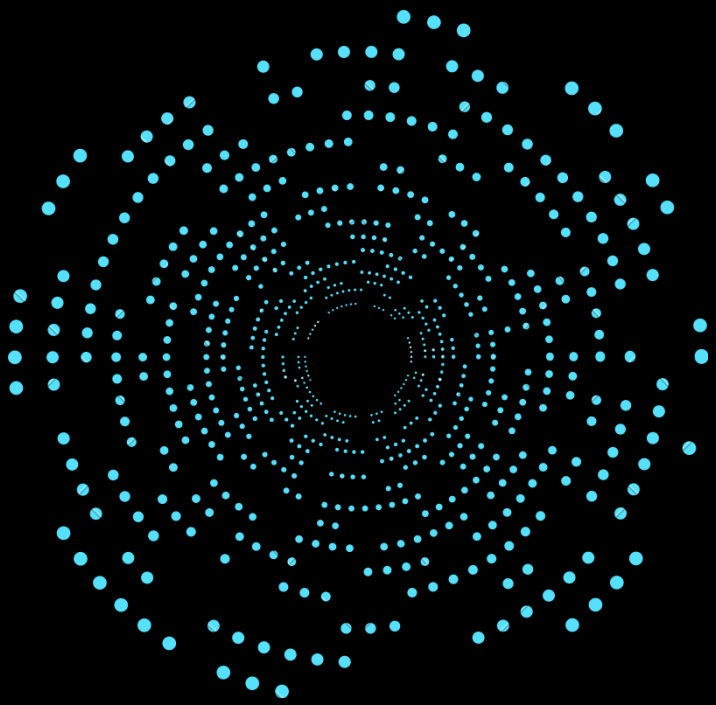
INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY



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/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

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

Volume I and Issue I of 2023

ISBN - 978-81-960677-4-8

Published by

Institute of Legal Education

https://iledu.in

LEGAL RAMIFICATIONS OF INDIAN DATA PROTECTION LEGISLATION ON GLOBAL COMPANIES

Author - S.SRINIDHI, Student at SAVEETHA SCHOOL OF LAW, SIMATS**.**

Best Citation - S.SRINIDHI, LEGAL RAMIFICATIONS OF INDIAN DATA PROTECTION LEGISLATION ON GLOBAL COMPANIES, INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE, 1 (1) of 2023, Pg. 48-52, ISBN (P) - 978-81-960702-2-9.

ABSTRACT

The Personal Data Protection Bill (PDPB) is a comprehensive legislation that seeks to regulate the processing of personal data in India. This legislation impacts multinational corporations that conduct business in India and requires them to comply with new rules and standards for the collection, storage, and use of personal data. The objective of this study is to analyse the legal ramifications of Indian data protection legislation on global companies and the challenges they face in complying with the PDPB requirements. Another objective is to explore strategies that multinational corporations can adopt to ensure compliance and mitigate legal and reputational risks. It highlighted the need for multinational corporations to collaborate with Indian regulators and stakeholders to develop effective data protection frameworks. This requires a proactive approach to compliance that goes beyond mere legal compliance to include ethical considerations and stakeholder engagement. By doing so, multinational corporations can build trust with Indian consumers and demonstrate their commitment to protecting personal data.

KEYWORDS: Indian Personal Data Protection Bill (PDPB), Data Privacy and Security, Multinational Corporations, Cross-Border Data Transfer, Data Localization

INTRODUCTION:

The topic of data protection and privacy has gained increasing attention in recent years, as individuals become more concerned about the use and misuse of their personal information. Governments worldwide have responded by enacting legislation to protect personal data, and India is no exception. The Indian government has taken significant steps to regulate the processing of personal data in the country, culminating in the proposed Personal Data Protection Bill (PDPB). This legislation will have significant legal ramifications for global companies that conduct business in India. The PDPB seeks to regulate the processing of personal data and establish new rules and standards for the collection, storage, and use of such data. Failure to comply with these requirements can result in legal and reputational risks, including penalties and fines. Factors such as the increasing use of digital technologies and the rise of data-driven business models have made data protection and privacy more critical than ever before. The PDPB represents the latest development in this trend and highlights the need for global companies to understand and comply with Indian data protection laws. This has evolved in response to changing societal attitudes towards data protection and the need for governments to regulate the use of personal data. The Indian government has played an active role in this process, and the PDPB is the latest manifestation of its efforts. The legal ramifications of this legislation on global companies are significant, and it is crucial for companies to understand and comply with the requirements of the PDPB and other international covenants that protect personal data.

