 ***DOI:*** *https://doij.org/10.10000/IJLMH.119649*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

**[ISSN 2581-5369]**

**Volume 8 | Issue 3**

**2025**

# Data Protection Framework in India: Criticism and Comments

IMRAN KHAN[1]

## ABSTRACT

*The following article examines the various deficiencies in the Digital Personal Data Protection Act, 2023. Specific attention is directed to the vacuum created for the consensual use of personal data and the transferring of such data to third parties in the said Act. The extent of the fiduciary relation between the Data Principal and the Fiduciary is liable to be corrected as this has serious repercussions on implementation of the said Act. Specific loopholes in the wording of the DPDP Act, 2023 demonstrate that the Act is insufficient to protect intentional illegal processing of personal data. In the opinion of the author, the grievance redressal mechanism has to be radically altered to ensure decentralised redressal of data leaks and violation of privacy. The article, inter alia, explores how even with the existence of consent, data privacy is likely to be exploited for commercial gain, specifically in relation to insidious marketing practices.*

## I. NATURE OF RELATIONSHIP BETWEEN THE PARTIES

The Act purports to form a contract between the Data Principal and the Data Fiduciary. However the relation between a Data Fiduciary and a Data Principal is a fiduciary relation and not a contractual one. The mechanism for obtaining the consent of the principal is based on a contract where consent to process data is the consideration for accessing the services for the Data Fiduciary. Contract law is easy to enforce and implement. However, it is very difficult to regulate, let alone punish for derogation from the law, if it is understood that the transaction is based on fiduciary relations between the parties. Thus the DPDP Act, 2023 specifies a fiduciary relationship between the parties.

## II. UNAUTHORISED PROCESSING OF PERSONAL DATA- A LEGITIMATE LOOPHOLE?

Section 2 (u) of the DPDP Act defines personal data breach as "*any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data."*[2] However the definition is not comprehensive of what would be misuse of

[1] Author is a student at Government Law College, Mumbai, India.
[2] The Digital Personal Data Protection Act, 2023, Section 2(u), No. 22 of 2023

 [ISSN 2581-5369]

personal data. Misuse of personal data would be any use of data other than the agreed purpose[3].

The General Data Protection Regulation (GDPR 2018), as enacted by the European union clearly distinguishes between personal data and sensitive personal data. It defines personal data as ‘‘Any information relating to an identified or identifiable natural person. It defines sensitive personal data as a specific set of ‘special categories’ which includes

- Genetic data
- Political opinions
- Racial or ethnic origin
- Data concerning health
- Trade union membership
- Religious or philosophical beliefs
- Data concerning sex life or sexual orientation
- Biometric data (where processed to uniquely identify someone’’[4]

Article 9 of the GDPR specifically outlaws processing of abovementioned types of sensitive personal data. The definition of personal data under the DPDP Act is very terse and the Government of India has left it upon the Courts to interpret what would constitute personal data under the terse statement of any personal data.

The Act nowhere punishes unauthorised processing of personal data in its entirety and has rather, allowed a loophole for the unauthorized processing of personal data. Perhaps, the biggest loophole in the entire Act, is that the Data Fiduciary has been allowed to process personal data for any purpose other than that which the Data Principal has not expressly indicated consent to. How will the Data Principal as defined in the Act come to know if the data has been used for anything other than the agreed purpose? Thus section 7 of the Act stands contrary to the basic principles of contract law.

*‘‘7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely: —*

*(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary*

[3]Swaroop Sham, *What Is Data Misuse?* OKTA BLOG, (Mar 27, 2025, 8: 16 PM), https://www.okta.com/blog/2020/06/data-misuse/

[4]REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018

*that she does not consent to the use of her personal data*[5]*."*

The presence of data brokers in the digital landscape is a major threat to the enforceability of this Act. These are companies whose primary business is to sell personal data. Tools like web scraping enable them to extract vast information from the online user. Elea Feit, senior fellow at Wharton Customer Analytics has made the following observation, "whether it's a mom-and-pop shop such as the corner tailor who keeps track of clients' shirt sizes and preferences or a big corporation like Walmart, companies track their customers to give them a better customer experience and provide relevant goods and services. They want to look at a customer's purchasing pattern so they can tailor experiences to that customer," [6] Thus, Data is a resource, especially in the marketing world.

