

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DATA PRIVACY VIS-À-VIS PROTECTION LAWS IN INDIA

AUTHORED BY - SIDHARTH NAIR*

Abstract

This article briefly discusses the provisions relating to data privacy and its protection. Wherein it touches upon the current regime, laws and its provisions governing data privacy and protection and also its shortfall embedded in it. This article further examines the naissance of the laws strictly governing data privacy and also the attempts made by the legislature to meet the indispensable demand of data privacy and protection laws. Furthermore, this article also canvasses the case laws and judgments expounded by the Hon'ble Supreme Court of India and various High Courts laying down edifice of the principle of privacy as an inherent part of Chapter III of the Constitution of India and the violation of the same and being oblivion to such violation as a potential threat and nemesis for the society.

Introduction

The idea of passing particular data privacy legislation had been under serious consideration since the beginning of the previous decade, while the country has witnessed a technological and industrial boom, whereby new age intermediaries and industries have been established, therefore it is not irrational in passing a new data privacy law in India to regulate and govern these industries.

As technology advances, it can now carry out tasks based on data analysis. Data is used for a variety of tasks, such as documenting, predicting the weather, health analysis etc. The volume and variety of data available online are growing as the internet is used more often. But due to this stockpile of data, the threat of data breach, misuse and violation of privacy has become imminent.

To tackle this situation of violation of privacy and misuse of the data, several international organizations and national governmental entities have framed several regulations, rules and frameworks concerning Right to Privacy and Personal Data.

Since 2010 there has been a significant radical increase in internet users in India because of the multiplicity of services offered, ranging from banking, education, news, social media networks etc. Post demonetisation, implementation of Goods and Services Tax and COVID-19 pandemic it has necessitated the usage of internet at a large scale and has also brought an upheaval towards the lifestyle of an individual making the society more digitalized and literate in terms of usage of internet. Furthermore, the initiative of Digital India propounded by the Hon'ble Prime Minister Narendra Modi has further revolutionized the concept of digital and cyberspace. The government has started pushing for the usage of digital space in its several programs. At the time of Covid, government launched several online portals namely "Aarogya Setu" and "CO-WIN" which mainly were used for contact tracing, self-assessment test and Covid vaccination service which acted as a boon to tackle the horrendous situation faced by citizen during Covid. The government also has many aspirational projects in line which seeks to collect, process and store many data including sensitive and critical data.

Despite the changing scenario, yet the legislature has failed in fulfilling the demands of current scenario by not introducing any effective legislation for governing and regulating the digital and cyberspace. At present, the Information Technology Act and rules made thereunder are used, but it has not been much effective in tackling the aforementioned situation of data breach and violation of privacy. Thus, it is an urgent need of the hour to introduce legislation specifically devoted towards the data uploaded in digital and online platforms.

Current Regime

Digital Personal Data Protection Act, 2023

The Ministry of Electronics and Information Technology after withdrawing the erstwhile bill i.e. Personal Data Protection Bill, 2019, in response to the multiple recommendations received through public consultation; and instead released the new Digital Personal Data Protection Act, 2023 ("Act"), a revised version of the aforementioned predecessor.

The foremost drawback of the aforementioned Act is the applicability of the Act, which is only limited to personal data that is collected online or offline and subsequently digitized.

Astonishingly, the Act gives personal data digitization more priority and encourages enterprises to do so. While at this juncture, collecting and managing offline data in physical form is far more expensive than collecting and managing data in digital form. Because such firms are covered by this Act and get proper protection, customers eventually favours them when handling personal data in digital format. However, it would be interesting to comprehend

the choices made by small firms and family-run enterprises.¹

In addition to the above, the Act even bestows unchecked and extensive discretionary powers to the government and its entities, such as data fiduciaries and startups, to access personal data and information under the garb of predictive policing and mass surveillance, thereby constituting an abject violation of the right to privacy.²

However, to counter-balance its foregoing shortcomings, the Act ensures that for the purpose of processing personal data lawfully, a Data fiduciary must obtain consent from the data principal and must be for legitimate uses.³ A plain reading of the Act reveals that the fiduciary is invariably fastened with an obligation to give notice and respond to access, correction and erasure request are only permissible if the processing is based on consent.

Furthermore, the Act ensures that the consent for processing of personal data must be ‘free’, ‘specific’, ‘unconditional’, and ‘unambiguous’ with a clear affirmative action.⁴ So as to meet the “informed” criteria, the Act requires that the notice must be given to principals before or at the time their consent is sought. Moreover, the notice must unequivocally ascribe the specific personal data in question, the purpose for processing, the right(s) of the data principal and mechanisms for their grievance redressal.

