JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 31

Data Localisation and Cross Border SaaS Business Compliance

Akshainie Thakur

Manipal University Jaipur

Recommended Citation:

Thakur (2026) "Data Localisation and Cross Border SaaS Business Compliance" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 31. (DOI)

ABSTRACT

This research paper endeavours to examine the way data is collected, processed and stored within the Indian Digital; ecosystems with particular emphasis on the legislative frameworks governing the privacy of citizens of India. It further seeks to analyse the regulatory mechanisms that govern cross-border transfer of data, and the obligation imposed upon the Central Government when permitting the transfer of sensitive data beyond national territories. Additionally, the paper explores the extent to which cross-border SaaS enterprises adhere to the principles of data sovereignty and remain compliant with the statutory mandates prescribed by the Government of India while processing sensitive personal data.

The paper adopts a doctrinal research methodology, drawing upon an exhaustive analysis of relevant statutes, judicial precedents, and ancillary legal material to substantiate its findings. During the research, a multitude of findings has surfaced, each of which shall be examined and deliberated upon in the subsequent sections of this paper.

KEYWORDS

Data localisation, DPDP Act, SaaS business, compliance, cross-border data transfer.

INTRODUCTION

Data localisation and sovereignty has become a very trending topic in the recent times mainly due to an excessive increase in the customers in the SaaS business sectors thus giving rise to an increased concern over how the data we provide to these businesses is stored and protected from misuse and unauthorized access. The legislative framework regarding data protection laws commenced from the Information Technology Act 2000[1]. This act laid basic procedures, guidelines for personal data protection and also laid procedure for safe cross border data transfer and also laid down penalties for non-compliance.[2]

Another milestone in the segment of data protection was established by the landmark judgement of the K.S Puttaswamy vs Union of India,[3] The judgement holds significance because this case established the "Right to Privacy" to all citizens of India. The nine bench judge ensured that privacy was an inherent right according to Article 21 of the Constitution of India guaranteeing Protection of Life and Personal Liberty.

Today the legislative framework regarding data protection laws is carried out by the DPDP Act of 2023[4]. The act also lays down the guidelines and procedure for cross-border data transfer — the act introduces a "whitelist" approach towards international data transfer[5]The Central Government of India prepares a list of countries to which data transfer is permitted; the rest of countries not on the list are considered to be "blacklisted". The countries who are on the "whitelist" are required to follow all the procedures and guidelines laid down by the DPDP Act and also any additional requirement must be fulfilled by these cross-border SaaS businesses who are being transferred the data of our citizens.

[1] Information Technology Act, 2000, No. 21 of 2000 (India)
[2] Smriti Parsheera, *A Brief History and Current Trends in Indian Data Localisation*, 15 IIMA Working Paper Series 1 (2018).
[3] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 35.
[4] Digital Personal Data Act, 203, No. 22 of 2023 (India)
[5] Ibid

The cross-border data transfers are administered by the Data Protection Board of India[6]. The board's duties are laid down by the act— some of these duties are regarding data breach. In the event of data breach, the board is empowered to undertake damage control measures, with the

[6] Ibid

primary objective of preventing further exposure of personal data. Beyond breach response, the board is also tasked with adjudicating complaints, and holds investigative and penalisation authority over consent managers found to be in violation of the act. Additionally, the board may investigate and penalise individuals who have been specifically referred to it by the Central Government. The board is also responsible for determining which foreign jurisdiction meets the requisite standards for receiving personal data originating from India, thereby is extremely significant to curate an approved list of the "whitelist" countries.

LITERATURE REVIEW

Data localisation and digital sovereignty can be studied from four main angles namely: general theories, the nation's own legal history, international comparison and practical effects on SaaS businesses.

On a theoretical note, scholars like Anupam Chander and Uyen Lê have argued that forcing countries to store data locally often ends up costing more than it is worth, without actually improving privacy in any meaningful way.[7] The idea that individuals should have control over their own personal data was first formally recognised by a German court in 1983, and this principle has since influenced privacy laws across the world, including in India.[8]

Within India, legal experts have long pointed out that the IT Act 2000 was simply not equipped to deal with the challenges posed by cloud computing and cross-border data flows[9]. The supreme court landmark Puttaswamy judgement in 2017, which recognised privacy as a fundamental right, has been widely written about and analysed.[10] Scholars have also tracked how India's data protection legislation gradually weakened its stance on strict data localisation- moving from the

