RES MILITARIS Social Science Journal

# SOCIAL MEDIA LAWS RELATED IN INDIA

**Inderjeet Kaur[1] , Sadhna Trivedi[2], V.V.B.Singh[3],Kaneez Fatima[4]**

**Abstract:**

Social media usage in India has grown exponentially in recent years, necessitating the formulation and implementation of laws and regulations to govern its usage. This abstract explores key social media laws in India, encompassing regulations related to content moderation, privacy protection, cyber security, and intermediary liability. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 stand out as a significant regulatory framework, imposing obligations on social media platforms to ensure the removal of objectionable content within specified timeframes. Additionally, the Personal Data Protection Bill aims to safeguard user data privacy, while the Cyber Laws of India encompass provisions addressing cybercrime and digital security. Understanding and compliance with these laws are imperative for individuals, businesses, and social media platforms operating in India's digital landscape.

**Keywords:** Social media, laws, regulations, India, content moderation, privacy protection, cyber security, intermediary liability, Information Technology Rules, Personal Data Protection Bill, Cyber Laws.

## Introduction

Have you ever sent an email, a phone call, or filed a tax return? Do you use a Smartphone, smart watch, or fitness bracelet? Do you use the Internet to shop online? Are you using Alexa?

Most of the answers to the questions above are yes. If the answer is yes, your personal information will be transferred.

Undoubtedly, there are many advantages to using these devices. At this stage, life without these skills is unimaginable. We rely on them in our day-to-day work and through this we interact with others. But there are risks. You may think that there is no harm done to you, but the picture is different. Our data tells a lot about us. It reflects our personality, our likes and dislikes, our friends, our lives, our thoughts, and more. Privacy extends to data and information protection.[5]

[1] **Dr. Inderjeet Kaur, Associate Professor, Faculty of Juridical Sciences, Rama University,**

[2] **Dr.Sadhna Trivedi, Associate Professor, Faculty of Juridical Sciences, Rama University**

[3] **.Dr.V.V.B.Singh, Associate Professor, Faculty of Juridical Sciences, Rama University**

[4] **Kaneez Fatima Teaching Associate,Faculty of Juridical Sciences, Rama University,**

[5] **Rakesh Chandra, Privacy Rights in India with reference to Information Age 188 (Mayur Printers, New Delhi, 2017)**

There is no doubt that our data is valuable and a new currency. The potential of data is still unknown, and almost everything people do generates it. Some questions to consider include: Who owns the data and who has access to it? How can I use it? How does this affect privacy and can it be a restriction on the data used by your company?

It is surprising that Face book recently shared 87 million user data with CA. This is not isolated or exceptional. State and non-state actors are detrimental to individual rights as they are largely unregulated. Protection of rights is necessary not for the benefit of one individual, but because such goodwill creates a collective culture in which people can resist unacceptable state behavior. Many businesses are taking advantage of digital information to benefit. Data can be easily misused and harm people. The worst-case scenario is when governments use data about vulnerable individuals. Therefore, strong data protection legislation is needed. The right to privacy is a fundamental right, and the responsibility for its protection and infringement rests with the state. Recent privacy decisions have highlighted the need for data protection legislation in the information technology era. The courts have said that appropriate legislation is needed for non-state actors. Kaul J. (paragraph 70)198 believes that states should ensure that information is not used without the user's consent. Therefore, in this regard, Congress has enacted data protection legislation to prevent non-state actors from violating the rights of citizens. In this light current chapter discusses the concept of data protection, the existing legal framework for the protection of data privacy in India. The newly drafted Data Protection Bill and its analysis. The chapter also highlights key reasons for modification in the current bill, And the need for a dedicated or omnibus piece of legislation in a country that protects privacy.[6]

## 1 Meaning of the Term Data Privacy and Data Protection

Before understanding the meaning of data privacy and protection, there is a need to know the concept of personal data. Data can be broadly classified into two:

### 1. Personal Data

It refers to any information that relates to an identified or identifiable living individual. Or any information, if combined with others, can lead to the identification of a particular person. Example: person name, surname, address, email, identification card number, financial information, medical history, etc. GDPR defines[7] personal data as any information relating to an identified or identifiable natural person (data subject). Personal data may be collected by individuals, organizations, governments or institutions.

