

ISSN :2582-6433



INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed 6th Edition

VOLUME 2 ISSUE 6

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 6 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIAL TEAM

EDITORS

Megha Middha



Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr. Ambedkar Law College, Pudupakkam. Published one book. Published 8 Articles in various reputed Law Journals. Conducted 1 Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench.

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

PERSONALIZE, PRIVATIZE, AND PROTECT: THE THREE P'S OF DATA PRIVACY

Authored By- Navya Shukla

Abstract

The internet has created entirely new markets for the collecting, organising, and processing of personal data, either directly or as a vital component of many business models. India currently lacks explicit data protection or privacy legislation. However, the relevant data protection laws in India are the Information Technology Act, 2000 (“IT Act, 2000”) and the Indian Contract Act, 1872. A Committee of Experts was formed to examine various aspects of data protection, the work of the Committee resulted in the creation of the first draft of the Personal Data Protection Bill in 2018. Consequently, the report of the Joint Parliamentary Committee on the proposed data protection law has given the Data Protection Bill of 2021 a new tone and tenure. The author through this article aims to analyse the elements of data privacy in Indian legislation essentially focusing on the PDP Bill and whether the laws adequately promote the utilities of the internet.

I. Introduction

In the well-known case of *Justice K.S. Puttaswamy v Union of India*¹, the Supreme Court issued a unanimous decision affirming that the right to privacy is a fundamental right guaranteed by the Indian Constitution. The Hon'ble Court also advised the Central Government to draw up a concrete data protection law for the country that protects the interests of the individuals as well as of the state while encouraging technological innovation and entrepreneurship. The Court reasoned that because there is no effective data protection law in place, determining what rights citizens possess is difficult, rendering the fundamental right to privacy practically useless.

Indian legislators were jolted awake by the Supreme Court's recognition of the right to privacy as a basic right under Article 21 of the Indian Constitution, and felt compelled to craft the necessary laws. Indian WhatsApp users are outraged by WhatsApp's most recent privacy policy amendment, which has exposed flaws in Indian data protection legislation. The bill in question is based on the General Data Protection Regulation² ("GDPR") of the European Union, and it aims to protect individuals' personal data, which is regularly acquired by digital media for a variety of reasons. A layman may be unaware of how far his or her data has travelled and who has access to it in such instances.³

As previously noted, the IT Act, 2000⁴ now oversees data privacy and protection in India, and an entity can be held accountable for the unauthorised use of an individual's data or personal information, as well as any negligent act using such information. However, one of the legislation's flaws is that the scope and meaning of "sensitive personal information" are limited, and the legislation's restrictions do not apply to government agencies that use residents' data.⁵ Individual ownership over their data, the ability to track who collects their data, where it is held, how it is used, and what recourse they have if their data is misused are all principles that make up a good data protection strategy. There have been far too many instances where personal information, whether anonymized or not, has been used with malicious intent.

As a result, the PDP Bill, 2019,⁶ is an attempt to protect individuals' privacy in connection to their personal data, as well as to regulate the interaction between persons and companies that process this data. It is also determined to promote innovation through digital governance in order to establish a

¹ K.S. Puttaswamy v Union of India, (2017) 10 SCC 1.

² General Data Protection Regulation, Regulation (EU) 2016/679.

³ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf. (Last visited on 25 May, 2022).

⁴ The Information Technology Act, 2000, Act No. 21 Of 2000.

⁵ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>. (Last visited on 25 May, 2022).

⁶ The Personal Data Protection Bill, 2019, Bill No. 373 Of 2019.

robust digital economy. On December 11, 2019, the Ministry of Electronics and Information Technology introduced the PDP Bill, 2019 in the Lok Sabha to restructure India's data protection management, which was previously managed by the IT Act, 2000 and its rules. The PDP Bill is mainly consistent with the requirements of the Draft Personal Data Protection Bill, 2018, and is broadly inspired by the principles of the European Union's GDPR, 2016.

II. Key Features Of The Pdp Bill

The Joint Parliamentary Committee gave its long-awaited report to the Indian Parliament on December 16, 2021, after two years of deliberation on the Personal Data Protection Bill, 2019.⁷This, hopefully, will be the ultimate consequence of a succession of JPC extensions, paving the way for a solid data protection law in the world's greatest democracy.

The PDP Bill seeks to regulate an individual's personal data, including its collection, storage, processing, and divulgence. Following are certain key takeaways of the Bill:

- It defines "Sensitive Personal Data" as financial data, health data, an official identifier, sex life, sexual orientation, biometric data, genetic data, transgender or intersex status, caste or tribe, religious or political beliefs.⁸
- It seeks to govern both companies and government agencies involved in the processing of an individual's data, which is currently limited to companies under the IT Act of 2000.
- A 'data principal' is a person whose data is being disclosed, processed, and used and who has been granted the rights to information, correction, completion, erasure, transfer, restricting disclosure, and withdrawal of their data.
- A 'data fiduciary' is the entity that collects and stores the data of a data principal. Certain obligations apply to data fiduciaries when it comes to the processing of personal data. Such processing, for example, should be subject to certain purpose, collection, and storage constraints. Personal data can only be processed for specific, clear, and legal purposes.
- Furthermore, all data fiduciaries must implement certain transparency and accountability measures, such as implementing security safeguards and establishing grievance redressal mechanisms to address individual complaints. Certain fiduciaries may be designated as "significant data fiduciaries," and they will be required to take additional accountability

⁷ Committee Information on the Joint Committee on the Personal Data Protection Bill, 2019, Lok Sabha. Available at: http://loksabhapn.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1. (Last visited on 25 May, 2022).