## III. THE MECHANISM OF GRIEVANCE REDRESSAL

Section 8 of the Act says:

*"8. General obligations of Data Fiduciary*

*(1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.*

*(2) A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract"*[7]

There is no clarity as to whether the contract as envisaged in subsection 2 of Section 8 of the DPDP Act, 2023, excludes the Data Principal or includes it. To leave large parts of the Act unexplained is bound to have legal consequences. The Act focuses more grievance redressal rather than compliance and ensuring best data practices. With regard to the grievance redressal provisions in the Act, question arises as to how the Consumer will ever come to know that his personal data is being used in violation of the consent he has given under section or that a cybersecurity data breach has occurred.

[5] The Digital Personal Data Protection Act, 2023, Section 7, No. 22 of 2023

[6]The Wharton Staff, *Your Data Is Shared and Sold… What's Being Done About It?* KNOWLEDGE AT WHARTON, (17 Apr, 2025 10: 35 AM), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/

[7] The Digital Personal Data Protection Act, 2023, Section 8, No. 22 of 2023.

 [ISSN 2581-5369]

## IV. NATURE OF THE DATA PROTECTION BOARD

Another strong criticism of the Act is with regard to the nature of the proposed data protection board. The data protection board has been essentially given 'litigation powers' under Section 27 and 28 of the Act. It remains to be seen how practicable it will be for a centrally constituted board to effectively address thousands of future individual data breach complaints. The fact is that another statutory body has been constituted to address the sacrosanct issue of data integrity. In India, statutory bodies have a history of failing in their stated missions. Take for example the pollution control boards that have been appointed under the various environment related legislations. The most common scenario is that these bodies are rendered useless due to overlapping government interests in the cases that are placed before these bodies. In essence the data protection board has been created as a grievance body with no powers of independent checking of data practices. The problem is further exacerbated as the rules of the DPDP Act 2023, direct the Data fiduciaries to undertake an audit of their own companies by themselves to the exclusion of the data protection board. This is called the data protection impact assessment. Government interest remains a significant challenge in most statutory authorities as the purpose for the activation of these bodies has always been an administrative function. Thus these bodies are by design bound to fail in their stated objectives. Undoubtedly the government has skin in the game with regard to the misuse of personal data.

## V. COMPANY DATA PRACTICES AND REGULATION

A major challenge will be to prevent intentional data sharing and transmission between companies. Since the relation between the consumer and Data Fiduciary is a fiduciary relationship, there is no adequate system of checks and balances in the process of data protection. Accordingly, what was needed in the Act was a good system to be prescribed upon companies for data profiling practices[8]. The DPDP Act has placed too much reliance on the consent of the Data Principal which will be immaterial. This problem is proved by the following example. A company named A collects data from its consumers, after giving them a notice that the said data will be shared with third parties for efficient data processing. The Company A shares the data with Company B which is known for selling and abusing data. The said Company B is not liable to the consumer in any scenario for any breach of data. In such a case the consent given by the Data Principal will not prevent a data breach, especially if the given

[8] *Data selling 101: protecting your business and your customers' privacy*, USERCENTRICS, (Apr 20, 2025, 03:30 PM), https://usercentrics.com/knowledge-hub/data-is-the-new-gold-how-and-why-it-is-collected-and-sold/

commodity or service being sold by the Data Principal is scarce or critical in nature.

Remedy to a data breach must be preventive. If a company is rolling out a consent mechanism, it must first verify the same as being foolproof with a competent authority. If data is indeed seen as a precious resource, preventive action is a must. This is because loss of data security is irreversible damage that cannot be corrected.