OVERVIEW OF INDIAN DATA PROTECTION LEGISLATION:

The Indian data protection legislation is a comprehensive framework that aims to protect the privacy and personal data of Indian citizens. The Personal Data Protection Bill (PDPB) seeks to regulate the processing of personal data by

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

companies operating in India, including global companies. The PDPB is modelled after the General Data Protection Regulation (GDPR) of the European Union and contains several provisions that establish new standards for data protection in India. The PDPB defines personal data as any data that relates to a natural person, which can be used to directly or indirectly identify the person. The bill requires companies to obtain consent from individuals before collecting, storing, or processing their personal data. The bill also establishes rules for the processing of sensitive personal data, which includes data related to an individual's health, finances, religion, or sexual orientation. The PDPB also contains provisions for the cross-border transfer of personal data. The bill requires companies to store personal data within India unless they obtain consent from the individual or the Indian government. Companies must also demonstrate that the country where the data is being transferred provides adequate data protection standards. The legal ramifications of Indian data protection legislation on global companies are significant. Companies that operate in India or process personal data of Indian citizens must comply with the PDPB requirements. Failure to comply can result in legal and reputational risks, including penalties and fines.

PROVISIONS OF THE INDIAN PERSONAL DATA PROTECTION BILL (PDPB):

The PDPB aims to regulate the processing of personal data, including sensitive personal data, by providing individuals with greater control over their personal information. The bill introduces concepts such as data fiduciaries, data principals, and the right to be forgotten. The PDPB mandates that data fiduciaries implement privacy by design principles and conduct regular privacy assessments to ensure that personal data is processed lawfully and transparently. The bill also imposes strict requirements on cross-border data transfer and mandates data localization requirements for certain categories of personal data.

IMPLICATIONS OF PDPB FOR MULTINATIONAL CORPORATIONS:

The PDPB will have significant implications for multinational corporations operating in India. Companies will need to comply with strict data protection requirements, which will impact their operations, processes, and data management systems. Multinational corporations that store and process data outside of India will need to comply with strict cross-border data transfer requirements, which may require them to invest in additional resources and technologies to ensure compliance. The implications of the PDPB for multinational corporations are significant. Companies that operate in India will need to review their data processing practices and take steps to ensure compliance with the provisions of the legislation. Failure to comply with the PDPB can result in legal and reputational risks, which can have significant consequences for the operations of global companies in India.

CROSS-BORDER DATA TRANSFER AND DATA LOCALISATION:

Cross-border data transfer and data localization are important considerations for multinational corporations that conduct business in India. The Indian Personal Data Protection Bill (PDPB) contains provisions that require companies to store and process personal data within India, subject to certain exceptions. This has raised concerns among global companies that may have operations in multiple countries and may need to transfer data across borders. The PDPB requires companies to obtain explicit consent from data subjects before transferring their personal data outside India. Failure to comply with these provisions can result in significant penalties and fines. To address the challenges associated with cross-border data transfer and data localization, companies should consider adopting measures such as developing a data localization strategy, establishing data centres within India, and implementing robust data protection measures.

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

CHALLENGES IN COMPLYING WITH INDIAN DATA PROTECTION LAWS:

Complying with Indian data protection laws presents a number of challenges for global companies. One of the key challenges is the lack of clarity in the Indian data protection landscape, which makes it difficult for companies to understand and comply with the regulations. Another challenge is the cross-border data transfer and data localization requirements, which can create significant operational and financial burdens for companies. Additionally, complying with the Indian data protection laws requires companies to balance the competing demands of privacy and data access, which can be a complex and delicate task. Overall, global companies face significant challenges in complying with Indian data protection laws and must develop robust strategies to meet these requirements.

