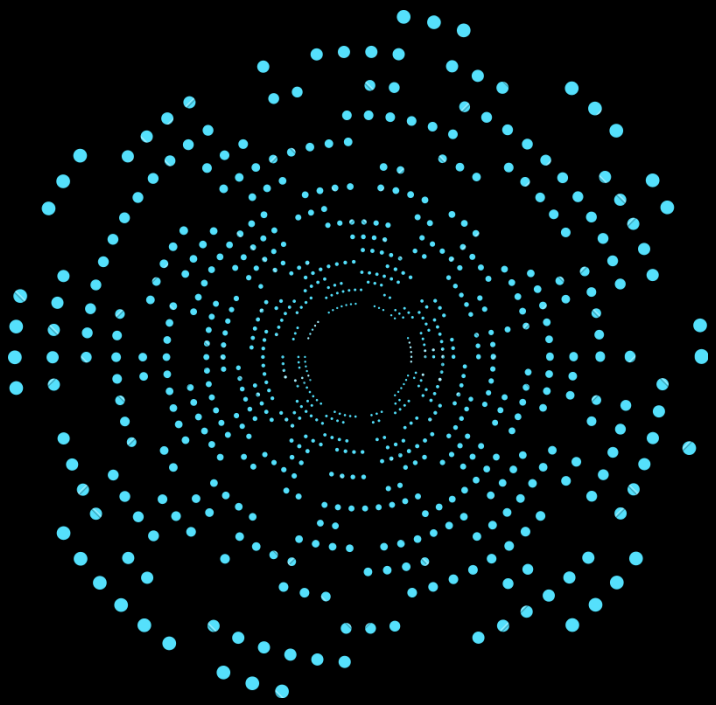
# INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY



VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

**International Journal on Cyberspace Law and Policy**

**(Free Publication and Open Access Journal)**

**Journal's Home Page – https://ijclp.iledu.in/**

**Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/**

**Volume 1 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/p-volume-1-and-issue-1-of-2023/)**

**Publisher**

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in




© Institute of Legal Education

**Copyright Disclaimer**: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer https://ijclp.iledu.in/terms-and-condition/

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-9-8

Published by

Institute of Legal Education

https://iledu.in

# Development of Data Privacy & Protection Laws in India – An Analysis

**Author -** Anjali Jain, Student at Government Law College, Ajmer

**Best Citation** - Anjali Jain, Development of Data Privacy & Protection Laws in India – An Analysis, *International Journal on Cyberspace Law and Policy,* 1 (1) of 2023, Pg. 06-12, ISBN (P) - 978-81-960702-9-8.

**Abstract**

The dynamically developing cyberspace everyday provides a new scope for its regulation to the nations. Cybercrimes, e-commerce transactions, data privacy, crypto currency, Web 3 and the developments in cyberspace are unstoppable. The developing cyberspace is thriving on Data. This article analyzes the regulation of data in India. It maps the journey of regulation of data over the years through the pillars of privacy, protection and processing. The article further focuses on the loopholes of the legislation and critically analyze the upcoming Digital Privacy Data Protection Bill, 2022.

**Keywords:** Data, Privacy, Data Protection, IT Act 2000, Personal Information, DPDP Bill 2022.

## I. Introduction

The Privacy and Data Protection are associated that is, if the personal information of any individual is shared without his/her consent, it will lead to violation of privacy. The right to privacy is a fundamental right. Hence, its violation leads to infringement of fundamental right. This sharing or receiving personal information in oral, written or electronic form is not protected by any stand-alone legislation in India. Safeguards exist but are scattered across different rules and regulations. Such as IT (Amendment Act of 2008) and IT (Sensitive Personal Data or Information) Rules of 2011, Indian Contracts Act 1872 and the forthcoming Personal Data Protection Act.

### A. The Information Technology Act, 2000

The Information Technology Act, 2000 (herein after referred as 'IT Act') was enacted primarily for facilitating the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions. It is pertinent to note that the act did not provide with any concept of 'personal data'. Personal Data is defined as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed or has been processed in a computer system or computer network, and may be in any form or stored in the memory of the computer.

#### 1. Roots of Personal Data Protection

Although data privacy was not mentioned in the preamble of the "IT Act." However, some parts of this legislation are regarded as the "backbone" of data protection. However, they lack adequate resources.

