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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION ACT IN INDIA: SPECIAL REFERENCES TO THE PRESENT NATIONAL ISSUES

AUTHOR - MR. MD JIYAUDDIN, ASSISTANT PROFESSOR AT SCHOOL OF LAW, BRAINWARE UNIVERSITY, BARASAT, KOLKATA, IMDJIYAUDDIN@GMAIL.COM

BEST CITATION – MR. MD JIYAUDDIN, DATA PROTECTION ACT IN INDIA: SPECIAL REFERENCES TO THE PRESENT NATIONAL ISSUES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (11) OF 2025, PG. 473-483, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

Protecting personal data has become a top priority for people, businesses, and governments throughout the world in an era characterised by an unparalleled growth of digital data and the unrelenting advancement of technology. The impact of social media on people's right to privacy has sparked considerable controversy. The importance of data protection has grown dramatically over the last several decades, reaching previously inconceivable heights as a result of global digitalisation, especially in India. Overall, data protection is more concerned with personal liberty, fairness, human dignity, individuality and family life. Data protection is generally recognised; nonetheless, the method of coding data is relatively recent. Because societies are always developing, there is an urgent need to redefine data protection. The article also looks at the technological components of data privacy, such as data encryption, anonymisation, and localisation restrictions, and how successful they are in protecting personal data. Furthermore, the article examines the obstacles that Indian organisations experience while implementing data privacy safeguards and recommends best practices for overcoming these challenges. By providing useful insights into the existing status of data privacy in India, this paper makes recommendations for improving data protection policies, which would benefit people, organisations, and society as a whole. This research paper also discusses legislative provisions, such as the Personal Data Protection Act of 2023 and the creation of regulatory organisations to protect privacy.

Key words: Digital data, Right to privacy, Data protection, Indian organisations, Safeguards and Recommends.

INTRODUCTION

Data privacy has emerged as a critical concern in today's digital age, as many entities acquire, exchange, and handle personal information. As India advances digitally, data privacy becomes more crucial than ever. India is facing several challenges and complaints as a result of a lack of data protection regulations and information security safeguards. The globe is also experiencing an increase in cybercrime.[753] Data theft and unlawful information transmission occur all across the cyber globe since the internet disregards physical jurisdictions. Globally, India is a super host for outsourced data processing, which has made it an epic centre of virtual offences in the lack of adequate cyber regulation. Though the Data Security Council of India and the Department of Information Technology are working to re-build data security infrastructure. However, the greatest approach is to prevent the criminal from committing the offence by raising public and private digital awareness. It is a critical time for the globe to make significant and universal measures for data protection and safety, as well as cyber security, as we observe

[753] Alafaa, "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World" (2022), *available at*: https://ssrn.com/abstract=4005750 (last visited on 14th March, 2025).

widespread digital reformation. There are several incidents of data breaches, as well as instances where the security of PMO, intelligence agency, or defence websites has been jeopardised. Furthermore, "we cannot simply declare a cat to be a tiger." India's cyber law must also be supported by robust cyber security and competent cyber forensics.[754] Companies and organisations, particularly those offering IT and BPO services, have a large information reservoir storing all types of secret, sensitive, or personal data around the globe. It also includes information about debit or credit card transactions, financial credentials, and significant movable or immovable goods. Typically, all such personal or organisational data are saved in electronic form. It is also susceptible when in the hands of their employees, since it is misused by unscrupulous individuals for monetary gain. In our nation, there have been several cases of security breaches and data leaks, including from well-known IT businesses.[755]

The present privacy issue focusses on third-party policies surrounding the information they gather and retain, such as whether it is secure or maintained, who has access to it, and under what terms. The government and commercial players collect, create, and own large datasets. For the government to provide welfare services, most of these massive datasets are either collected by private technology companies, administered by private parties, or obtained by the government itself. Large volumes of data are kept by a number of Indian government organisations, including the Income Tax Department, the Ministry of Rural Development for the Mahatma Gandhi National Rural Employment Guarantee (MGNREGA), the Stock Exchange, the Census of India, and the Unique Identification Authority of India (UIDAI).[756] The Central Monitoring System, Human DNA Profiling, the Smart Cities Mission, and the Digital India program are just a few of the several projects for which the Indian government keeps enormous data. Along with the government, a number of non-state actors, including telecom companies, online retailers, and travel agencies, are using big data analytics to market their businesses. As of November 2021, 86.63 million people in India were compromised, placing the country third in terms of data breaches, according to Business Today. Data breaches are regarded as one of the most prevalent forms of cybercrime and violate consumers' privacy. These breaches include the sale or sharing of personal information with third parties for analytics or cybercrime purposes, such as name, sex, phone number, address, passwords, and unique identifying numbers. The 2021 Air India personal data breach involving 4.5 million passengers, the 190,000 PII test results from the Common Admission Test (CAT) 2020, and the COVID-19 lab test that were stolen via government websites are a few instances of data breaches in India.[757]

