Impact Of Data Localisation Laws On Global Tech Companies

Table of Contents

Abstract

This research paper undertakes an extensive examination of the far-reaching consequences of data localisation laws on global technology corporations, with a specific emphasis on the regulatory landscape within India. This encompasses an in-depth analysis of India's Data Localisation Laws, prominently featuring the Digital Personal Data Protection Bill of 2023, and a comprehensive exploration of the broader impact of these laws on the operations, innovation, competitiveness, data security, and compliance dynamics of global tech giants.

The study unravels the intricate web of effects stemming from data localisation laws. It investigates how these regulations substantially increase operational costs for multinational technology firms, driven by the need to establish local data infrastructure and compliance mechanisms. Furthermore, it explores how these laws can stifle innovation by imposing constraints on the free flow of data and the development of cutting-edge technologies that depend on global data accessibility. The paper also reveals how data localisation mandates can limit competition, inadvertently favouring domestic companies over international tech giants. While scrutinising the regulatory landscape, the research paper highlights potential risks to data security arising from data localisation laws. It offers insights into how these regulations may inadvertently lead to fragmented data storage practices that expose sensitive information to new vulnerabilities.

In addition to dissecting the challenges, this research paper investigates how global tech companies are strategically adapting to India's data localisation laws. It provides detailed case studies of industry leaders like Google and Facebook, shedding light on their innovative compliance strategies. These strategies include establishing on-premises data storage facilities, partnering with local cloud providers to maintain a presence while adhering to data localisation requirements, implementing advanced data anonymisation and pseudonymisation techniques, and entrusting specific data processing tasks to third-party entities.

In conclusion, this paper summarises its key findings and recommends policymakers navigating the complex terrain of data governance and global technology innovation. These recommendations are intended to strike a delicate balance between safeguarding data privacy and fostering an environment conducive to global technology enterprises' continued growth and advancement. The research serves as a valuable resource for shaping corporate strategies and regulatory frameworks in an increasingly data-centric world, contributing significantly to the ongoing discourse surrounding the nexus of data governance and the global technology industry.

Introduction

Data localisation laws are becoming increasingly common worldwide, and India is no exception. In 2006, British mathematician Clive Humbly said, "Data is the oil of the 21st century." This has indeed been valid with the rapid growth of the digital economy. Data plays an increasingly important role as an economic and strategic resource. It can be used to make decisions with economic impacts, environmental impacts, or effects on health, education, or society in general. The volume of data in the world is increasing exponentially. As per the UN's digital economy report, in 2021, 64.2 zettabytes of data were created in 2020, a 314 per cent increase from 2015.[1] Data localisation refers to various policy measures that restrict data flows by limiting data's physical storage and processing within a given jurisdiction's boundaries. **National security, privacy, and economic development** concerns often motivate these laws.

India is one of the countries that has enacted data localisation laws. In 2019, the Indian government introduced the Digital Personal Data Protection Bill, requiring businesses to store certain types of personal data within India. The Bill was passed in Parliament in August 2023. According to Rajeev Chandrasekhar[2], Minister of State for Electronics and Information Technology of India, this bill has two primary objectives. *"Firstly, it puts a break on companies misusing personal data. Secondly, it will teach a deep behavioural change in how companies deal with citizens, consumers and businesses. It aims to bring more responsibility and accountability".*

This paper will explore the impact of data localisation laws on global tech companies. We will first provide a background on data localisation laws, discussing their purpose and the different types of existing laws. We will then discuss the impact of data localisation laws on global tech companies, focusing on the challenges and opportunities these laws create. Finally, we will offer some recommendations for global tech companies on mitigating the challenges of data localisation laws.

The impact of data localisation laws on global tech companies can be significant. These laws can increase costs, make innovation more difficult, limit competition, harm data security, and pose compliance and operational challenges. Global tech companies must consider these laws' impact before operating in countries with data localisation requirements. The paper will conclude by discussing the future of data localisation laws. As the digital economy grows, more countries will likely adopt data

[1] https://unctad.org/system/files/official-document/der2021_en.pdf
[2] https://www.youtube.com/watch?v=WqXC0D0RvQ8

localisation laws. This will create challenges for global tech companies and opportunities for new businesses and business ways.