⁸Key Takeaways: The JPC Report and the Data Protection Bill, 2021, Internet Freedom Foundation, <https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-bill-2021-saveourprivacy-2/>. (Last visited on 25 May, 2022).

measures, such as conducting a data protection impact assessment before conducting any large-scale sensitive personal data processing (including financial data, biometric data, caste, religious or political beliefs).

- The PDP Bill will apply to data fiduciaries or data processors who are not physically present in India if they process personal data in connection with (a) any business carried on in India, (b) systematic offering of goods and services to data principals in India, or (c) any activity involving profiling of data principals within the territory of India.
- It proposes establishing a Data Protection Authority to serve as a grievance redressal forum for an aggrieved individual whose grievances were not adequately addressed by the data fiduciary.
- Exemptions have been provided for processing personal data without the consent of the data principal in certain circumstances, such as (i) when required by the State to provide benefits to the individual, (ii) legal proceedings, and (iii) responding to a medical emergency.⁹
- Personal data has been defined in terms of identifiability standards. Although 'anonymised data' is not covered by the provisions, the Central Government is empowered to create policies directing data fiduciaries or data processors to share anonymised data or non-personal data to enable better targeting of service delivery.
- The PDP Bill emphasises compliance requirements for all forms of personal data, expands individuals' data rights, establishes a central data protection regulator, emphasises the restrictive conditions for personal data transfer, lists the penalties for reckless de-identification/misuse of data, and establishes data localization requirements for certain forms of sensitive data.
- Any entity that re-identifies and processes de-identified personal data without consent faces a penalty of up to three years in prison, a fine, or both.

⁹ Mathew Chacko, Aadya Misra, *A Guide to the Data Protection Bill, 2021*, LEGAL500, <https://www.legal500.com/developments/thought-leadership/a-guide-to-the-data-protection-bill-2021/>. (Last visited on 25 May, 2022).

III. Analysis And Impact Of The Bill

With the Indian economy becoming increasingly digital, a regulatory sandbox may be required. In certain cases, exempting government agencies from the PDP Bill's restrictions may contradict the bill's goal and jeopardise an individual's fundamental right to privacy. The data localization rules may generate general security and national security concerns. The PDP Bill declares that the government must have access to "important" or "sensitive" personal data, such as religious or political beliefs, if necessary to defend national interests, but such unlimited access to these information could lead to data misuse.¹⁰

Furthermore, the concept of the right to be forgotten has been discreetly placed in the PDP Bill under the right to erasure. The idea for the development of this right is that a person should be able to govern their data by requesting that data processed by a data fiduciary be erased. Users will be able to request that companies remove their personal data, which means they will have the right to be forgotten if their purpose has been met or if they desire to withdraw their consent. However, the PDP Bill grants only a limited and arbitrary right, requiring the consent and scrutiny of an Adjudicating Officer before the data can be wiped.

The scope of the Personal Data Protection Bill has been enlarged in response to the JPC Report¹¹ to include both personal and non-personal data. Instead of "Personal Data Protection Bill," the bill is now known as "Data Protection Bill (Bill)." Because "it is impossible to discriminate between personal and non-personal data when mass data is collected or conveyed," both categories of data will be regulated by the same regulator. The inclusion of non-personal data, including anonymized data, in the scope may be a sensitive issue, as some of the non-personal data will be considered proprietary by enterprises who have invested large resources to obtain it.

The establishment of the DPA and other accompanying infrastructure, as outlined in the study, are some critical activities that must be done in stages. Companies must quickly embrace and implement a successful compliance plan by focusing on investments and alignment of people, process, and technology. Both the government and private firms must implement dedicated training and awareness programmes to train the staff and assure timely compliance.

¹⁰ Smitha Krishna Prasad, *Data Bill: Safe from prying Govt*, Deccan Herald, <https://www.deccanherald.com/national/sunday-spotlight/data-bill-safe-prying-govt-685674.html>. (Last visited on 25 May, 2022).

¹¹ Report of the Joint Committee on the Personal Data Protection Bill, 2019. Available at: [http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17%20Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17%20Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill%202019_1.pdf](http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17%20Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill%202019_1.pdf). (Last visited on 25 May, 2022).

IV. Conclusion

The Data Protection Bill is a much-needed and long-awaited piece of legislation that would replace India's current archaic, obsolete, and inadequate data protection policy. It would assist preserve individuals' privacy rights and promote fair and transparent data use for innovation and growth, unlocking the digital economy, in comparison to present standards. It has the potential to create jobs, increase user understanding of their privacy, and hold data fiduciaries and processors accountable. Furthermore, with the rapid adoption of cutting-edge technologies such as blockchain and artificial intelligence, it would be worthwhile to track and study how the current set of regulations would be applied to frameworks based on decentralisation and anonymization.

Despite being influenced by the EU General Data Protection Regulation, India has developed its own approach to data protection, including merging personal and non-personal data under one roof, data localization, hardware device coverage, social media platform management, and more. Though it still has certain flaws, it will bring India up to speed with other countries' rigorous data privacy rules once completely implemented. Companies should start preparing for compliance with the various provisions as soon as possible. Enterprises should contemplate conducting periodic audits and assessments of their privacy procedures in order to better visualise the types of data collected, its flow within the company, storage timelines and locations, and to initiate remediation steps to close any gaps they discover.

Compliance with the requirements of data privacy can be difficult in today's information age. However, if organisations are proactive and plan ahead of the enforcement date, this does not have to be the case. Organizations can confidently embrace the Bill and, once compliant, consider it a competitive advantage by implementing a tiered, comprehensive data security strategy.