[7] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677 (2015).
[8] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (2014).
[9] Prashant Reddy T., *The Evolution of Data Protection: Analysing India's Legal Framework and Global Implications*, 14 NUJS L. Rev. 1 (2021).
[10] Supra 3

strong localisation proposals of the Srikrishna committee report in 2018[11] all the way to the more flexible approach finally adopted in the DPDP Act, 2023.[12]

Looking at international pictures, researchers have extensively studied Europe's GDPR, particularly its system of approving certain countries as safe destinations for data transfers- a concept very similar to India's own whitelist model. Studies by the European Centre for International Political Economy have shown through data that heavy localisation requirements can negatively impact a country's economy.[13]

However, despite all this existing research, very little has been written specifically about how Indian data protection law affects SaaS businesses in practice, especially in business-to-business settings.[14] The paper aims to fill this gap.

METHODOLOGY

This research paper follows a doctrinal and comparative analysis approach where we shall see how the statutes regarding data protection are effective, and how they efficiently work to protect our data and shield it from misuse and unauthorised access when cross-border transfers come into play. We shall further delve into how the SaaS businesses comply with the data protection regulations laid down by the Central Government.

The primary sources heavily relied upon in this paper include statutes and legislative instruments such as Information Technology Act 2000, and the DPDP Act, 2023. Judicial precedents such as K.S Puttaswamy v. Union of India(2017)[15], also form a core part of the primary source material.

[11] Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India) (lapsed).
[12] Smriti Parsheera, *A Brief History and Current Trends in Indian Data Localisation*, 15 IIMA Working Paper Series 1,8 (2018).
[13] Matthias Bauer et al., The Costs of Data Localisation: Friendly Fire on Europe's Digital Economy 3 (ECIPE 2014)
[14] Nehaa Chaudhari & Sai Vinod, *Cross-Border Data Transfers and Data Localisation Mandate under the Data Protection Regime*, 5 Indian J. L. & Tech. 1 (2022).
[15] Supra 3

Additionally, official government documents including parliamentary committee reports, ministry consultations papers, and regulatory circulars issued by bodies such as the Reserve bank of India have been examined.

Secondary sources consulted include journal articles, academic commentaries, policy reports, and comparative legal literature dealing with data protection framework in other jurisdictions, particularly the European Union's General Data Protection Regulation[16] And The California Consumer Privacy Act.[17] These sources have not been used as an introduction of empirical dimension but rather to critically evaluate the Indian legislative framework with a broader global conversation.

The paper does not rely on empirical methods such as surveys, interviews, or statistical analysis. The scope of the research is therefore limited to what can be derived from legal texts, judicial reasoning, and established academic commentary. This paper adopts an interpretive approach, drawing on the legislative history and stated objectives of the DPDP Act to arrive at reasoned conclusions.

RESEARCH QUESTIONS

1. How effective are the data localisation provisions under India's Digital Personal Data Protection Act, 2023 in regulating cross-border transfer of personal data by SaaS platforms?

2. How do cross-border SaaS platforms comply with the data privacy laws and rules regulated by India?

3. Are SaaS companies exploiting the compliance vacuum created by India's unpublished

[16] Council Regulation 2016/679, General Data Protection Regulation, art. 6, 2016 O.J. (L 119) 1 (EU).
[17] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199 (West 2023).

restricted country list?

EFFECTIVENESS OF THE DPDP ACT

The DPDP Act, 2023 provides a legal framework to protect the personal data of the citizens of India. The act is applicable to domestic as well as international businesses, it sets guidelines for how data is collected, processed, stored and shared. This act covers what is considered essential for today's economic growth, that is cross-border data transfer. It addresses all the unanswered topics from the past which were yet to be addressed by the Legislature. With rising international SaaS businesses, it is very important for the Central Government to lay a legal framework to guide the transfer of the data and to also overlook the entire process to ensure that the data we provide to these businesses is in safe hands and is protected from misuse.

The provisions that discuss the issue of cross-border data have been regarded in section 16,17,19 and 18. We shall see what these sections talk about briefly.