REVIEW LITERATURE

Sujay H. Deshpande, 'Data Privacy in India Technical and Legal Perspective',[758] the author in this detailed research provides an in-depth review of the data privacy situation in India, focussing on both technological and legal aspects. It includes an overview of India's current legislative structure and regulatory environment, as well as a review of industry practices. The author also looks at the technological components of data privacy, such as data encryption, anonymisation, and localisation restrictions, and how successful they are in protecting personal data.

[754] Ajinkya Kawale, "One-third of organisations report data breaches costing over $1 mn in 3 yrs" (2024), *available at:* https://www.business-standard.com/industry/news/one-third-of-organisations-report-data-breaches-costing-over-1-mn-in-3-yrs-124112100702_1.html (last visited on 16th February, 2025).

[755] Komal Arora, "Data Protection and Data Privacy Laws in India" (2024), *available at:* https://blog.ipleaders.in/data-protection-laws-in-india-2/ (last visited on 21th March, 2025).

[756] Anirudh Burman, "Understanding India's New Data Protection Law" (2023), *available at:* https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited on 28th May, 2025).

[757] "Top 5 Recent Data Breaches in India" (2024), *available at:* https://www.dpdpconsultants.com/blog/top-5-recent-data-breaches-in-india-2024-2.php (last visited on 19th March, 2025).

[758] Sujay H. Deshpande, "Data Privacy in India Technical and Legal Perspective" *Social Science Research Network,* 1- 8 (2018), available at: https://ssrn.com/abstract=4420148

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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

Furthermore, the author examines the obstacles that Indian organisations experience while implementing data privacy safeguards and recommends best practices for overcoming these challenges.

Economic Laws Practice Advocates & Solicitors, 'Data Protection & Privacy Issues in India',[759] the authors have thoroughly examined the requirements of the Information Technology Act of 2000. The authors have highlighted various grey areas in the Acts, such as data protection and privacy issues in India. The authors have also proposed corrective amendments based on Indian jurisprudence on the right to privacy, current issues surrounding data privacy, and concerns and difficulties in order to strengthen the Act.

Sameer Asif, Government Initiatives for Digital Inclusion and Data Protection in India',[760] in this article, the author analyses India's digital transformation, focusing on the interconnected goals of digital inclusion and data protection. It emphasises government efforts such as Digital India and PMGDISHA, both of which aim to improve marginalised people's access to technology and digital literacy. Despite progress, issues such as geographical inequality and increased cybercrime remain. The author also discusses legislative attempts, such as the Personal Data Protection Act of 2023 and the creation of regulatory agencies to protect privacy.

OBJECTIVES

- To analysis data protection laws and regulations in India.
- To make a relationship between data protection and the right to privacy.
- To discuss evolving threats to digital privacy in India.
- To explain recent data breaches in India.

DATA PRIVACY AND DATA PROTECTION

Indian civilisation is rapidly evolving towards digitisation and digital financial infrastructure. As a result, India has liberalised foreign investment regulations and legislation. To acquire the status of developed nation, the FDP (Foreign Direct Investment) and PPP modals (Public Private Participation) have been accepted and implemented.[761] These favourable initiatives are intended to encourage an increasing number of international players to participate in the make in India effort. To comply with global economic reforms, we changed India into a digitally empowered nation through the application of numerous cyber approaches, as well as the recognition of e-transactions and e-governance, among others. Every excellent item has certain advantages, and information technology is no exception. International investors arrive in India with sophisticated international standards for "data protection" and "data privacy," expecting India to be a similarly cyber-empowered country that satisfies those criteria at the very least. It's interesting to note that no Indian law, including IT laws, specifically defines data privacy. The concept of privacy has occasionally been entangled by the Indian judiciary in its interpretation of the right to life and personal liberty guaranteed by Article 21 of the Indian Constitution. In accordance with Article 21 of the Indian Constitution, the supreme court has definitively ruled that the right to privacy is a basic right.[762] However, this right might be enforced against the State, raising conflicting problems about which legislation governs the non-state related aspects of privacy breach.