A. Background on data localisation laws

Governments enact data localisation laws for various reasons, including

a. To protect national security: Governments may want to ensure that sensitive data, such as military or intelligence, is not stored in foreign countries.
b. To protect privacy: Governments may want to give individuals more control over their data and prevent it from being transferred to countries with weaker privacy laws.
c. To promote economic development: Governments may want to create jobs in the local data storage and processing industry to encourage economic growth.

There are many different types of data localisation laws. Some laws require businesses to store all data within the country, while others only require firms to keep certain data types, such as personal or financial data. Some laws also allow businesses to store data in a foreign country if the data is encrypted or if the foreign country has strong privacy laws.

Data Localisation Policy Around the World

Data localisation policies have become increasingly prevalent as governments seek to balance the need to protect citizen privacy with the desire to promote economic growth. On the one hand, data localisation can strengthen personal data protection. For example, the European Union's General Data Protection Regulation (GDPR) requires businesses in the EU to keep personal data within the boundaries of the EU or to transfer it only to countries that offer adequate data protection safeguards.

On the other hand, data localisation can also demotivate businesses from operating in a particular country. It can limit the ability of governments and companies to reap the full benefits of data. For example, Russia's strict data localisation laws have been criticised for discouraging foreign investment and innovation.

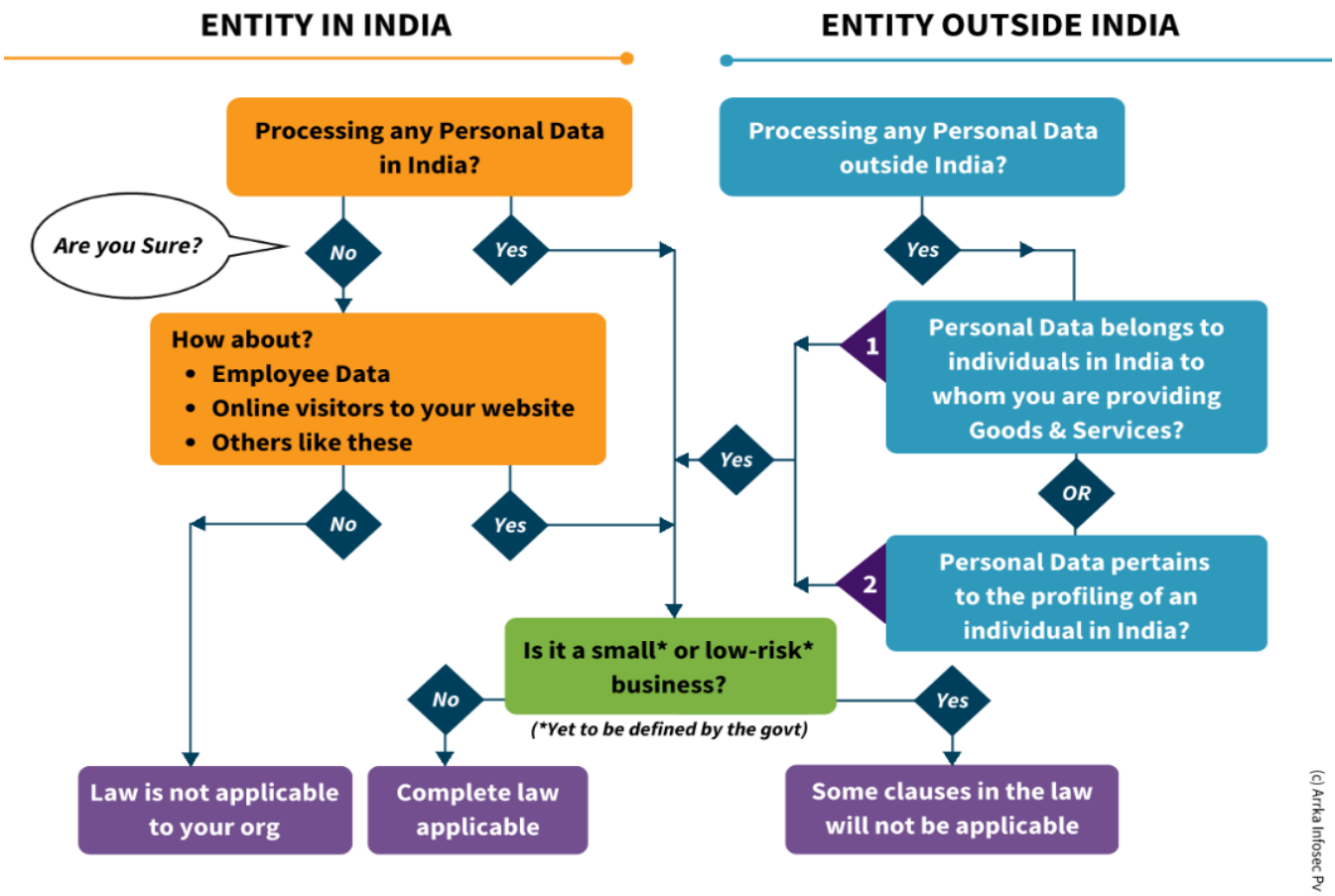
In the wake of Brexit, the UK has allowed most data to continue flowing from the EU and the European Economic Area without additional safeguards. However, in the case of "restricted transfers," such as data related to national security or law enforcement, UK laws will mirror the GDPR.