STRATEGIES FOR COMPLYING WITH PDPB REQUIREMENTS:

Multinational corporations can adopt several strategies to comply with PDPB requirements, including implementing robust data management policies and procedures, conducting regular privacy assessments, and engaging with regulatory authorities. Companies may also need to invest in additional resources and technologies to ensure compliance with cross-border data transfer requirements and data localization requirements. To comply with the PDPB, multinational corporations should prioritise the following steps:

1. Conduct a comprehensive data inventory: Companies should identify and inventory all personal data that they collect, process, store, and transmit.
2. Conduct a privacy impact assessment: A privacy impact assessment (PIA) can help companies identify and assess the privacy risks associated with their data processing activities.
3. Develop data management policies and procedures: Companies should develop policies and procedures to govern the collection, use, storage, and sharing of personal data.
4. Appoint a data protection officer: Companies should appoint a data protection officer (DPO) to oversee their data processing activities and ensure compliance with the PDPB requirements.
5. Implement appropriate technical and organisational measures: Companies should implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, and destruction.

INTERNATIONAL COVENANTS:

The legal ramifications of Indian data protection legislation on global companies are significant, as these companies must comply with both domestic Indian law and international covenants that protect the privacy and personal data of individuals. The most relevant international covenants in this context are:

1. *The Universal Declaration of Human Rights: This covenant outlines the right to privacy and protects individuals from arbitrary interference with their privacy, family, home, or correspondence. It also states that everyone has the right to the protection of the law against such interference.*
2. *The International Covenant on Civil and Political Rights: This covenant establishes the right to privacy and personal data protection as a fundamental human right. It obligates states to protect individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence.*
3. *The General Data Protection Regulation (GDPR): This covenant is a regulation that protects the privacy and personal data of individuals in the European Union. It applies to all companies operating in the EU, regardless of their location, and sets out strict rules for data protection, including the right to access, rectification, and erasure of personal data.*
4. *The Asia-Pacific Economic Cooperation (APEC) Privacy Framework: This framework outlines principles for the protection of*

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
Volume I and Issue I of 2023
ISBN - 978-81-960677-4-8
Published by
Institute of Legal Education
https://iledu.in

personal data across the Asia-Pacific region. It emphasises the importance of transparency, accountability, and consent in the collection and use of personal data.

Compliance with these international covenants is crucial for global companies operating in India, as failure to do so can result in legal and reputational risks. Companies must ensure that they have adequate policies and procedures in place to comply with these covenants and protect the privacy and personal data of individuals.

CASE LAWS:

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017): This landmark case recognized the fundamental right to privacy as a fundamental right under the Indian Constitution. The judgment has significant implications for the data protection framework in India.
2. Google India Private Limited v. Visakha Industries (2017): In this case, the Supreme Court of India held that online intermediaries, such as search engines, are not liable for defamatory content posted by third parties on their platforms. This case has implications for liability of online intermediaries under Indian data protection laws.
3. Aadhaar (UIDAI) v. Justice K.S. Puttaswamy (Retd.) and Ors. (2019): This case upheld the constitutional validity of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, which established a national biometric identity system in India. The case has implications for privacy and data protection in India.

THE WAY FORWARD:

The legal ramifications of Indian data protection legislation on global companies is crucial in the current digital age where data privacy and protection have become a critical issue. As technology advances and data collection increases, it is imperative that companies comply with both domestic Indian law and international covenants that protect the privacy and personal data of individuals. To move forward with this research, it is important to identify and analyse the challenges that global companies face in complying with Indian data protection laws and international covenants. This could involve conducting case studies of companies that have faced legal or reputational risks due to non-compliance, examining the implications of cross-border data transfer and data localization on multinational corporations, and identifying strategies for complying with the provisions of the Indian Personal Data Protection Bill (PDPB). The way forward for this research also involves analyzing the potential impact of the PDPB on global companies and their operations in India. This could involve examining the key provisions of the bill, assessing the challenges in complying with these provisions, and identifying strategies that companies can adopt to ensure compliance.