RELATIONSHIP BETWEEN DATA PROTECTION AND THE RIGHT TO PRIVACY

- The indisputable normative reality is that there is a connection between the data protection laws and the right to privacy. There is a genuine relationship between

[759] Economic Laws Practice Advocates & Solicitors, "Data Protection & Privacy Issues in India" *e Economic Laws Practice*, 5-12 (2017).

[760] Sameer Asif, "Government Initiatives for Digital Inclusion and Data Protection in India" 9 *International Centre for Information Systems and Audit,* 12-19 (2024).

[761] *Ibid.*

[762] M P Jain, *Indian Constitutional Law* (Lexis Nexis, 8th edn., 2018).

the right to data protection and the right to privacy, despite the fact that these two abstract concepts are probably logically exclusive. The argument that data protection laws have advanced so far is based on the fact that the right to privacy has been recognised as a fundamental right. However, the right to privacy must be precisely and unambiguously defined for the purposes of the Data Protection legislation. The concept of the right to privacy is conceptual in nature, and there is much ambiguity among national lawmakers over a clear definition of this right.[763]

- Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others is one of the most widely accepted interpretations of the right to privacy in the context of personal information protection. That is the "Right to Self-Determination". It is an ideology that has a lot of weight in any democratic structure, and it wields a lot of power over the people. Though individuals have the right to self-determination, data that has been supplied must be protected from being shared with others in order to preserve their privacy. Therefore, it's vital to understand what data protection is.[764]
- The word "data protection" refers to the processes, safeguards, and legally binding rules put in place to secure the personal information you supply and ensure that you keep control over it. In a word, one should be able to choose whether or not to divulge specific information, who should have access to it, for how long and for what purpose, and the ability to alter some elements of this information, among other things. According to jurists, the term data protection is a catch-all for anything related to the processing of personal data. This is because the term data protection is used to cover everything related to the processing of personal data.[765]
- In general, the terms "personal data" and "processing" refer to two aspects of data protection rules. Because the definition of processing is as wide as the entire data protection laws, it should be defined in a flexible manner in order to broaden the scope of the protection provided by the law. Processing refers to any tangible activity that has a direct impact on data, which includes data collection, storage, utilisation, and delivery. The great majority of sophisticated data protection laws argue for the broadest possible interpretation of the word. It must be acknowledged that allowing the definition of "processing" to be interpreted in an excessively wide way would defeat the purpose of having data protection laws. The concept of "Personal Data" is, predictably, the second element of the Data Protection Laws. Anything that could be used to identify a person or any information that could be connected to a person's unique identity is included in this term. Anything that may be used to identify a group of individuals is also included.[766]

[763] Jon Toor, "What is Data Protection and Privacy?" (2024), *available at:* https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/#:~:text=Although%20both%20data%20protection%20and,not%20represent%20the%20same%20thing.&text=Data%20privacy%20is%20focused%20on,focuses%20on%20applying%20those%20restrictions (last visited on 24th May, 2025).

[764] Janvi Shukla, "Right to Privacy and Data Protection era" (2023), *available at*: https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html?__cf_chl_tk=9dR2NR8AsP1oTag32g0c80N6LGxnBqvffl2lnIAHjcw-1736407725-1.0.1.1-eirBDHGT8iLSBIRZO9DmK4QjdOqkoDuljvhKL2_2TSY (last visited on 18th March, 2025).

[765] Manoj Roy Sarkar, "The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government"9 *International Centre for Information Systems and Audit* 23-29 (2024).

[766] Ankita Yadav, *Right to Privacy and Data Protection Special Reference to India* (Satyam Law Internation, 1st edn., 2023).

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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION LAWS & REGULATIONS IN INDIA

India's data protection has evolved significantly in recent years, with the implementation of essential legislations and laws aimed at securing individuals' personal data and ensuring privacy in the digital era.

Information Technology Act of 2000: The Information Technology Act of 2000 is India's fundamental legislation covering electronic transactions, digital signatures, and cybercrime. The IT Act of 2000, enacted to offer legal status for electronic records and enable e-commerce operations, paved the way for resolving cybersecurity problems and preserving digital assets. The IT Act of 2000 created the legal basis for digital transactions and cybersecurity, but the lack of comprehensive data protection laws demanded further legislative measures. However, the IT Act of 2000 has measures to address cyber concerns and difficulties, such as those pertaining to data or information protection. The scope of access to data kept on a computer, computer resource, computer-based devices, or computer network is defined under the IT Act. However, it does not increase the need for strict data privacy regulations. The requirements to address the growing problem of cybercrimes were included in the revised IT Act of 2008. Two new provisions, sections 43A and 72A have been added to create a robust legal framework for data protection. However, these clauses are insufficient to guarantee data security and privacy.