In 2010, **Malaysia** enacted the Personal Data Protection Act. Personal data can only be transferred outside Malaysia if the government approves the action.

In 2012, **Australia** enacted the Personally Controlled Electronic Health Records Act, which requires that personal health records be stored only in Australia.

B. Impact of data localisation laws on global tech companies

Data localisation laws have a profound impact on global tech companies, primarily resulting in increased costs, innovation challenges, and limitations on competition. These regulations necessitate local infrastructure and compliance personnel investments, driving up operational expenses. Innovation is hindered as companies may hesitate to develop products dependent on cross-border data transfers due to regulatory hurdles and compliance concerns. Furthermore, these laws create barriers that impede foreign tech firms' ability to compete in local markets, as they often mandate local data storage, adding complexity and expenses to market entry.



3

[3] https://www.linkedin.com/company/arrka/

India's Data Localisation Laws

A. The Digital Personal Data Protection Bill, 2023

The Digital Personal Data Protection Bill 2023 (DPDP) is a proposed law regulating personal data processing in India.[4] The Bill defines "data" as *a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means*, and "personal data" means *any data about an individual who is identifiable by or in relation to such data*. The DPDP Bill would require organisations that process personal data to obtain consent from the individual before doing so. The Bill also sets out several other requirements for organisations that process personal data, such as taking appropriate security measures to protect the data. Some have criticised the DPDP Bill for being too restrictive. For example, the Bill would require organisations to store all personal data of Indian citizens within India. This could make it difficult for organisations to operate in India, as it would need them to set up data centres in the country.

According to Chapter IV, clause 16 of the DPDP Bill,
(1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.
(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

This section quoted from the Digital Personal Data Protection Bill, 2023 (DPDP Bill) gives the Central Government the power to restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified. This means that the Central Government can ban the transfer of personal data to certain countries or territories if it believes that the data will not be adequately protected in those countries or regions.

The DPDP Bill defines a "**Data Fiduciary**" as *any person who, alone or in conjunction with others, determines the purpose and means of processing personal data*. This means that any entity that decides what personal data to collect, how to use it, and who to share it with is considered a Data Fiduciary.

---

[4] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

The PDP Bill also includes a provision that nothing in the section restricting the transfer of personal data outside India shall limit the applicability of any other law in force in India that provides for a higher degree of protection for or restriction on the transfer of personal data outside India. Any other Indian law that prohibits or restricts the transfer of specific personal data outside India will take precedence over the section in question.

Here are some examples of how the Central Government could use its power to restrict the transfer of personal data outside India:

1. The government could ban the transfer of personal data to countries that do not have adequate data protection laws.
2. The government could ban personal data transfer to countries with a history of engaging in mass surveillance or other human rights abuses.
3. The government could ban the transfer of personal data to countries considered geopolitical rivals of India.
4. The government's power to restrict the transfer of personal data outside India is intended to protect the privacy and security of Indian citizens' data.

However, some critics have argued that this power could be used to stifle economic growth and innovation.