### 2. Non-personal data

Refers to information that one cannot identify. It holds economic value, but in this case, there is no violation of personal information. Some examples of data that can be considered as personal data - company registration number, company email address, anonymous data, etc[8].

[6] "What Does Privacy Mean?", Available at: https://iapp.org/about/what-is-privacy/ (last visited on April 14, 2022)

[7] Information Technology (Reasonable Practices and Procedures and Your Sensitive Data or Information)

[8] Regulations, 2011, available at: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (last visited by April 14, 2022

Data privacy is a human right to control his or her personal information. It is the right to determine how personal information is collected, shared, and used. It is part of the right to privacy, and in the case of complex technology development, it needs to be protected.[9]

Data confidentiality is not only about data management but also about personal expectations for privacy. In these technological years personal data is an asset that needs to be protected from reckless action. In simple terms, it can be said that data privacy means who is authorized to access data. The main focus of data privacy lies in the use and management of personal data.[10]

The concept of data protection is related to personal data. Ensures that data is processed fairly and legally. In data protection, policies and procedures seek to limit the access of personal privacy through the collection and use of personal data. It can be defined as legal control over access to and use of data. Data protection can be referred to as a process of protecting personal information from misuse. It involves the relationship between data collection and distribution and technology. Data protection is not just a measure of technology; rather, it includes an administrative measure. Administrative action refers to the legal component of it.

Data privacy is focused on the use and management of personal data such as setting policies to ensure that consumer personal information is collected, shared, and used in appropriate ways. Data protection is primarily focused on protecting data from malicious attacks and exploitation of stolen data for profit.[11]

Although security is needed to protect data, it is not enough to deal with privacy[2].

## 2 Current National Data Protection Regulations

There is currently no specific data protection law in the country. Privacy and data protection are subject to various laws pertaining to information technology, criminal law, intellectual property rights, and contractual relationships. The Planning Commission forms a committee of experts led by retired judge A.P. Shah. The Committee has developed policies to protect the right to privacy.[12]

The use and transfer of personal data is governed primarily by the IT Act (2000) and its Regulations, 2011[3]. A code of conduct provides rules governing the collection, transfer, and use of personal information. This law is primarily intended to protect electronic data and other aspects of information technology such as cybercrime and e-commerce. What worries you most is e-commerce, not privacy, as it used to be who was beaten as a result of the adoption of the UNCITRAL e- commerce law model in 1996.[13] The IT Act was amended in

[9] Information and Technology Act, 2000 (Act 21 of 2000), subsection. 2 (1)

[10] Id., E.g. 2 (1) (v)

[11] Id., E.g. 2 (1) (v)

[12] Id., E.g. 43

[13] Id., E.g. 43 Definition (ii).

2008 and received approval from the President in 2009.[14] The Act provides for certain provisions relating to data protection after the 2008 amendment. It now provides us with mandatory policies and penalties in the event of a breach of those privacy policies. The following categories of action that may be considered appropriate for data protection are:

- Section 2 (1) (o) of the Act defines the term "data." According to it, data is a representation of information, knowledge, facts and concepts instructions

That is corrected or corrected in a legal way. It is also intended to be processed or used or processed in a computer program or network or stored within a computer memory. It does not provide a definition of personal data.[15]

- Section 2 (1) (v) provides the term "information" which includes: data, message, text, images, sound, voice, codes, computer programs, software and website, film or computer produced.[16]
- S. 43 covers a wide range of issues, which create public liability against the perpetrator and provides for damages to the person affected by the circumstances described. It is noteworthy that compensation for online violations in this category can only be granted if anyone is involved in that access, disruption, denial, etc. The section does not consider the case where the subject of the data was not created in any unauthorized access. , but such access has resulted in a violation of her privacy rights.
- S. 43A has been added and is an appropriate provision for protecting data privacy. Requires anyone involved to use and maintain proper security and procedures when managing, selling, or managing SPI with computer resources. It states that the action must result in an unjust loss or unfair gain to any person in order to hold the board company accountable.[17]

