India's Proposed Data Protection Law and Analysis of India-US Executive Agreement Under the CLOUD Act

INTRODUCTION

The digital economy is burgeoning in India. The country has more than 300 million social media users, more than 580 million internet subscriptions, and 74 billion UPI transactions reaching INR 125.84 trillion in 2022, and at last, the e-commerce consumer base is expected to outplay the US in coming years. The data and data storage are non-rivalrous good. Data is consumed by large numbers of people and corporations, its control and distribution however happen without the consent of the owner. The concepts of security and privacy are still developing. In November 2022, Central Depository Services Limited (CDSL) central securities depository detected cyber malware in machines, disconnecting from the capital market. Recently, data from AIIMS, Delhi was also breached. Furthermore, the frequency of ransomware attacks in 2021 impacted even Indian organizations. The majority of such attacks happen in data centers. Cybersecurity risks make individuals and organizations extremely vulnerable. With the internet, every aspect of life from home automation to individual fitness routines is now digitized. Therefore, all such incidents command a public policy to protect data and a person's privacy. The right to Privacy has now been regarded as a fundamental right by the Supreme Court in 2017. This further brings the question of protecting personal data to the forefront. The right held that informational privacy or privacy to maintain personal data and facts also comes under the ambit of the Right to Privacy. This paper intends to understand and analyze India’s Data Protection Bills introduced in 2019

and again in November 2022. It also emphasizes the debate around India- US Executive Agreement under the CLOUD Act.

TRACING ROOTS OF THE PROPOSED LAW

In recent years, both public and private entities have made use of a large amount of personal data for decision-making processes. The right to informational privacy or privacy of informational facts or data comes under the reach of the Right to Privacy. The right to Privacy was declared as the fundamental right by the Supreme Court in the *Puttaswamy v Union of India* case in 2017. Considered as a part of Article 21 i.e. right to life and personal liberty, the right to privacy also includes the right to be forgotten. Personal data of an individual pertains to traits, characteristics, or attributes of the identity of an individual, helping to identify the person. Non-personal data means any information through which the identity of a person cannot be known. Data protection can be understood as safeguarding personal data from practices like corruption, compromise, or loss, through policies and procedures established by the government ensuring minimum intrusion into an individual's privacy. Presently there has been no specific regulation dealing with data protection of personal information. Information Technology Act 2000 is the only regulation so far that specifies security safeguards for data collection, disclosure, and transfer of information for data agencies. In July 2018 committee was established under Justice Srikrishna focusing on the issues related to data protection and widening realms of the digital economy. The committee in its report suggested that the IT Act has not kept up with the ongoing pace of digital transformation. Also, the definition of sensitive personal data is narrow and some provisions are overridden by contract. It has made recommendations to draft specific

rules for data entities involved in procuring the data along with forming a data protection body to bring in more compliance with the law.

DATA PROTECTION DRAFTS SO FAR

The draft for the first data protection law in India came up in 2018. It was proposed by the Justice Srikrishna Committee set up by the Ministry of Electronics and Information Technology (MeitY). With revisions to this draft, it was introduced as Personal Data Protection Bill, 2019 (PDP Bill, 2019) in the Lok Sabha in 2019. This draft was also referred to the Joint Parliamentary Committee of both Houses of Parliament. Adhering to the recommendations, a new draft called the Data Protection Bill came up in 2021. The bill was introduced in Lok Sabha in 2019 by the Ministry of Electronics and Information Technology aiming to ensure personal data protection. Major motives of the Bill included ensuring that the privacy of an individual is maintained concerning personal data, establishing a framework for processing such data, and establishing a Data Protection Authority for the same purposes. Data Protection Authority, with a chairperson and six members having 10 years of experience in the data protection, public administration, or information technology field, must be responsible for the following :

1. Prevent misuse of the data
2. Compliance with the act for the stakeholders
3. Protect the interests of the individuals by taking the required steps

However, the bill has now been withdrawn in August 2022.