Section 16[18] talks about how a data fiduciary can restrict transfer of personal data upon the notification of the Central Government. The whitelist mechanism means that transfers to countries not on the approved list are. Impermissible, effectively giving the Central Government gatekeeping authority over outbound data flows. Section. 18[19] and 19 of the DPDP Act establishes the Data Protection Board of India as the primary regulatory authority responsible for overseeing compliance, adjudicating complaints and penalising violations, including those relating to unlawful cross-border transfers. Despite the whitelist being a conceptually sane approach towards data transfers, the central government has not yet published the whitelist of approved countries. This means that the act's primary instrument for cross-border transfers remains entirely inoperative, leaving SaaS platforms and data fiduciaries without any clear legal guidance on permissible transfer destinations. The resulting regulatory vacuum is not a minor

[18] Digital Personal Data Protection Act, §16 (India)
[19] Digital Personal Data Protection Act, §18 (India)

procedural gap but it is a fundamental deficiency that renders the cross-border transfer framework effectively unenforceable in its current state.

The DPDP Act does not require SaaS companies to store Indian user's data within India, it only restricts which countries data can be transferred to. However, since the whitelist of approved countries has not yet been published, there is currently no meaningful restriction in place at all, allowing SaaS platforms to freely transfer Indian user data anywhere with legal consequences. While certain sector-specific rules such as the RBI's 2018 payment data directive[20] impose localisation requirements, these apply only to specific data categories and do not extend to general purpose SaaS platforms. Compounding this problem is the fact that even when the Act's provisions do not come into force, enforcing them against foreign SaaS companies will remain a serious challenge. The Data Protection Board is not truly independent, its members being appointed by the Central government, and it is yet to become fully operational, leaving the enforcement framework largely untested.

COMPLIANCE OF THE DPDP ACT

The DPDP Act prescribes specific guidelines that SaaS platforms must adhere to in relation to both cross-border data transfers and data security obligations.

With respect to data transfers, SaaS platforms are permitted to transfer Indian user's personal data only to countries appearing on the Central Governments whitelist. Any transfer of data beyond this list is impermissible and will be considered as a breach of the rules laid down by the DPDP Act. Data can only be transferred to a third party or another processor with the explicit authorization of the data fiduciary- a SaaS vendor cannot independently decide to transfer data to a sub-processor without client knowledge. Further, data can only be transferred for purposes that fall within the scope of the original consent obtained from the user.

[20] RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018

The act requires every SaaS platform processing Indian users' personal data to implement reasonable technical and organizational safeguards to prevent unauthorised access, disclosure, alteration, or destruction of personal data.[21] In the event of data breach or failures to non-compliance of the regulations laid down, penalties up to ₹200 crore may be imposed. The act also incorporated the principle of storage limitation, requiring that personal data be retained only as long as necessary for its stated purpose, after which it must be deleted.

However, despite these concrete rules, there is a significant legislative gap in this regard. The act does not define what constitutes "reasonable" security safeguards, nor does it prescribe specific technical standards such as encryption requirements or access control protocols. This ambiguity affords SaaS platforms considerable discretion in determining their own security standards, which risks producing inconsistent levels of data protection across different platforms and creates uncertainty for regulators attempting to assess compliance.

ADDRESSING THE VACUUM CREATED

Section 16 of the DPDP Act empowers the central government to notify a list of permitted countries for data transfer, but as of the time of writing, no such notification has been issued. The most significant operational deficiency of the DPDP Act's cross-border transfer framework is the continued absence of the Central Government's whitelist of approved countries. In the absence of a published whitelist, there is technically no list of prohibited countries either, meaning that cross-border transfers of Indian user's personal data currently operate in a regulatory vacuum where neither permission nor prohibition has been formally established.

[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R 313(E) (India).

This is stark contrast to the GDPR, under Article 6,[22] The SaaS vendor needs to have a valid legal reason to collect and process personal data. Article 32 talks about the security of the personal data provided, there should be pseudonymisation and encryption of personal data, the ability to ensure confidentiality of data.[23] Article 45 is quite similar to the 'whitelist' approach that the DPDP Act follows, the Commission in the GDPR looks after all the issues relating to cross-border transfer, they follow a criteria that the countries to whom the data is transferred must adhere to the criteria or must adopt to the criteria mentioned.[24] This is also one of the stark differences in the Indian approach, while the DPDP Act stated that the countries on the whitelist will be the only territories which are allowed cross-border transfer, there is no strict criteria that is mentioned in the DPDP Act while selecting territories for the same.