Legal liability is unavoidable under the current arrangement on the grounds that there has been no negligence on the part of the company in implementing or maintaining appropriate security procedures. Sensible safety measures and procedures will do develop procedures and procedures to protect information from unauthorized access, damage, use, modification, disclosure, or damage as may be specified in the agreement between the parties or as may be specified in any applicable law. In the absence of such an agreement or law, the federal government may put in place security measures and procedures in consultation with professional organizations and organizations. But s. 43A says nothing about "Personal Identification Details," The definition of SPD is limited. Provides a community solution under s. 43A only when there is negligence in the organization and it causes unfair loss and wrong gain to others and the offer is quiet about the extra-territorial app. Ss. 43 and 43A are also lacking in the provision of compensation; due to this shortage, the supply is often misused by companies. Companies file frivolous claims against their former employee, who has joined another company in the same file.[18]

---

[14] Id., E.g. 45

[15] Id., E.g. 43 Definition (ii)

[16] Id., E.g. 66.

[17] [4]Information and Technology Act, 2000 (Act 21 of 2000), subsection. 2 (1) (o

[18] Id., E.g. 2 (1) (v)

- A residual penalty or compensation in the event of non-compliance with legal provisions is also specified.

• The action and makes any person charged with if dishonest or fraud does not apply to the verb specified in subsection.43[19]

In addition, some new features have been added, which address cyber security and cybercrime challenges, though not directly. Ss. 66A- 66F[20], added to the 2008 amendment, includes a number of cybercrime charges, including offenses related to sending offensive messages[21] with the help of a computer or communication device, receiving or storing any stolen service or device for dishonest communication, or for any reason.[22] Similar beliefs, using an electronic signature, password or other identifiable identifier, impersonation cheating, breach of privacy, cyber terrorism.[23]

S. 66E[24] is a straightforward arrangement for personal privacy. This section is primarily aimed at preventing voyeuristic behavior in the field of assisting the secret clicks of video technology. Electronic transmission of obscene material, penalty for publishing or transmitting sexually explicit material, etc., electronically penalty for publishing or transmitting child pornography to the sexually explicit material, etc., electronically and electronically[25].

Responsibility for data storage and storage rests with the 177 coordinators and the powers vested in the authority's (Institution and State) to issue guidelines for the concealment or monitoring or interpretation of any information on any computer system.[26] "[2021] IT Rules, 2009, are provided under subsection. 69A of IT Act to restrict access to any information to any computer service by the public.219 the power to issue directives to restrict public access to any information on any computer resources by the federal government is in addition to failure to comply with the order. has a prison sentence and a fine.[27]

[23] Supra note 201, s. 69A

---

[19] Id., S. 66C. [6] Id., E.g. 43

[20] S Id., E.g. 66A

[21] Id., E.g. 66D.

[22] [13] Id., S. 66C. [6] Id., E.g. 43

[23] [7] Id., E.g. 43 A

[24] Id., E.g. 66E.

[25] Id., E.g. 66F

[26] Id., E.g. 67

[27] [22]Information Technology (Procedures and Protections for Blocking Public Information) 2009, available at: https://meity.gov.in/writerreaddata/files/Information%20Technology%20%28%20Procedure%20and%2 0protection% 20for% 20blocking % 20for% 20access% 20of% 20information% 20by% 20public% 29% 20R ules% 2C% 202009.pdf. (last visited April 14, 2022).

• The following important provision in the law is s. 72 relating to breach of confidentiality and secrecy.28[28]
• S. 72A also deals with privacy law when information about a breach of legal contract is disclosed. Penalty under the previous clause. 72 for the disclosure of information was limited only to those who were legally authorized to obtain access to an electronic record and document under the law, and therefore s. 72A installed. The 2008 Act also provides for debt to creditors and other persons for breach of confidentiality and confidentiality under a contractual contract.[29]
S. 72A also does not specifically mention the use of additional space to protect data and privacy. S. 72A criminalizes the breach of privacy and confidentiality. However, in cases where a criminal sentence cannot be imposed for breach of confidentiality and confidentiality, no remedy is available for any form of compensation to victims of such breach of privacy and confidentiality. It seems to be a bit of writing as it only deals with information, which is found in the contractual relationship between the parties. There is therefore a lack of formal protection of unauthorized information that is compromised by violating the privacy of data in electronic services.
Rule 2 (1) (i) [30]defines personal information as any other information relating to a natural person. It may be directly or indirectly related and, if combined with other available information, could identify such a person. SPDI, on the other hand, is said to be part of the personal information system that contains information related to: Password, financial information such as bank account or credit card or debit card or other details of payment instrument, physical, physical, and mental health, sexual orientation, medical records and history, biometric information, or any information related to the above categories as provided by the board company, by providing a service; and, any information obtained under the above clauses by a company that is working hard to be processed or retained under a legal contract or otherwise.[31]
It provided otherwise that information that is freely available or publicly accessible or provided under the RTI Act, 2005, will not be regarded as SPDI. The SPDI[32] type provided in the law is limited compared to other available definitions. The definition does not consider information related to a person's political opinion, philosophy, culture, or religious beliefs. Other rules and regulations that a hardworking company must comply with are:

