintained by a public or private service provider (such as a government service department, a bank, a document repository, etc.). This can include both static and transactional documents. However, the idea of data is not limited to electronic information; it also includes information saved in physical form, such as on a sheet of paper."

CONCEPT

India's Digital Personal Data Protection Act, 2023 (DPDPA) is a comprehensive privacy and data protection law that recognises the right of individuals, known as data principals, to safeguard their personal data while it is processed for authorised purposes. The bill is the culmination of a seven-year journey that began in 2017 when the Indian Supreme Court determined that the right to privacy is protected by the Indian Constitution.

The DPDPA includes requirements on consent, legitimate uses, breaches, data fiduciary and processor obligations, and individual data rights. A person is defined as an individual, an undivided family, a corporation, a firm, an organisation, the state, and any "artificial juristic person." The legislation does not apply to paper data unless it is digitised or gathered for personal, creative, or journalistic purposes. The law does not set a date for enforcement, although several aspects are scheduled to take into effect in 2024, according to the official register. Fines for noncompliance vary from 10,000 Indian rupees for individuals to 2.5 billion INR for organisations, or around $120 to $30,000,000.

Evolving Threats to Digital Privacy in India

India has experienced a revolutionary wave of digitalisation, with e-Government, digital payment systems like UPI, and Aadhaar changing how the government operates. Government agencies use digital transformation to improve public services, increase efficiency, and interact with the public. The digitisation of many government services raises worries about the security and privacy of people' data usage and possible violations of their right to privacy, even while it promises increased efficiency.

i. **Data breaches and leaks, as well as cybersecurity attacks**: Attacks against cybersecurity, such as ransomware, malware, and phishing, are a continual threat to people and businesses. For nefarious or financial gain, attackers want to get sensitive data without authorisation. Identity theft, financial fraud, and the disclosure of personal information are all consequences of data breaches that can seriously damage a person's or an organization's reputation.

ii. **Dangers Associated with E-Commerce and Digital Payments**: As e-commerce and digital payments expand, they bring with them dangers including payment fraud, illegal access to financial data, and platform breaches. People could suffer from identity theft, financial loss, and interrupted internet transactions.

iii. **Problems with Data Localisation**: For businesses with intricate data processing processes, data localisation rules may pose difficulties in guaranteeing safe data management and storage in India. During localisation procedures, there may be difficulties with compliance and a higher chance of data unauthorised access.

iv. **Insufficient Knowledge**: It's possible that many people are unaware of the dangers to their digital privacy, safe online conduct, and the significance of protecting personal data. Lack of

understanding makes it more likely that one will become a victim of phishing scams, cyberthreats, and other types of online manipulation.

v. **Innovation in Technology**: Algorithmic bias and data manipulation are two new privacy issues brought about by the use of cutting-edge technology like blockchain, AI, and machine learning. When these technologies are used improperly, privacy hazards might increase, resulting in discrimination and a loss of control over personal data.

CRITICISM OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

While digital personal data protection is crucial, it has been criticised and scrutinised for a variety of reasons. The following are some typical complaints of data protection measures.

- **Ineffectiveness of Regulations**: Regulations are generally ineffective, according to critics, in deterring data breaches and privacy infractions. Some businesses may identify loopholes or suffer low penalties for noncompliance.
- **Lack of Enforcement**: Even when restrictions exist, enforcement may be lax. Regulatory bodies may lack the resources or power to effectively monitor and penalise businesses.
- **Data Monopolies**: Large technology businesses frequently gather massive quantities of personal data, raising worries about monopolistic control over people's information. Critics worry that large businesses can benefit from their dominance and may not be held accountable for data breaches**.**
- **Data Collection Practices**: Many digital platforms and services have come under fire for their extensive data collection practices. Critics argue that companies collect more data than necessary and use it for purposes that individuals did not consent to.
- **User Consent Challenges**: Obtaining informed consent from users for data collection and processing can be challenging. Critics contend that privacy policies are often lengthy, complex, and written in a way that makes it difficult for users to understand the implications of sharing their data.
- **Data Profiling and Discrimination**: Data-driven profiling and algorithms can lead to discrimination and bias, especially in areas like employment, housing, and financial services. Critics argue that data protection efforts should address these issues more comprehensively.
- **Data Security Gaps**: Despite data security measures, data breaches still occur. Critics argue that organisations frequently choose convenience above security and do not invest enough in securing personal data.
- **Lack of User Control**: Some believe that individuals have little control over their data after it has been acquired. They may be unable to access, amend, or remove personal data from databases, which is considered a breach of user rights.
- **Data Export and monitoring**: Some nations have laws forcing businesses to exchange data with government agencies, prompting worries about government monitoring and the possible abuse of personal information.
- **Data Resale**: Personal data is frequently bought and sold on data marketplaces, which some consider to be an ethical problem. Critics contend that people should have greater say over how their data is used and who benefits from it.
- **Overreliance on Consent**: Critics argue that the "consent model" of data protection places an undue burden on individuals to understand and maintain their privacy. Critics believe that there should be a greater emphasis on

reducing data collecting and guaranteeing data security by design.