Once data is processed outside of India, it is the organisation's responsibility for handling the information, to keep it protected from unauthorised access. Some of the most important areas organisations usually need to keep in mind is-

The SaaS business must ensure that they take informed consent from the customer before transferring the data internationally. This step is necessary to maintain transparency amongst the users. The vendors must only collect what is necessary for the current operation, they must not collect extra personal data of the consumer than necessary. There must be provisions regarding deletion of excessive data transfer and also deletion of data once the task for which data was completed has been completed. Whenever there is a data breach in the facility, the SaaS business or the vendors must inform the concerned authority that is Data Protection Board as per the DPDP Act, as soon as possible to mitigate the damages.

Due to lack of operational function, there is a lot of grey area that needs to be addressed. By the legislative authority with regards to the Data Protection laws, the DPDP Act is a very concrete

[22] General Data Protection Regulation §6, 2016 O.J. (L 119) 1 (EU).
[23] Ibid § 32
[24] ibid § 45

framework but due to unenforceability of the act there is little to no actual backbone to support the SaaS businesses and their responsibility to adhere to the compliance law because there is no hardcore provisions relating to the same.

DISCUSSION

Based on the research question, we can conclude that there is ambiguity regarding the data protection laws and also the compliance with regard to the cross-border compliance. The DPDP Act provides a solid backbone for data protection laws in India however to it in non-operational there is nothing for the data privacy laws to rely upon and the international SaaS businesses suffer as well[25].

We see how well the European data privacy laws have been drafted in the consolidated version of GDPR, where it is clearly established what criteria will be followed when the Commission decides what countries are allowed the transfer of the personal data. This is quite the same for the DPDPA, but there is still quite a grey area that needs to be addressed.[26]

Firstly, there must an established criteria as to what countries will be on the whitelist approved by the Central Government, there must be a set of rules and regulations that the data is transferred internationally is the responsibility of the SaaS businesses or vendors to protect the data provided, as provided in the GDPR, the territories to whom the data is provided they must encrypt the data or pseudonymisation the personal data provided. This step ensures that the data consumers provide is in safe hands and is protected from misuse. This is what the Indian privacy laws can also adopt in its legislative framework, with increasing Indian consumers and an

[25] Vila Seoane, M. F. (2021). Data securitisation: the challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750. https://doi.org/10.1080/01436597.2021.1915122
[26] Rana Saurav Kumar Singh et al., Data Localization and Its Impact on Cross- Border Digital Trade in India: Legal, Economic, and Strategic Implications, 30 Educ. Admin.: Theory & Prac. 3326,3330 (2024).

increasing cross-border data transfer demand, data breach or misuse of the data provided is inevitable thus to mitigate the risks, encryption of data is a necessary and important step.

Secondly, there must be strict non- compliance penalties as mentioned earlier, in the event of non-compliance a fine of ₹200 crore will be imposed on the SaaS businesses however due to the accountability in case of data breach comes on the data fiduciary rather than the SaaS vendor this means that Indian enterprise client that transferred the data to the international SaaS company will be liable more in the event of data breach. This a serious concern for when it comes to cross-border data transfer, because even if the data fiduciary transfers the data after following all the required background checks and taking all the necessary precautionary steps, the data breach after a successful transfer is now part of the SaaS business data inventory and it is their responsibility to ensure that the data is protected from breach. Hence, the Indian legislative machinery must work on this particular issue as well.

CONCLUSION

The Indian data privacy laws have come a long way, from simple and minimal data storage to cross-border data transfer to multi-millionaire companies. Earlier there wasn't much of a need to transfer data internationally but as globalisation happened, businesses expanded and so did the Indian consumer base. The Central Government recognised the need to transfer data internationally rather than to store data domestically is better for the economy in the long run. With the enforcement of the IT Act in 2000 which established the laws regarding localisation of data and the very tiniest mention of cross-border transfer, they provide very basic legal structure regarding cross-border transfer.

The final advancement comes in the form of DPDPA, 2023 where it is clearly established the laws and the legislative framework regarding cross-border transfer. The whitelist approach is a very concrete approach to cross-border transfer, however as stated above multiple times the lack

of a Government approved list of countries published creates a very grey area in a very otherwise solid approach. The government needs to have a proper analysis done of all international territories that have all the requirements for a safe data transfer and storage. They must possess all the acumen and advanced technology to also minimise the risks of data breach because the data of Indian consumers is very sensitive and it can be misused when approached with malicious intent. If the legislative machinery works on the above mentioned grey areas, the DPDPA can be a very foolproof execution of the legislative minds at work and this legislative piece can be followed without hesitation across the nation.