[31] Id., Rule 5 (4[33]

[32] Id., Rule 5 (5).

[28] Supra note 200, rule 2 (i).
[29] Id., Rule 4 (1
[30] Id., Rule 5 (1

[31] Id., Rule 5 (2).

[32] Id., Rule 5 (3
[33] Id., Rule 5 (4

• Privacy and Disclosure Policy:[34] The Corporation and any person on behalf of the business will provide a privacy policy for the management or handling of personal information, including the SPD. That policy will be published on the board's website. The policy will consist of the following components:[35]
1. Policies and policies should be clearly defined, and that should be easily accessible.
2. Type of personal or sensitive personal data or information collected.
3. Purpose of the collection and use of such information.
In accordance with rule 6, disclosure of SPD or information.
5. As a rule 8 safety procedures and procedures must be in place.
When these rules are changed by the body corporate, what to do is never discussed. Whether there is a need to give notice in advance or not, is not stated in the rules.
• Collection Permit: rules authorizing a board organization to seek approval before collecting SPDI. Permission must be in writing, faxed, or emailed about the purpose of use.
• Limitation on collection: A body corporations may collect information, for the first time, if it is collected for a legitimate purpose, linked to a business activity. Second, data collection is required.
• Direct information collected:[36] there is a need for specific action, through a corporate board, while direct information is collected. It should be ensured that the information provider is aware of the following points:
1. The fact that information is collected.
2. Purpose of the collection.
3. Who is the target of such information?
Organizational information collected and stored information, i.e., name and address.
• Retention limit: [31]the governing body may not retain information collected for longer than required for the purpose for which it was collected or by other legislation.
• Purpose: Information collected cannot be used for any purpose other than that collected.[37]

---

• Modification or amendment: At the request of the information provider, the board company must provide an opportunity for the provider to review the information. It must ensure that any information found to be incorrect or defective is corrected or amended. But the board body will not be responsible for the accuracy of the information.

---

[34] Id., Rule 5 (5).

[35] Id., Rule 5 (6

[36] Id., Rule 5 (6).

[37] [34] Id., Rule 5 (7).

• Withdrawal of permit: Business body prior to collecting information, will notify the information provider that you have the opportunity to remain anonymous. The law also gives the information provider the right to withdraw the license. This withdrawal will be sent in writing.[38]

• Protect information: the governing body is responsible for protecting the information provided.[39]

• Complaints Officer: the governing body will appoint a grievance officer to resolve any dispute with the information provider[40].

**4 Review of Your Data Protection Bill, 2019**

The PDPB, 2019, proposes to protect individual privacy.[41] The bill is designed to process data and create trust relationships. Faith and belief should be maintained among people whose data is processed and businesses process personal data. It describes how personal data should be handled, that is, provides for social media, arbitrator, border transfers, and other related matters.

**1 Key elements of the Bill**

• Application of the Law:[42] The Bill governs the processing of personal data in the event of data collection, disclosure, distribution, or processing in India. (i) Government, (ii) Companies, Indian citizen and any other person included. under Indian Law, and (iii) data keepers or data analysts working in India with personal data are included in this bill.

**5 Certain points will be reconsidered in the 2019 Bill[43]**

Undoubtedly, the bill is an important law that promises to give authority over personal data to its principal. A pending consideration before the Joint Committee of Parliament, the bill is enshrined in the fundamental rights and constitutional principles enshrined in any democratic society. The bill is designed to protect the constitutional guarantees of privacy. A bill to provide a just and equitable perspective on India's digital economy in the future.