- **Compensation for failure to protect data**: According to section 42A of the IT Act 2008, if a company that owns, controls, or operates a computer resource that contains sensitive personal data or information is careless in putting in place and upholding appropriate security practices and procedures and as a result causes someone to suffer an unjustified loss or gain, the company will be responsible for compensating the affected party with damages up to five crore rupees.
- **Punishment for publication of information in violation of a legitimate contract**: According to section 72A of the IT Act 2008, except as otherwise provided in this Act or any other law currently in force, any person, including an intermediary, who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material.[767]

Proposed Digital India Act, 2023: The proposed Digital India Act 2023 establishes a more comprehensive legal framework for digital governance, cybersecurity, and data protection. The Act, which includes requirements for data localisation, cross-border data transmission, and cybersecurity safeguards, aims to build India's digital infrastructure and foster confidence in the digital ecosystem. The proposed Digital India Act 2023 supplements the Personal Data Protection Act 2023 by addressing crucial concerns including data sovereignty and cybersecurity risks, strengthening India's commitment to preserving digital assets and fostering responsible data management practices.

Personal Data Protection Act, 2023: An important turning point in India's data protection history is the Digital Personal Data Protection Act 2023, which is derived from the Digital Personal Data Protection Bill that was proposed in 2019. The Act seeks to protect people's right to privacy in the digital sphere and govern the handling of personal data. It lays up guidelines for the gathering, storing, processing, and sharing of personal information

[767] Mathew Chacko and Aadya Misra, "India - Data Protection Overview" (2024), *available at:* https://www.dataguidance.com/notes/india-data-protection-overview (last visited on 20th December, 2024).

while giving people rights including the ability to view, update, and remove their personal information. In order to enforce data protection regulations, regulate data processors and controllers, and resolve disputes pertaining to data protection violations, the Act also requires the creation of a Data Protection Authority (DPA).[768]

Ministry of Electronics and Information Technology (MeitY): MeitY is essential in developing data protection policies and laws, supervising the IT Act 2000's implementation, and encouraging cybersecurity efforts across a range of industries.

Sectoral Regulators: To ensure adherence to industry-specific data privacy standards, several sectors, including banking and telecommunications, have their own regulatory bodies (such as the Reserve Bank of India and the Telecom Regulatory Authority of India).

Judiciary: By interpreting statutory legislation and constitutional requirements, the Indian judiciary is crucial in deciding data protection cases and establishing precedents that influence the developing field of data protection jurisprudence.

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.[769]

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.[770]

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

[768] MINISTRY OF LAW AND JUSTICE, THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023), *available at*: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf (last visited on 15th March, 2025).

[769] R. Jayaprakash, "Digital Data Protection: Role of SAI" 9 *International Centre for Information Systems and Audit* 23-29 (2024).

[770] Id 13.

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.

CURRENT ISSUES DATA BREACHES IN INDIA

India had multiple data breaches in 2024. In September, millions of personal documents, including medical information for Star Health Insurance clients, were exposed online. A UK-based researcher originally disclosed the incident, claiming that the data had been acquired by a hacker dubbed xenZen. Angel One, a Mumbai-based stockbroking business, exposed personal information of around 7.9 million clients in July, revealing critical details such as bank accounts. Previously, in January, a huge breach revealed 750 million individuals' personal data, including Aadhaar information, and the data was sold by threat actors online. According to July research provided by IT giant IBM, the average cost of a data breach in India would reach an all-time high of Rs 19.5 crore in the first half of 2024.[771] This was a 9% increase over the previous year and a whopping 39% increase since 2020. These expenditures were not just financial, but also included operational interruptions. Globally, 70% of compromised organisations experienced substantial interruptions due to data breaches.[772] According to a survey by think tank Data Security Council of India (DSCI), India detected an average of 761 cyberattack attempts every minute this year, with the healthcare industry being the most targeted, followed by banking and hotels.[773]

The Hon'ble Supreme Court has established three requirements for the State's interference with basic rights.[774] While the State may intervene to protect legitimate state interests, (a) there must be a law in existence to justify an encroachment on privacy, which is an express requirement of Article 21 of the Constitution, (b) the nature and content of the law imposing the restriction must fall within the zone of reasonableness mandated by Article 14, and (c) the means adopted by the legislature must be proportional to the object and needs sought to be fulfilled by law. Therefore, any future legislation that aims to violate someone's right to privacy must pass the proportionality and reasonableness test. Before jurisprudence about what qualifies as fair and proportionate State interference settles down for the foreseeable future, a few years will pass. Based on this ruling, the Adhar Scheme's legitimacy will now be examined.[775]