CONCLUSION:

In recent years, the Indian government has taken significant steps to regulate the processing of personal data in the country. The Personal Data Protection Bill (PDPB), which is currently under consideration in the Indian parliament, is a comprehensive legislation that seeks to protect the privacy and personal data of Indian citizens. The PDPB establishes new rules and standards for the collection, storage, and use of personal data by companies operating in India, including global companies. Multinational corporations that conduct business in India will be impacted by the PDPB, and it is essential for them to understand and comply with the requirements of the legislation. Failure to do so can result in legal and reputational risks, including penalties and fines. In this context, multinational corporations need to adopt robust data management policies and procedures to ensure compliance with the PDPB requirements. Overall, the legal ramifications of Indian data protection legislation on global companies are significant, and companies need to be aware of the requirements of the PDPB and other international covenants that protect the privacy and personal data of

individuals. By adopting robust data management policies and procedures, companies can ensure compliance with the legislation and avoid legal and reputational risks.

REFERENCES:

1. The Personal Data Protection Bill, 2019: Bill No. 373 of 2019, 17 December 2019.
2. The European Union General Data Protection Regulation (EU GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
3. The International Covenant on Civil and Political Rights (ICCPR): United Nations, General Assembly, 16 December 1966, United Nations Treaty Series, vol. 999, p. 171.
4. The Right to Privacy judgment by the Indian Supreme Court (Puttaswamy judgment).
5. Cadwalladr, C. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.
6. Heinze, A., & Kouvakas, I. (2018). The Facebook-Cambridge Analytica data scandal and its aftermath. Journal of Data Protection & Privacy, 2(3), 192-200.
7. Meltzer, J. P., & Sheridan, N. (2018). The impact of data localization on the global economy. Brookings Institution.
8. Sharma, R., & Choudhary, A. (2021). Data Protection and Privacy in India: An Overview. International Journal of Information Management, 57, 102308.
9. Baliga, V. (2021). India's Draft Personal Data Protection Bill: Key Features and Implications. Journal of Public Affairs, e2664.
10. Duraiswamy, K. K., & Rajesh, R. (2019). Personal Data Protection in India. International Journal of Engineering and Advanced Technology, 8(5S2), 465-471.
11. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. Chandrachud, D. Y. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India: A landmark decision. International Data Privacy Law, 7(4), 228-232.
12. Google India Private Limited v. Visakha Industries, (2017) 3 SCC 756. Singh, S. P., & Gautam, R. (2019). Intermediary liability and data protection in India: Google India v. Visakha Industries. Journal of Media Law, 11(1), 74-89.
13. Aadhaar (UIDAI) v. Justice K.S. Puttaswamy (Retd.) and Ors., (2019) 1 SCC 1. Verma, N. (2019). Privacy, Aadhaar and data protection in India. Journal of Social and Political Sciences, 2(1), 1-6.
14. Dangi, S., & Verma, P. (2018). Data Protection Laws in India. International Journal of Pure and Applied Mathematics, 119(18), 3025-3034.
15. Seth, P., & Agarwal, S. (2020). Impact of the Indian Personal Data Protection Bill on the Financial Services Sector. Journal of Financial Economic Policy.
16. Swaroop, A., & Jain, V. (2020). Personal Data Protection Bill, 2019: A Comparative Analysis with GDPR. International Journal of Engineering and Advanced Technology, 9(5), 1521-1526.
17. Gupta, T. (2020). Comparative Analysis of GDPR and Personal Data Protection Bill, 2019. Journal of Internet Law, 24(10), 1-11.
18. Singh, A. K. (2020). Personal Data Protection Bill, 2019 and its Implications for the Indian E-commerce Industry. Journal of Cyber Law & Intellectual Property, 3(1), 1-9.
19. Mallya, T., & Rane, S. (2020). Impact of India's Personal Data Protection Bill on the Healthcare Industry. Indian Journal of Health Sciences and Biomedical Research (KLEU), 13(2), 147-152.
20. Rajasekaran, V., & Murali, S. (2020). Personal Data Protection Bill: a closer look at the regulation of cross-border data transfer. Journal of International Trade Law and Policy.
21. Rastogi, A. (2018). Personal Data Protection Bill, 2018: What it means for businesses and individuals. Economic and Political Weekly, 53(2), 38-44.