The PDP bill is based on both the laissez-faire method, U.S. law, and the GDPR's strong system, the European Union; The bill is designed to balance between two key issues in any nation, namely, privacy and security. Includes features that have later entered the legal dictionary, such as the right to forget. It is a much-needed step towards a growing digital economy and society. All stakeholders are kept in mind during the drafting of the bill, and the resulting economic and industrial economic impact is evident.[44]

Nevertheless, the bill is not far from being criticized, and is widely criticized by civil society organizations, companies, lawyers and academics across the country. B.N. Srikrishna J.

---

[38] Id., Rule 5 (7).

[39] [35] Id., Rule 5 (8).

[40] Id., S. 2 (A) (a).

[41] [38] Id., E.g. 2 (A) (b) & (c).

[42] Supra note 248

[43] Supra note 249, s. 26(4).

[44] s.93 (1) (d) & s. 28(3).

himself has warned about the uncontrolled power and legal status granted to the Supreme Government. He described it as a "dangerous practice,"[45] which could lead to "Orwellian Province." Other concerns regarding surveillance, government access to anonymous and private information with companies, lack of clarity on local data processing requirements, and deregulation of DPA powers by giving greater power to Central Government. Some of the key points that will be considered in the bill are:

- Uncontrolled Power in Central Government: Many attacks are carried out on systems that give greater power to the Central Government. For the purpose of surveillance, the open alternatives offered by the government have been challenged by civil society organizations.[46]

## 6 Comparative Analysis of Personal Data Protection Bill, 2019 with Srikrishna's Committee Draft Bill, 2018

The PDP Bill, 2019 is mainly based on the draft bill proposed by the Justice Srikrishna Committee. However, the 2019 bill introduces some new concepts and deviates from the 2018 bill in certain respects. Here is a comparative analysis of the bills to see how the bill of 2019 differs from the bill of 2018.[47]

- Personal Data and Sensitive Personal Data: The draft bill, 2018 provide that personal data relate to characteristic, traits or attributes of identity that can be managed to identify an individual. The bill of 2019 added an identifiable trait whether online or offline. Thus, including any inference drawn from such data for the purpose of profiling. The definition has been extended to incorporate inferred data, which is a positive move as it will expand data principals right under s. 17, he can ask for such data as well.

Further, in 2019 bill, the term password has been removed from SPD, which was there in 2018 bill, the power to further categorise personal data has been given to the Central Government (in consultation with DPA).[48]

- Social Media Intermediaries and voluntary verification: Term SMI was missing form draft bill of 2018. Not only the term SMI is defined but SMI are identified as "significant data fiduciaries."[40] They have to obey certain additional obligations and are mandated to give their users the option to voluntarily verify their accounts in the prescribed manner.[41] Obligations such as data protection assessment, maintenance of records, audit and appointment of data protection officer are to be performed by such SMI.[49]

The officials of the government in support of the provision have remarked that it will decrease the anonymity of users and prevent trolling and the process is voluntary for users and can be completely designed by the company.[50]

- Data Localization requirement diluted: The 2019 bill has dropped the mandatory

[45] Id., s.93 (1) (d) & s. 28(3).

[46] [42] Supra note 248, s. 40

[47] [42] Supra note 248, s. 40

[48] Supra note 249, s. 33 & 34

[49] Id., s. 35

[50] Supra note 248, s. 42

requirement for storing a mirror copy of all personal data.[42]The bill trifurcates personal data and some types of personal data are considered SPD and another subset is CPD. However, storage/ transfer of SPD and CPD are still restricted. Under the 2019 bill, CPD can be transferred to another country/ class of entity/ international organization deemed permissible and where the transfer in the Central Government's opinion does not prejudicially affect the security and strategic interest of the State. This is a departure from the 2018 bill, and hints at a greater emphasis on State interest and a noticeable devaluation of the interests of data fiduciaries.[51]

Removing mandatory mirroring requirement, in case where explicit consent has been given, is a favorable change made, as State should not impose these kinds of restrictions.