Digital Personal Data Protection Rules, 2025

To further operationalise the aforementioned Act, the Government of India, Ministry of Electronics and Information Technology, *vide* notification dated November 14, 2025, formulated the Digital Personal Data Protection Rules, 2025 (“*Rules*”)⁵. In order to achieve effective operationalisation of the Act, the Rules comprehensively enunciates actionable guidance on imperative and/or critical aspects such as data processing, consent management, breach notifications and cross-border data transfer. Therefore *in sequitur*, the Rules, acting as the guidance principle towards implementation of the provisions of the Act, marks a significant step taken towards building a robust data protection framework in India.

Information Technology Act, 2000

Section 43A of the Information Technology Act, 2000 (“*IT Act*”) which was inserted *vide* Information Technology (Amendment) Act, 2008 also states that a body corporate that is in

¹ Digital Personal Data Protection Act, 2023

² <https://lawreview.mnlumumbai.edu.in/>

³ Section 4, Digital Personal Data Protection Act, 2023

⁴ Section 6, Digital Personal Data Protection Act, 2023

⁵ Digital Data Protection Rules 2025

possession, handles and manages any sensitive personal data or information in a computer resource which it owns or controls. Negligently causes any loss or wrongful gain to any person, such body corporate shall be obligated to pay damages by way of compensation to the person so affected.⁶

Indian Penal Code, 1860

The Indian Penal Code, 1860 also provides for the provision relating to data protection and prevention of data theft. Offences under this code include theft, criminal breach of theft, and misappropriation of property, resulting in imprisonment or fine or both. Although these offences apply only to movable property, whereby this code recognizes data as part of the definition of movable property.

Concerns

There are several concerns about the existing regime of data protection some of them are as follows:

1. **Limited Liability-** The aforementioned rules and provisions apply solely to organisations engaged in professional or commercial activity. As a result, both private individuals and government officials are not included in its scope. Additionally, it excludes charity, social, and non-profit activities as well as non-professional pursuits.
2. **'Personal' and 'Sensitive' data-** The regulation defines both sensitive and personal data. The concept of personal data is more restricted for purposes involving sensitive data. Additionally, the majority of the provisions apply to sensitive data.
3. **Data Provider and subject-** Instead of the data subject, the regulation primarily discusses the data supplier. The subjects and the data supplier don't have to use the same terminology. As a result, it violates a person's right to control personal data about him because he could not be a data source.

Attempts towards enacting a data privacy law

Over the two decades legislators have been discussing and debating to come up with an appropriate legislation recognizing and protecting data privacy and consequently to this effect many bills were introduced in the Parliament since 2006 that unfortunately failed. The initial bills were private member bill.

⁶ Section 43A of the Information Technology Act, 2000

The first bill to be tabled was 'The Personal Data Protection Bill' in 2006, which was tabled by Parliamentarian Shri Vijay Jawaharlal Darda.

Mr. Manish Tiwari introduced "The Intelligence Services (Powers and Regulation) Bill" in 2011 to achieve harmony amongst the rights to privacy and the capabilities and usefulness of intelligence services.

'The Right to Privacy of Personal Data Bill' was introduced in the Rajya Sabha by lawmaker Vivek Gupta in 2016. A similar measure was introduced in the Lok Sabha that same year by lawmaker Om Prakash Yadav.

Later in 2017 Mr. Shashi Tharoor introduced the '*Data Privacy and Protection Bill*' which was a comprehensive bill directed towards data privacy and protection.

In the same year, a Committee of Expert was constituted under the Chairmanship of Justice B.N Krishna, subsequently the Committee submitted its report on 2018 and on its recommendation '*Personal Data Protection Bill, 2019*' was tabled before the Lok Sabha and was referred to Joint Parliamentary Committee. However, on August, 2022 the Ministry of Electronics and Information Technology (Government of India) was obliged to drop the bill as a result of several recommendations obtained through public consultation.

Thus, on November 18, 2022 '*Digital Personal Data Protection Bill, 2022*' was proposed by the Ministry of Electronics and Information Technology (Government of India) replacing the erstwhile '*Personal Data Protection Bill*', 2019. The Union Cabinet has approved the draft for tabling it in the upcoming monsoon session of Parliament. In the event that the draft legislation is approved, it would replace the 2011 notified Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules. The draft bill was introduced on August 3 2023 before the Lok Sabha, during the monsoon session of the Parliament and after an array of debates and discussion, on August 7, 2023, the Act was formally passed by the Lok Saba and followed by Rajya Sabha on August 9, 2023. Thereafter following its approval and/or ratification from both the Houses, the President of India Mrs. Draupadi Murmu on August 11, 2023 gave her assent to the Bill.