*Any misappropriation of the computer network, system, resources, database is termed as cyber contraventions and the person indulging in the same is heavily penalized. It facilitates us with an exoteric or long arm jurisdiction, meaning thereby, if any person contravenes the data and privacy rights of an individual by means of computer, computer system or computer network locates in India, he would be liable under provisions of the Act. Any nature of unauthorized use which leads to damage, tampering with computer source documents, hacking with computer system and access to electronic record, register, book, correspondence, information, and document without consent of the person concerned is liable to punished under the Act.*

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-9-8
Published by
Institute of Legal Education
https://iledu.in

Hence, it further ropes in the network service provider for violating the privacy right of third party. But all these offences are subjected to one exception, that, 'if the person charged proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention'.

Section 43 A of the IT Act explicitly provides that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected"

Further Section 72 A provides that "Punishment for disclosure of information in breach of lawful contract. -Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of 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 to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both".

## 2. Gaps in the legislation

It is apparent that both the sections mentioned above are not dealing with data privacy and protection directly. Excluding the third party obligation, it restricts the scope of the law. Furthermore, legislation hides the intent of the act by putting the shadow of negligence and due diligence. Hence, the IT act is focused more on regulation of exchange of information through computer networks instead of protection of personal data.

### B. IT Rules, 2011

The Department of Information Technology notified Information Technology the 2011 Rules on April 11, 2011 vide notification no.G.S.R. 313(E). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to support the data protection regime under The IT Act. The Rules are with protection of "Sensitive personal data or information of a person", only. The Rule 3, of the rules defines the scope of personal information for the first time and provides a list of items that are to be treated as "sensitive personal data", which includes such personal information which consists of information relating to:-

i. Passwords;
ii. Financial information such as bank account or credit card or debit card or other payment instrument details;
iii. Physical, physiological and mental health condition;
iv. Sexual orientation;
v. Medical records and history;
vi. Biometric information.

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected under the act.

#### 1. The Principles of Reasonable Security Practices and Procedures established in the Rules

- **Transparency:** The IT rules cast a duty upon the Body Corporate to provide a privacy policy for dealing with personal

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-9-8
Published by
Institute of Legal Education
https://iledu.in

information and sensitive data and it also requires that the policy should be available on the website of the body corporate. The policy shall include all the necessary details for e.g. type of personal data collected, statements of practices, purpose of collection, provisions related to disclosure and security practices etc.

- **Consent**: Body Corporate shall not collect sensitive personal data without obtaining consent in writing or by fax or e-mail form the provider regarding the purpose for which the data is being collected.
- **Retention:** The information collected shall be used only for the purpose for which it is collected and shall not be retained for a period longer than which is required.
- **Purpose:** Any personal information or sensitive data shall not be collected unless and until it is for a lawful purpose and the collection is necessary for the fulfillment of that particular purpose.
- **Right to Opt-Out-** The provider shall be given an option to opt out of providing such information along with an option to withdraw his consent to the collection at any later stage as well.
- **Grievance Redressal**: The Body Corporate shall keep the data secured and it shall designate a grievance redressing body for any discrepancies arising in future.
- **Security Practices:** A Body Corporate shall be considered to have complied with reasonable security practices if they have implemented and documented the standards of these security practices. Rule 8 (2) mentions the name of one such ISO security standard for data protection.

**2. Gaps in the legislation**

While the IT Act does not define 'reasonable security practices and procedures', the IT Rules 2011, framed under the IT Act, specify minimum standards of data protection for sensitive personal data. The IT Rules 2011 are not intended to be exhaustive, but require companies to have a privacy policy, to obtain consent when collecting or transferring sensitive personal data or information, and to inform data subjects of recipients of such collected data. The IT Rules implementation helped in increasing the scope of the IT Act, yet it lacked the present day needs such as jurisdiction of transfer of data in foreign countries, development of separate ecosystem for data protection, coverage of non-corporate etc.

Further, in Justice K.S. Puttaswamy vs Union of India, a nine-judge bench of the Supreme Court passed a historic judgment affirming the constitutional right to privacy. It declared privacy to be an integral component of Part III of the Constitution of India, which lays down our fundamental rights, ranging from rights relating to equality (Articles 14 to 18); freedom of speech and expression (Article 19(1)(a)); freedom of movement (Article 19(1)(d)); protection of life and personal liberty (Article 21) and others. These fundamental rights cannot be given or taken away by law, and all laws and executive actions must abide by them. The Supreme Court has, however, clarified that like most other fundamental rights, the right to privacy is not an "absolute right". Subject to the satisfaction of certain tests and benchmarks, a person's privacy interests can be overridden by competing state and individual interests.