B. Other data localisation laws in India

In addition to the DPDP Bill, several different data localisation laws exist in India. These laws apply to specific sectors, such as finance and telecommunications. For example, the Payment and Settlement Systems Act of 2007[5] requires payment system providers to store all payments-related data within India. The Telecom Regulatory Authority of India (TRAI) has also issued regulations that require telecommunications service providers to keep all call detail records (CDRs) within India.[6]

C. The analysis of India's data localisation laws

Some have criticised the data localisation laws in India for being protectionist. They argue that these laws make it difficult for foreign companies to operate in India and stifle innovation. Others say that the data localisation laws are necessary to protect the privacy of Indian citizens. They say that these

[5] https://lddashboard.legislative.gov.in/sites/default/files/A2007-51_0.pdf
[6] https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf

laws help prevent organisations' misuse of personal data. The impact of India's data localisation laws on businesses still needs to be determined. Some companies can comply with the rules with little difficulty. However, other businesses may need help to comply and change their operations. The data localisation laws in India are a complex issue. There are several factors to consider, such as the need to protect the privacy of Indian citizens, facilitate innovation, and ensure that businesses can operate effectively in India.

Impact of India's data localisation laws on global tech companies:

A. Increased costs

Data localisation can make it more difficult for global tech companies to innovate. This is because they may be restricted from accessing data stored in other countries.

B. Difficulties in innovation

Data localisation can make it more difficult for global tech companies to innovate. This is because they may be restricted from accessing data stored in other countries. For example, a global tech company that develops a new machine learning algorithm may only be able to use this algorithm in India if the data the algorithm is trained on is stored in India. This could limit the company's ability to sell its products and services in India.

C. Limitations on competition

Data localisation can give local businesses an unfair advantage over global tech companies. This is because local businesses can access data unavailable to international tech companies. For example, a local business that provides cloud storage services may be able to offer its services at a lower price than a worldwide tech company if the local business does not have to comply with data localisation laws. This could make it difficult for the global tech company to compete in the Indian market.

D. Potential harm to data security

Data localisation can potentially harm data security. This is because it can make it more difficult for businesses to protect data from unauthorised access. For example, suppose a business is required to store data in a data centre in India. In that case, it may be more difficult to protect this data from unauthorised access by the Indian government or other third parties.

E. Compliance and Operational Challenges

Data localisation can pose compliance and operational challenges for global tech companies. This is because they may need to comply with a variety of different laws and regulations, and they may need to adapt their operating procedures to meet the requirements of data localisation laws. For example, a global tech company that operates in India may need to appoint a data protection officer, implement security measures to protect data, and report data breaches to the Indian government. These requirements can add to the workload of the company and can make it more challenging to operate in India.

How Global Companies Are Adapting to India's Data Localization Laws

A. Google

Google is one of the largest technology companies in the world. It collects user data, including search history, email, and photos. To comply with India's data localisation laws, Google is setting up a data centre in India. The data centre will be located in Hyderabad, Telangana, and is expected to be completed in 2024. The data centre will store data from Google's users in India, which will help the company to comply with the law.

B. Facebook

Facebook is another large technology company that collects a lot of user data. To comply with India's data localisation laws, Facebook works with local partners to store data in India. The company has partnered with the Indian telecommunications company Reliance Jio to keep data from its users in India. Facebook is also working with other local companies to store data in India.

Compliance strategies for global tech companies in India

A. On-premises data storage

On-premises data storage is storing data on physical servers within the company's premises. This is the most secure way to store data, as it is not accessible to third parties. However, setting up and maintaining on-premises data storage can be expensive and time-consuming. There are several benefits to on-premises data storage. First, it is the most secure way to store data. The data is physically located within the company's premises, and it is not accessible to third parties. This makes it less likely that the data will be stolen or compromised. Second, on-premises data storage gives the company more control over the data. The company can choose the hardware and software that is used to store the data, and it

can also decide the security measures that are implemented. This gives the company more flexibility and control over data storage and management. Third, on-premises data storage can be faster than cloud-based data storage. This is because the data is located closer to the users, reducing the time it takes to access it.

However, there are also some challenges associated with on-premises data storage. First, setting up and maintaining on-premises data storage can be expensive. The company needs to purchase the hardware and software, and it also needs to hire staff to manage the data storage infrastructure. Second, on-premises data storage can take time to scale. If the company needs to store more data, it may need to purchase additional hardware and software. This can be a challenge, especially for small businesses. Third, on-premises data storage can be less reliable than cloud-based data storage. The data is on physical servers, which can be damaged or destroyed in a natural disaster or other event.