The Srikrishna committee in its report noted that, to obtain consent should not be a compulsion in all circumstances. In order to limit the scope of non-consensual data processing, it specified separate four grounds based on which data can be processed in a non-consensual manner. "These are:

(i) where processing is relevant for the state to discharge its welfare functions,

(ii) to comply with the law or with court orders in India,

(iii) when necessitated by the requirement to act promptly (to save a life, for instance), and

(iv) in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer)."[9]

Question arises as to why individual consent is not possible in all cases. In the Cambridge Analytica - Facebook scandal of 2018, a company called Cambridge Analytica had harvested data of thousands of users was leaked without their consent with active conniving by Facebook. The scandal came to light only after a whistleblower himself, provided this confidential information to the Observer. The whole scandal did not involve any security breach as is usually understood in cyber data protection, rather it involved Facebook itself intentionally and actively allowing the Company to exploit the platform.[10]

The problem compounds with the introduction of Language AI models that are data hungry to the point that these language models scrape data from the four corners of the internet[11].

In 2019, Twitter (now X) disclosed and admitted that phone numbers and email addresses of users processed for account security had been shared with third party advertisers without the explicit consent of users[12]. The entire admission by Twitter in a blog post was completely

[9] *Report Summary on A Free and Fair Digital Economy*, PRS INDIA (Apr. 23, 2025, 4: 58 PM), https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy

[10] Carole Cadwalladr *and* Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* THE GUARDIAN, (Apr 20, 2024, 1:24 PM) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[11] Katharine Miller, *Privacy in an AI Era: How Do We Protect Our Personal Information?* STANFORD UNIVERSITY HAI, (Apr 23 2025, 5:13 PM), https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information

[12] Queenie Wong, *Twitter Profited from Users' Data Without Their Consent, Lawsuit Alleges*, CNET (Apr 15, 2025, 10: 27 AM) https://www.cnet.com/tech/services-and-software/twitter-profited-from-users-data-without-

voluntary. The U.S. Federal Trade Commission then launched an investigation into Twitter's data sharing practices. It is to be noted that, had twitter not voluntarily disclosed this breach of data, there would have been no investigation into the company's data sharing practices.

The marketing of sensitive data must be made unlawful. This sensitive data is sufficient to be defined as provided under the GDPR 2023. Even if the user consents to his personal data to be used for targeted advertising and marketing, it should nevertheless be an obligation upon the Data Fiduciary to secure the sharing and processing of data. It is observed that marketing itself is an insidious practice, as it involves the processing of data without the user's explicit consent. Marketing of data leads to an erosion of trust. How then is the relation between a Data Fiduciary and a Data Principal to be considered a fiduciary one?

A solution to the above problem lies in strengthening the contractual mechanism involved in taking consent of the user. A standard form of notice as provided under section 5 of the DPDP Act can be prescribed which gives no room for the Data fiduciaries to take advantage from the marketing consent as given in the notice. The legal requirements for the structure of the said notice must be strengthened to prohibit many marketing data processes. Under the current provisions of the Act, companies are freely taking consent of the user to sell the information of the user. Thus, what could have been made illegal has been made legal by the DPDP Act.

It is to be noted that bulk data collection is done by companies online. Such data is significant, in that it relates not only to buying patterns and preferences, but also the age, telephone numbers, email ids, political preferences, opinions on social issues, and criticism of the government. Upon a bare reading of schedule III and IV of the draft DPDP Act 2023 rules, which spell out the limitations of purposes for which data can be processed, the abovementioned data can be easily collected and there would be no legal obstacles to processing it. In a judgement of the Court of Justice of the European Union in ***Tele2 Sverige case (C-203/15 and C-698/15)***, the Court held that processing of private data in transmitted in telecommunications must be stored only for a limited period of time and for the direct object of providing necessary service. Any other processing must happen only according to clear and precise consent of the subscriber of the telecommunication service. Further, the provider of the service is required to specify precise information on the nature of data processing. Thus the CJEU found unlawful Section 1 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) of the UK which empowered the

their-consent-lawsuit-alleges/

 [ISSN 2581-5369]

Secretary of State to require public telecommunications operators to retain communications data.[13]

*****

[13] *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson, Joined Cases C-203/15 and C-698/15, EU:C:2016:970, Judgment of 21 Dec. 2016, ECLI:EU:C:2016:970, O.J. (C 053) 2017/16, http://curia.europa.eu/juris/document/document.jsf?docid=186492.*

 [ISSN 2581-5369]