- **Issues in Emerging Technologies**: As new technologies such as artificial intelligence and biometrics emerge, critics question the ability of current data protection methods to manage the particular issues created by these technologies.

RECENT DATA BREACHES IN INDIA

Organization	Details	Impact	Data Exposed	Hacker	Source
Boat Data Breach (April 2024)	**Data leak size:** 7.5 million boAt customers. **Dark Web Price:** 8 credits (around two euros). **Potential future availability:** Free on Telegram.	Increased risk of financial fraud, identity theft, phone scams, and email scams.	Names, addresses, email addresses, phone numbers, and customer IDs.	**ShopifyGUY** claimed responsibility	Money Control
Indian Telecom Data Breach (Jan 2024)	**Data Size:** 1.8 Terabytes (estimated 750 million records, impacting 85% of the Indian population). **Dark Web Price:** $3000 for the entire dataset. **Affected Parties:** All major telecom providers in India. **Significance:** Exposed vulnerabilities in government and telecom data security systems.	Financial loss, identity theft, cyber-attacks, and potential for future large-scale attacks.	Names, mobile numbers, addresses, and potentially Aadhaar information.	Threat actors named **CyboDevil** and **UNIT8200**	ToI
Sparsh Portal Data Leak (Jan 2024)	**Affected Personnel:** Primarily personnel from Kerala, India. **Possible Cause:** Malware named "lumma." **Severity:** Highlighted vulnerabilities in the TCS-developed SPARSH portal. **Additional Concerns:** Leaked data found on a Russian marketplace, raising possibilities of international criminal activity.	Increased risk of unauthorized access to pension accounts and potential financial loss.	Usernames, passwords, and pension numbers.	N/A	Business Standard

Hyundai Motor India Critical Data Breach (Jan 2024)	**Bug Details:** The bug involved web links shared by Hyundai Motor India via WhatsApp after customers had their vehicles serviced. **Exposed Information:** These links, leading to repair orders and invoices in PDF format, contained the customer's phone number. **Availability:** Customer's personal information in the South Asian market. **Current Situtaion:** Hyundai Motor India reported that bug is fixed now.	Increased risk of identity theft and fraud.	Registered owner names, Mailing addresses, email addresses, phone numbers, and vehicle details (such as registration numbers, colors, engine numbers, and mileage)	N/A	Techcrunch
Data breach of FreshMenu (Jan 2024)	**Data Exposed:** Over 3.5 million order details **Cause:** Unprotected 26GB MongoDB database (missing password).	Increased risk of identity theft, phishing attacks, and targeted scams.	Device information, email addresses, names, phone numbers, physical addresses, and purchase history	N/A	Techcircle
Data breach of UP Marriage Assistance Scheme site (Jan 2024)	Over 250 fraudulent applications submitted within two days. Funds transferred from accounts of 196 individuals. **Fraud Amount:** Over Rs 1 crore (Rs 1,07,80,000). **Target:** Uttar Pradesh's Marriage Assistance Scheme web portal. **Affected Portals:** UPLMIS.in and snauplmis.	Double payments to ineligible beneficiaries. Compromised ID of the Additional Labour Commissioner. Exploited connection to Uttar	N/A	N/A	India Today

		Pradesh Building and Other Construction Workers Welfare Board's portal (which administered the scheme).			
Data breach of documents containing data from EPFO, Indian PMO, and other public and private organizations	**Leak Platform:** Documents purportedly leaked on social media platform X (formerly Twitter). **Data:** No confirmation of what data was leaked (claims by attackers only). **Current Situation:** No concrete evidence of a breach beyond attackers' claims.	**Potentially Affected Entities:** Prime Minister's Office (PMO)Employees' Provident Fund Organisation (EPFO)Other public and private organizations (unspecified)	N/A	N/A	Economic Times