B. Cloud-based data storage with a local presence

Cloud-based data storage with a local presence is a type of cloud computing that stores data in a cloud environment but with the data being physically located in a specific country or region. This contrasts with traditional cloud computing, where data is stored in multiple locations worldwide. There are several benefits to using cloud-based data storage with a local presence. First, it can help to comply with data localisation laws. Many countries have laws that require businesses to store certain types of data within the country. Companies can ensure compliance with these laws by storing data in a cloud environment with a local presence. Second, it can improve data security. By keeping data in a specific country or region, businesses can reduce the risk of data being accessed by unauthorised parties. This is because the data will be physically located within the country's borders and subject to the country's laws and regulations. Third, it can improve data performance. Businesses can reduce data access latency by storing data in a cloud environment with a local presence. This is because the data will be located closer to the users, reducing the time it takes to access it.

However, some challenges are associated with using cloud-based data storage with a local presence. First, it can be more expensive than traditional cloud computing. Businesses must pay for the additional infrastructure and resources to store data locally. Second, it can be more complex to manage. This is because companies need to control the data in multiple locations and ensure that the data complies with the laws of each country. Third, it can be less flexible. This is because businesses may need help to move data between different cloud regions quickly.

C. Data anonymisation and pseudonymisation:

Data anonymisation and pseudonymisation can make data less identifiable. This can be done by removing or replacing specific personal identifiers, such as names, addresses, and phone numbers. Anonymised data can still be used for statistical analysis and research purposes but cannot be used to identify individuals. There are several benefits to data anonymisation and pseudonymisation. First, it can help to protect the privacy of individuals. Removing or replacing personal identifiers makes it more difficult to identify individuals from the data. Second, data anonymisation and pseudonymisation can help to reduce the risk of data breaches. If the data is anonymised or pseudonymised, it is less valuable to attackers. Third, data anonymisation and pseudonymisation can help to comply with data protection laws. Many data protection laws allow for the processing of anonymised or pseudonymised data without consent.

However, there are also some challenges associated with data anonymisation and pseudonymisation. First, anonymising or pseudonymising data can be difficult without losing too much information. If too much information is removed, the data may no longer be valid for its intended purpose. Second, data anonymisation and pseudonymisation can be a time-consuming and expensive process. The company needs to carefully consider the data that needs to be anonymised or pseudonymised, and it also needs to implement the appropriate technical measures.

D. Transferring data to a third-party processor

Transferring data to a third-party processor is outsourcing data processing to a third-party company. This can be a good option for companies needing more in-house resources or expertise to manage data processing. However, it is essential to choose a third-party processor with a strong security track record that complies with India's data localisation laws. There are several benefits to transferring data to a third-party processor. First, it can help to reduce the costs of data processing. The company does not need to invest in its data processing infrastructure; it can also benefit from the expertise of the third-party processor. Second, transferring data to a third-party processor can help improve data processing efficiency. The third-party processor can often process data more quickly and efficiently than the company can do in-house. Third, transferring data to a third-party processor can help improve data processing security. The third-party processor may have a more robust security track record than the company and more experience handling sensitive data.

However, some challenges are associated with transferring data to a third-party processor. First, the company must choose a third-party processor with a strong security track record that complies with all

applicable laws and regulations. Second, the company needs to sign a data processing agreement with the third-party processor that clearly defines the responsibilities of each party. The agreement should include data security, privacy, and breach notification provisions. Third, the company must monitor the third-party processor's compliance with the data processing agreement. The company should also regularly audit the third-party processor's data processing practices.