**C. Personal Data Protection Bill, 2022**

The Ministry of Electronics and IT ("MeitY") introduced a draft of the Digital Personal Data Protection Bill, 2022 ('DPDP Bill') and had invited the public to submit feedback on the DPDP Bill by 17th December 2022. This move comes a few months after MeitY withdrew the DPDP Bill's predecessor, the Personal Data Protection Bill, 2019 ('PDP Bill') in August 2022.

**i. Intent**

The need to safeguard citizens' private information and make data usage transparent

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-9-8
Published by
Institute of Legal Education
https://iledu.in

is pressing need considering the rise of digital platforms. India is consistently experiences one of the highest rates of data breaches, and both private and public websites frequently experience data loss. A non-partisan law that democratizes the user data privacy ecosystem for both big tech companies and governmental organizations is the need of the hour.Data exchange is essential if India is to become a global leader in data. Additionally, the seamless flow of data is impossible without a strong Data Protection law.

The new law must adequately address the worries of citizens whose private data is constantly in danger, without harming the interests of the thriving start-up ecosystem. Sensitive data regulation is covered by some provisions in the current IT Act of 2000. But no laws have been passed.

### ii. Highlights of the Bill:

- Only personal data that is collected online or offline and later converted to digital form falls under the purview of the Bill.
- Among other definitions, the 'DPDP Bill' includes new terms like Data Principal (i.e., the person to whom the personal data relates, which includes the person's parents or legal guardians if the person is a child) and Data Fiduciary (i.e., the person who, alone or jointly with others, determines the purpose and means of processing of personal data) ("DF"). In contrast to the current Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (the "IT Rules 2011"), which only apply to body corporations, the DF now covers HUFs, artificial judicial persons, individuals, and the State
- To ensure that the rights granted to Data Principals are not abused, the Bill has added a few responsibilities for them. The Bill also includes a penalty for duty violations of up to INR 10,000.
- The Bill requires that the notice given to the Data Principal and the request for consent be available in English or, at the Data Principal's option, any of the 22 languages listed in the Eighth Schedule to the Constitution of India.
- Unlike section 72A of the IT Act of 2000, the Bill makes no mention of any criminal penalties for failing to comply with its requirements.

### iii. Analysis of Bill

i. **Applicability of the Bill**: While the Bill applies to processing of digital personal data within India and processing related to offering goods and services and profiling of Data Principals within India, it does not highlight whether it would apply to any individual whose personal data is processed within the territory of India.

ii. **Sensitive Personal Data**: Unlike the earlier laws, the Bill does not differentiate between personal data and sensitive personal data. The bill has taken a holistic approach of safeguarding all personal data with equal level of protection as it mentions obtaining explicit consent for collection of personal data.

iii. **Elements of Privacy Notice:** The Bill mandates that Data Fiduciaries notify Data Principals of the personal data they have collected and why it is being processed. Non-automated means: Processing of personal data that is not automated is not covered by the Bill's provisions. This could result in the exclusion of certain Data Fiduciaries who do not process personal data automatically. The Bill should take into account applying provisions on the processing of personal data by partially automated means and to processing

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-9-8
Published by
Institute of Legal Education
https://iledu.in

other than automated means in order to include such Data Fiduciaries in the Bill's scope.

iv. **Breach notification:** In the event of a data breach, the Bill imposes an obligation on Data Fiduciary and Processor to notify each affected Data Principal. The Bill does not specify any particular time period in which the Data Fiduciary is required to inform the Data Protection Board and Data Principals regarding data breach.

v. **Rights of Data Principal:** The Bill has introduced right to grievance redressal where the Data Fiduciary is required to respond to the grievance of Data Principal within 7 days or shorter period that may be prescribed. This is a welcome move to reduce the time taken by Data Fiduciary to acknowledge the grievance of the Data Principal and provide appropriate solution for the same.

vi. **Right to data portability:** The Bill does not provide the right to data portability to Data Principal. In this era of population-scale data repositories, individuals should be able to extract data related to them from data repositories in which they have been stored.

vii. **Right to access:** The Data Principal have right to obtain information regarding the categories of their personal data shared and identities of all the Data Fiduciaries with whom the personal data has been shared. This right should be extended to include the right to obtain information about Data Processors with whom the personal data has been shared.

viii. **Right to nominate**: The Bill establishes the right to appoint a representative in the event when the data principle cannot exercise his right or dies. This could provide appropriate guidance for certain industries facing such scenarios and ensure protection to data principle whose data is processed according to the processing operations.

ix. **Cross border data transfer**: The bill reduced the requirement for cross-border data transfer, where data fiduciaries can transfer personal data to other countries notified by the central government. In addition, the requirement to retain sensitive personal data has been eliminated in India. This has been a big help for data fiduciaries who keep their servers overseas and startups don't need to invest in local storage solutions. However, the bill may consider creating a legal mechanism to transfer personal data to countries that are not on the central government's white list.