CONCLUSION

The numerous recent data breaches and leaks highlight how crucial strong cybersecurity measures are in the current digital environment. These examples, which range from breaches that compromise private data to weaknesses in large databases and platforms, demonstrate the many dangers that people and organisations must contend with. Proactive cybersecurity solutions, such as frequent audits, strong encryption methods, and quick incident response processes, must be given top priority by businesses in light of these difficulties. More accountability and openness are also desperately needed when it comes to resolving data breaches, as demonstrated by instances where impacted firms failed to recognise or appropriately manage the breaches in a timely manner. India's efforts to create comprehensive data protection laws have advanced significantly with the passage of the Digital Personal Data Protection Act, 2023. It has received praise for being a strong stand-alone data security system. When a person gives their information to reputable organisations, they may do so under the guise that it is secure and won't be shared with any other agencies or third parties without their permission. Furthermore, it appears contradictory that the DPDP Act, which was designed to safeguard data principals' rights, places obligations on them. It involves not pretending to be someone else when sharing

data, occasionally according to laws and regulations, not hiding any important information, not making baseless complaints against data fiduciaries, and providing accurate information. Another criticism of the legislation is that it weakens the RTI Act by prohibiting the disclosure of public officials' personal information. One area of worry among citizens was the Act's overriding impact on the RTI Act. In actuality, though, no data protection law can, in a legal sense, grant complete informational autonomy. A robust legislation, on the other hand, may ensure that the shared data is protected, protecting privacy in the process.

SUGGESTIONS

- Speak with the appropriate lawyers to make sure that the permission and privacy disclosure rules are followed and that "compliance and privacy by design" are ingrained in the procedures for gathering, storing, and using personal data in the course of conducting business.
- Determine and evaluate whether the company's handling of information, even if it is small, meets the statute's definition of "personal information."
- Create and put into place data management procedures and systems that will allow for statutory compliance, particularly with regard to the notice of consent obligation and consent recording.
- The ability to map data process flows and classify data will be essential for reacting to a customer exercising their legal rights. Being ignorant is not a defence.
- Adopt and operationalise the statute's provisions for the receipt and handling of consumer complaints.
- To successfully manage cyber and privacy risk throughout your company and to maintain resiliency, create a fully integrated, comprehensive risk management plan that prioritises people, capital, and technology safeguards.
- Create and prioritise regular, frequent, and continuously updated and improved trainings for staff members on data protection, cyber risk awareness, and process-related topics.
- Maintaining the confidentiality, integrity, and accessibility of third-party personal information entrusted to their care, custody, and control requires a regular auditing process of the technology and procedures used by third-party service providers, particularly data management subcontractors.

REFERENCES

- Rang Nath Pandey, *Law of Digital Personal Data Protection in India* (Sweet & Soft, 1st edn., 2024).
- George, L., (2023). Digital Personal Data Protection Act, 2023. Retrieved from https://www.techtarget.com/searchdatabackup/definition/Digital-Personal-Data-Protection-Act-2023#:~:text=India's%20Digital%20Personal%20Data%20Protection,or%20about%20$120%20to%20$30%2C000%2C000.
- Economic Laws Practice Advocates & Solicitors, "Data Protection & Privacy Issues in India" *e Economic Laws Practice*, 5-12 (2017).
- MINISTRY OF LAW AND JUSTICE. (2023). Digital Personal Data Protection Act, 2023. Retrieved from https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
- Anirudh, B., (2023). Understanding India's New Data Protection Law. Retrieved from https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en
- Sameer Asif, "Government Initiatives for Digital Inclusion and Data Protection in India" 9 *International Centre for Information Systems and Audit,* 12-19 (2024).

- Lalit, K., (2024). Decoding the Digital Personal Data Protection Act, 2023. Retrieved from https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023
- What Data is Protected by the India Digital Personal Data Protection Act 2023? A Comprehensive Guide to the India Data Privacy Law. Retrieved from https://secureprivacy.ai/blog/india-digital-personal-data-protection-act-2023-guide-protected-data
- Ishwar, A. & Sakina, K., (2023). Digital Personal Data Protection Act, 2023 – A Brief Analysis. Retrieved from https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis
- D.P. Mittal, *The Digital Personal Data Protection Act, 2023* (Commercial Law Publishers (india) Pvt. Ltd., 1st edn., 2024).
- Digital Personal Data Protection Act, 2023 – Key Highlights 2023. Retrieved from https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/
- Ali Talip P., (2023). India's Digital Personal Data Protection (DPDP) Act, 2023: everything you need to know. Retrieved from https://www.didomi.io/blog/india-digital-personal-data-protection-dpdp-act-2023-everything-you-need-to-know
- Demystifying the 'Digital Personal Data Protection Act 2023'. Retrieved from https://www.wtwco.com/en-in/insights/2023/07/digital-data-protection-bill-key-provisions-implications-and-recommendations-for-india-inc
- Ankita Yadav, *Right to Privacy and Data Protection Special Reference to India* (Satyam Law Internation, 1st edn., 2023).
- MAMTABEN D. P., (2023). Critical analysis of Digital Personal Data Protection Act, 2023: Safeguarding Privacy in the Digital Age, 11(8) International Journal of Research in all Subjects in Multi Languages, 37-41.
- Kavita, D., (2024). Critical Analysis of Digital Personal Data Protection Act, 2023 with reference to Right to Information Act, 2005, Educational Administration Theory and Practice journal 30(5):15209-15214, DOI:10.53555/kuey.v30i5.8548