Conclusion

A. Summary of the key findings

i. Data localisation is a complex issue: There are many factors to consider when evaluating the potential benefits and challenges. These factors include the type of data being localised, the location of the data, the security measures in place, and the impact on businesses and individuals.
ii. Data localisation can help protect individuals' privacy: Data localisation can make it more difficult for unauthorised actors to access personal data. This is because the data will be stored in a specific location, and it will be subject to the laws and regulations of that location.
iii. Data localisation can also harm innovation and economic growth: It can make it more difficult for businesses to operate and innovate. Companies may be restricted from accessing data stored in other countries. This can lead to higher costs, decreased efficiency, and lost opportunities.
iv. The impact of data localisation will vary depending on the specific circumstances: The effect of data localisation will vary depending on several factors, such as the size and type of business, the industry, and the location of the data. For example, data localisation may significantly impact businesses that rely on data for their operations, such as businesses in the technology sector.

B. Recommendations for Policymakers

In today's digital age, the crossroads of technology and data governance have never been more crucial. India's data localisation laws are instrumental in ensuring data security and sovereignty but require careful calibration to accommodate global tech companies' operational needs and foster innovation. To this end, this paper proposes a set of actionable recommendations aimed at creating a balanced data localisation ecosystem that encourages compliance, enhances data security, and keeps pace with industry dynamics. These recommendations include the establishment of a Unified Compliance Portal, the Implementation of a robust Data Access Framework, and the introduction of Periodic Regulatory Impact Assessments. Each of these measures contributes to a regulatory environment that

is both supportive of data protection and innovation while simplifying compliance for global tech companies.

1. **Establish a Unified Compliance Portal:**

   Create a centralized online platform that serves as a one-stop resource for global tech companies to understand, submit, and track compliance requirements related to data localisation. This portal should provide comprehensive information, guidelines, and forms, making it easier for companies to navigate the regulatory landscape. It should also offer a user-friendly interface for submitting compliance documents, reporting data breaches, and seeking clarifications. By centralizing compliance processes, policymakers can reduce the administrative burden on businesses and enhance transparency in regulatory procedures.

2. **Implement a Data Access Framework:**

   Develop a clear and standardized framework for data access that outlines how government authorities can request and access data stored locally. This framework should include strict privacy safeguards, specifying the conditions under which data can be accessed, ensuring proper authorization, and requiring transparency in data requests. It should also establish an independent oversight body responsible for reviewing and approving government data access requests. This approach strikes a balance between data security and accessibility, assuring global tech companies that their data remains protected from unauthorized access.

3. **Periodic Regulatory Impact Assessments:**

   Institute a regular and mandatory process for conducting Regulatory Impact Assessments (RIAs) of data localisation laws. These assessments should evaluate the impact of regulations on global tech companies, considering aspects like compliance costs, innovation hindrances, and competitive dynamics. Policymakers should use the findings from these assessments to adapt and refine data localisation laws as needed. The process should be transparent, involving industry stakeholders, legal experts, and technology experts to ensure a comprehensive evaluation of the regulations' effects on the tech ecosystem.

References:

1. https://deloitte.wsj.com/cmo/3-data-management-challengesand-4-ways-to-respond-01667325840
2. https://www.linkedin.com/company/arrka/
3. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264
4. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
5. https://www.livemint.com/Industry/3F1s3435zQCPBgkvYjDSEK/How-localization-of-data-will-affect-firms-consumers.html
6. https://www.wsj.com/articles/for-u-s-tech-indias-draft-privacy-bill-has-hidden-risks-11669989692
7. https://www.washingtonpost.com/business/indias-data-protection-bill-has-a-privacy-problem/2022/11/22/972e6a90-6ac2-11ed-8619-0b92f0565592_story.html
8. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
9. https://www.barandbench.com/columns/rbi-mandates-data-localisation-for-payment-services
10. https://www.livemint.com/Opinion/P9bGTw36JUx8YTK0RxKGhN/The-economic-impact-of-a-strict-data-localization-regime.html
11. https://www.pwc.in/assets/pdfs/consulting/risk-consulting/the-digital-personal-data-protection-act-india-2023.pdf
12. https://www.wsj.com/articles/BL-252B-10438
13. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357
14. https://www.livelaw.in/lawschool/articles/the-indian-space-program-237249?infinitescroll=1
15. https://www.livelaw.in/articles/arbitration-award-stamp-duty-indian-stamp-act-238558?infinitescroll=1
16. https://www.washingtonpost.com/opinions/2021/09/27/internet-freedom-decreases-again/
17. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019
18. https://www.wsj.com/articles/for-u-s-tech-indias-draft-privacy-bill-has-hidden-risks-11669989692