***i. Processing of Data:***

The 'DPDP Bill' presents three grounds on which DF can process the personal data. First, the provisions of the DPDP Act must be followed when processing digital personal data. Second, provided that the processing is not expressly prohibited by law, such processing is permitted. Third, DP should give consent (express or implied) before processing such personal data

***ii. Deemed Consent:***

In addition, the 'DPDP Law' allows for the concept of "deemed consent" in a few limited circumstances (where the consentof a Data Principal is deemed "essential"). This covers circumstances inwhich a Data Principal is obivously required to give his or her personal information to a Data Fiduciary (for any lawful function, such as to avail of any beneficial services, or to obtain a licence, certificate, permit, etc.); in which such information is required to comply with judicial orders,for employment purposes; in situations where it is in the public interest; and in situations where it is required for other "fair and reasonable" purposes. It's interesting to note that the

DPDP Law makes no explicit mention of reviewing, managing, or rescinding a Data Principal's "deemed consent.

***iii. Constitution of the Data Protection Board of India***

The 'DPDP Bill' provides for the establishment of the "Data Protection Board of India" as a regulatory body.

According to the Bill, the Board's main duty is to ascertain if there is any non-compliance of this Act's provisions and to impose penalties in accordance with their terms.It appears odd that theBoard would give the executive this authority (to identify the pertinent details). Further, if the current Bill is approved by the Parliament, the Rules under the Act will take effect after a straightforward publication in the Official Gazette (and will not undergo deliberations fromboth houses of the Parliament).The Bill should have ideally mentioned at least some pertinent information about the Data Protection Board of India (such as its composition, qualifications, and selection process), which has been given extensive powers to impose penalties to the tune of INR 500 crore. The Board has been given powers equivalent to of a Civil Court and exclusive original jurisdiction to entertain challenges under the intended legislation (including industry experts).

More importantly, the qualifications and the terms and conditions of the chief executive mustcarefully discussed by the Parliament and the general public because they will serve as the presiding member at the top of the Board.Although the executive's authority to make rules is not in doubt, the government should have included such important details about the Board in the Bill itself (instead of giving the power to the executive to decide to take a call on such aspects). Furthermore, it is extremely remarkable that the administration has been given the authority to choose the composition of an intended judicial body, given that the Board will observe the functions of an adjudicating body (which will raise questions on the independence of functioning of the Board)

## D. Conclusion

The fundamentals right to privacy in the times where personal information has become a commodity will be upheld by the judiciary subject to certain restrictions. The legislature is also embarking to protect its citizens from external society and develop a balance between business motives. India, home to the second largest base of internet users, lacks an independent data regulator. The data subjects have limited rights. As an aspirational digital economy with big stakes on 5G infrastructure, the nation needs to show better preparedness to navigate the mounting data challenges. An inclusive data protection legislation empowering users and enthusing businesses can catalyze the change. The new Digital Personal Data Protection Bill, 2022 brought in this light, fill the loops of the earlier legislation and devises new concept to regularize the Data World unfolding before the nation.

## E. References

1. https://www.mondaq.com/india/data-protection/1262298/the-digital-personal-data-protection-bill-2022
2. https://www.ahlawatassociates.com/blog/analysis-of-digital-personal-data-protection-bill-2022/?utm_source=mondaq&utm_medium=syndication&utm_term=Privacy&utm_content=articleoriginal&utm_campaign=article
3. •https://timesofindia.indiatimes.com/readersblog/why-india-needs-an-inclusive-data-protection-law/why-india-needs-an-inclusive-data-protection-law-44601/

4. https://www.khaitanco.com/sites/default/files/2021-04/Data%20Protection%20in%20India%20Overview.pdf
5. https://www.mondaq.com/india/data-protection/626190/information-technology-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
6. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf
7. https://kpmg.com/in/en/home/insights/2022/12/privacy-digital-personal-data-protection-bill-2022.html
8. https://www.wionews.com/india-news/explained-experts-raise-concerns-about-indias-digital-data-protection-bill-2022-545276
9. https://www.mondaq.com/india/data-protection/1269900/comparing-the-digital-personal-data-protection-bill-2022-with-the-data-protection-bill-2021
10. https://www.mondaq.com/india/data-protection/1262298/the-digital-personal-data-protection-bill-2022
11. https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1