Pillars of Data Protection: Krishna Committee

An Expert Committee was constituted under the chairmanship of Justice B.N Krishna in 2017 by the Ministry of Electronics and Information Technology to comprehensively scrutinize the concept of data privacy and protection in context of India and suggest principles to be considered in terms of data protection and also prepare a draft data protection bill in order to espouse the principles of data protection and management.

The foremost purpose of the Ministry of Electronics and Information Technology through this data protection bill was to strike a balance between growth of digital economy and protection of personal data of citizen.

The 7 principles that were proposed by the Committee in terms of data protection are as follows:

1. Technologically malleable – The data protection law must be malleable towards the continuous change in technology and shall consequently reform the standards of compliance.
2. Integrated application - Both the public and private sectors must be governed by the law. However, the Expert group also promulgated that different and distinct obligations be followed when certain legitimate state goals are involved and to be achieved.
3. Data minimization – The data consolidated, formulated and processed must be a minimal and only those data be collected that are requisite for accomplishing the purpose sought for.
4. Intimated consent – The consent obtained must be an informed and meaningful consent, though it is still silent upon the definition of informed consent, if it refers to the collecting of data from users while keeping them informed about the process of data collection, or if it relates to the term in its more traditional definition -- where users' consent will be initially sought out and they will have the option to opt out.
5. Controller Accountability-The committee makes plain and subtly suggests that the data controller is liable for all data processing, whether it is done by itself or by companies with which data is shared.
6. Structured Enforcement- A High-Powered Statutory Authority would be established, according to the committee, and it must co-exist with appropriately decentralised enforcement mechanisms.

7. Deterrent Penalties- The Committee also proposed strict penalties against the perpetrators and offenders for wrongful processing and leakages of data.⁷

Principles directed towards Privacy

Privacy in itself is an obscured term where no straight jacketed definition be provided and solely relies on the differential perception of individuals depending on various factors like social, geographical, political and legal. The concept of privacy in all parlance is evolving. In India the 'Right to Privacy' explicitly isn't provided under Chapter III of the Constitution of India rather has been developed through constructive judgements passed by the Hon'ble Supreme Court of India and different High Courts of India and has now been included and interpreted under Article 21 of the Constitution of India.

In India the evolution of 'Right to Privacy' as a Fundamental Right can be divided in two different phases Pre-Puttaswamy and Post-Puttaswamy era. Initially during the Pre-Puttaswamy era, in the matter of MP. Sharma and others v. Satish Chandra, District Magistrate, Delhi⁸ and in the matter of Kharak Singh v. State of Uttar Pradesh and others⁹ the Courts vehemently denied to recognize 'Right to Privacy' as part of Chapter III of the Constitution of India.

Later in, Justice K.S. Puttaswamy v. Union of India¹⁰, the former Chief Justice of India, D.Y. Chandrachud gave threefold principle and requirement towards the notion of privacy that are as follows:

1. Existence of law - He insisted that any surveillance or invasion of someone's privacy must be authorized by law. Therefore, no one right may be interfered with unless it does so in accordance with Article 21's exemption, or the legal process. According to the judicial manifest, the aforementioned process must be impartial, just, and reasonable.
2. Reasonableness - As provided under Article 14, the limitations and restrictions imposed by legislation must be reasonable. The right of an individual is actually limited by the arbitrariness.

⁷ Sri Krishna Committee, 2017(Headed by Retd. Justice B.N Krishna)

⁸ M. P. Sharma and others vs. Satish Chandra, District Magistrate, Delhi (1954 SCR 1077)

⁹ Kharak Singh vs. State of Uttar Pradesh and Ors., [AIR 1963 SC 1295]

¹⁰ Justice K.S. Puttaswamy v. Union of India, AIR 2015 SC 3081

3. Proportionality - The goals that the state wants to accomplish and the limitations set by the legislation should be related.

In the aforementioned case the apex court unequivocally and unanimously recognized Right to Privacy as a part of Chapter III of the Constitution of India arising out of Right to Life and Liberty under Article 21 of the Constitution of India. The incorporation of the right to privacy by the court is not of the type of modifying the constitution, which is an exclusive legislative role reserved to the legislature, as Hon'ble Justice D Y Chandrachud further demonstrated.

Conclusion

By addressing the changing demands of internet users and international traders, the implementation of the Digital Personal Data Protection Act, 2023 and the Rules made thereunder are a significant step toward achieving data protection and privacy goals. The groundwork for improved cooperation and collaboration with multinational corporations and industries is also laid forth by this legislation.

By establishing a thorough framework for the protection and processing of personal data, this Act demonstrates India's dedication to contemporary data protection standards. Additionally, it is essential for our legislature to take into account, adopt, and apply data protection legislation from diverse jurisdictions throughout the world as needed to address data protection-related challenges.

In addition, given that data privacy infractions and breaches are a global problem, India should actively involve foreign leaders in conversations about the issue.