•Extensive powers of the Central Government: The draft bill, 2018 has permitted government to access the personal data for security purpose.[45], Under this proposed bill the power of Government has been widened by giving Central Government unrestricted authority to immune any government agency from applicability of the bill.[46] The Central Government is also given additional powers to make rules on the following:

1. Other categories of SPD.[47]
2. The procedure of voluntary identification of social media and the identifying mark of verified users.[48]
3.The fashion in which the Central Government can issue a direction for seeking non-personal data from data fiduciary and data principal (including specific purposes for which such data is sought) and the form of disclosing such directions.[49]

The bill usually deals with data collected by consent and does not apply if the data is used without permission. Without consent, this does not mean that it is illegal; instead, it is legally permitted and monitored.[52]

- Exempt Small Businesses: The proposed bill allows for exceptions in the case of small businesses looking at personal customer information. However, it does not claim any relevance qualifications and gives power to DPA.
- Data Principal Rights: The data principal rights under the 2018 Bill include the right to obtain consensus, to attempt to adjust and control (transfer or restrict) further disclosure of their data. The 2019 bill adds another right, that is, the right to delete personal data if it is no longer needed.[50] This submission is beneficial to the data principal as he may request the deletion of data if it is no longer required.[53]
- Removal of a Member of the Judiciary: The Srikrishna committee bill provides for the inclusion of a member of the judiciary in the electoral committee.[51] The electoral committee under the 2018 bill was mandated to make recommendations to the government regarding the appointment of DPA members. This member's involvement in the judiciary has been withdrawn from the current draft bill.[52] Now it is only controlled by the Central Government with regard to its composition and selection considerations.[54]

---

[51] Supra note 249, s. 35

[52] Id, s. 15.

[53] [48] Id., s. 28(4).

[54] Id., P. 91 (2).

## Conclusion

Strict law in the field of data privacy is an hour requirement. Despite a few actions by various government agencies directed at data protection legislation, to date, the Government of India has failed to come up with a comprehensive law. The need for confidentiality of information has been raised by various parties and recent court rulings also highlight the great need for effective law. Incidents, such as academy details sold on the black web, [53] CA Scandal, Pegasus spy line and many other similar breaches raise concerns about data security in India.

The purpose of the data protection law is not just to protect personal data but its purpose is to protect the fundamental rights and freedoms associated with personal data. Complete provision of data protection is not only necessary for the protection of rights but also ensures a fair and just trade for consumers. Two of the main concerns of data management are: protecting the privacy of the right person and using the same data for the benefit of the economy. The two of them enter freely so there is a need to resolve this dispute while writing the data law.

The drafting of a data protection law in India has been quiet and unpredictable. To date data protection is governed by the IT Act, 2000, which deals primarily with online security. The bill, which is being considered by a select committee before it is passed, is widely criticized for its inconsistencies. Although your privacy and infringement are kept in mind at the time of writing this law be respectful. The current bill is very protective in nature as it primarily governs the collection and use of personal data. It does not protect the privacy of information but rather provides a solution in the event of a breach. The bill significantly transferred more power to the State's role in the data economy and increased threats to State surveillance.

From its point of view and the clause of intent, the bill seeks to place the privacy interests of individuals and businesses and the State in the same place. The bill brings some disappointment especially after the Supreme Court's strong decision regarding the right to privacy and the committee's report. In a very different language it was said by the court that coding these files was a step towards fulfilling a fundamental right. However, this framework works for the political economy. In the current government, technology and national security are a priority and protecting privacy is not the main goal of government.

The current bill fails to fully succeed as it is unable to deliver on its promises and raises fears about privacy protection. The bill did not provide for the protection of the individual but rather passed a form of private agency power to public bodies. Certain problems in this bill require an effective approach. The bill requires social media companies to verify who the users of social media are to combat falsehoods, forced non-personal transfer of personal data to government, separate State agency is one of the major risks to this bill. These threats to India's privacy protection may hold back emerging Indians trying to grow globally, or at large data processing companies in India.

Moreover, the blurring of the distinction between non-personal data and personal data remains a matter of concern. The bill ultimately reduces the protection of individual data rights by allowing the state to have access to anything it feels is within its reach. Giving excessive power to the government and its authority without proper scrutiny is a major law. It must adhere to clear and concise guidelines for the executive council to exercise its powers. This important law should not be ignored by the PDP Bill.

The bill should look at India's ability to regulate emerging market economies and small democratic countries. The current bill makes India an unpopular model for those countries looking to establish a new data management concept that combines the right to privacy with fundamental civil liberties. Hopefully, the Joint Committee of Parliament looks at the shortcomings and perceived implications of this bill before it is finalized. As this bill will have a huge impact not only on its citizens but also on Indian businesses and MNCs.

_____-