It is frequently claimed that India should adopt a 'rights-based' data protection paradigm rather than the current consent-based model. Under the consent-based approach, the data controller is free to use, process, and share the data with other parties once the user's approval has been gained. However, many people are unaware of the true effects of indiscreet data sharing when they provide consent. On the other hand, the 'rights-based' approach gives users more control over their data while requiring the data controller to guarantee that such users' rights are not violated. This gives users greater control over their personal data. The Hon'ble Supreme Court's ruling gives Indian residents the ability to file a lawsuit if their data privacy rights are violated. This may affect the privacy and security measures that Indian IT businesses have put in place. Users have the ability to

[771] Shravani Nag Lanka, "IFF's cybersecurity report for the third quarter of 2024" (2024), *available at:* https://internetfreedom.in/iffs-cybersecurity-report-for-the-third-quarter-of-2024/ (last visited on 26th May, 2025).
[772] Prakriti Bakshi, "India's Data Breach Crisis Exposes Regulatory Gaps" (2024), *available at:* https://thesecretariat.in/article/india-s-data-breach-crisis-exposes-regulatory-gaps (last visited on 19th March, 2025).
[773] Collaco, A. M, "Contours of data protection in India: the consent dilemma" *International Review of Law, Computers & Technology*, 1–19 (2024), *available at:* https://doi.org/10.1080/13600869.2024.2364991 (last visited on 14th March, 2025).
[774] D.D. BASU, *Introduction to The Constitution of India* (Lexis Nexis, 24th edn., 2019).
[775] Khushi Chopra and Surya Pratap K., **"**From Constitutional Rights to Data Protection: Article 21 and Comparative Perspectives on Privacy" (2024), *available at:* https://articles.manupatra.com/article-details/From-Constitutional-Rights-to-Data-Protection-Article-21-and-Comparative-Perspectives-on-Privacy (last visited on 17th March, 2025).

assert their basic right to privacy in addition to tort-based claims.[776]

[776] D.P. Mittal, *The Digital Personal Data Protection Act, 2023* (Commercial Law Publishers (india) Pvt. Ltd., 1st edn., 2024).

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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

RECENT DATA BREACHES IN INDIA IN 2024[777]

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, e mail addresses, phone numbers, and customer IDs.	**Shopify GUY** clai med responsi bility	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 **CyboDe vil** and **U NIT8200**	ToI
Sparsh Portal Data Leak (Jan 2024)	**Affected Personnel:** Primarily personnel from Kerala, India. **Possible Cause:** Malware named "lumma." **Severity:** Highlight ed 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	Busines s Standa rd

[777] "Case Study On Recent Data Breach In India In 2024" *available at:* https://cybervie.com/case-study/case-study-on-recent-data-breach-in-india-in-2024/ (last visited on 28th May, 2025).

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 Pradesh Building and	N/A	N/A	India Today

		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

Data protection and privacy are essential for protecting personal information in the current digital era. For security purposes, people's personal information is crucial. An important step in India's efforts to create thorough data privacy laws is the Digital Personal Data Privacy 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. One step in that direction is the DPDP Act.[778] India's advancement in this area is essential to bringing it into compliance with international norms since data privacy is still vital. The DPDP Act, however, has come under heavy fire for rushing the Digital Personal Data Protection Bill, 2023 through both chambers of Parliament without conducting a thorough debate. Certain aspects are up to the Central Government's judgement, which raises concerns about unbridled rulemaking and possible regulatory gaps. Furthermore, the DPDP Act's obligation to data principals appears contradictory given that its purpose was to safeguard their rights. It involves refraining from impersonating oneself while sharing data with others, occasionally adhering to legal requirements, hiding any important information, refraining from baseless complaints against data fiduciaries, and providing accurate information. The law is also criticised for weakening the RTI Act, which prohibits the disclosure of public officials'

[778] Rang Nath Pandey, *Law of Digital Personal Data Protection in India* (Sweet & Soft, 1st edn., 2024).

private information. Citizens were concerned about the Act's dominating impact on the RTI Act. It is a fact, therefore, that no data protection law can, in theory, grant complete informational autonomy. However, a robust legislation may ensure that the shared data is protected, protecting privacy in the process.