DIGITAL PERSONAL DATA PROTECTION (DPDP) BILL 2022

The draft **Digital Personal Data Protection Bill 2022** was released in November 2022 by the Ministry of Electronics and IT (MeitY). The bill outlines the rights and duties of digital citizens while laying out procedures for companies for data collection. Data Protection Board of India as established by the law, will deal with violations of the procedures of the law and also imposes heavy penalties. The decisions however can be challenged in the High Court. The proposed law is based on seven principles:

1. The first principle stated is personal data collection and usage by organizations must be lawful, fair, and transparent to the individuals involved.
2. The second principle states that data must be used only for the purpose it was collected.
3. The third principle is based on Data Minimisation. It means the data controller must set the limits of the collection of personal information only to the purposes that are relevant and essential for serving the required purpose.
4. The fourth principle stands for data accuracy.
5. The fifth principle of the draft states data collection should only be for a limited period and cannot be done by default by the data collectors.
6. The sixth principle reinforces that safeguards are necessary ensuring unauthorized collection and processing of data must not happen.
7. The seventh principle discusses the accountability of the person collecting and processing personal data.

The law defines personal data as " any data by which an individual can be identified." Processing means "the entire cycle of operations that can be carried out in respect of personal

data.” Therefore it includes a complete process of collection, storage, and processing. The bill defines “Data Principal” as the individual from whom data is collected. “Data Fiduciary” is the entity deciding the “purpose and means of the processing of an individual’s data.” This entity could be an individual, enterprise, company, or even a state. The bill discusses the data collection and accountability even for children (users under the age of 18 would be classified as children), here parents would be considered “Data Principals”.

Data Fiduciaries under the Law 2022

Data Fiduciaries will be defined on numerous factors ranging from the volume of data collected, the risk of the potential harm it holds, and its impact on the sovereignty and integrity of the nation. Data Fiduciaries will be obliged to manage additional obligations for ensuring a greater sense of security. These entities will also have to appoint Data Protection Officer and Data Auditor to ensure grievance redressal and compliance with the act respectively.

Other Provisions

Data Principals have the right to demand the erasure and correction of data by the Data Fiduciary. And file a complaint when the latter fails in the compliance with the law. The bill allows cross-border storage and transfer of data to “certain notified countries and territories” after a significant assessment of relevant factors by the Central government. In case of data breaches or failure to inform data principles for data breaches, financial penalties will be imposed on the concerned entity.

Upcoming Digital India Bill intends to commit crimes like identity theft, catfishing, cyberbullying of children, doxxing, gaslighting, and impersonation. Online platforms like social media platforms, e-commerce, fact-checking portals, and artificial intelligence platforms will also be given a set of guidelines to follow. Such social media handles will be responsible for algorithmic accountability. Online intermediaries with complete access to internet services while having no control over the content issued by them will be brought under the proposed Bill. It is stated that a regulatory body akin to TRAI will be established. Directives will be formed for violations, and regulatory procedures for metaverse and blockchain to be patterned. Previously it has been mentioned by the Ministry that for cross-border data, the enforceability of Indian citizens' rights, reciprocity (in aspects of digital trade), and access to data in an emergency will be mandatory.

RECOMMENDATIONS

- Experts have argued about the reduced independence of the proposed Data Protection Board and vast exemptions in the law concerning the Central government and its bodies. Thus it is recommended to ensure regulatory authorities work independently keeping individual interests.
- Data collection solely on the Data Principal’s consent ignores that concerned individuals are not always aware of complete know-how of the processes and information which is sufficient for a particular need. The DPDP Bill must categorize personal data as “sensitive personal data” which may include biometric data, genetic data, and health data. Such sort of data may require higher protection, especially in terms of explicitly stated consent and compulsory data protection impact assessment.

- A clear mandate for Data Fiduciaries is necessary for the information which must reach the Data Principals. This includes the rights of data principals, grievance redressal mechanism, the retention period of the information obtained, the motive of information collected, the sources it will reach, and even the potential harm it may or may not cause.

DATA PROTECTION GLOBALLY

EU Model- General Data Protection Regulation or GDPR is the EU's landmark data protection law for collecting and processing personal data. The law has been criticized for its stringency and multiple obligations on part of organizations involved in data processing. The law has also served as a template for many nations globally. The EU recognizes the right to privacy along with the right to protection of personal data, which must be maintained by both private and public entities where data collection and processing comes into the picture. However, certain exemptions for the same include national security, defense, and public security. These grounds are also well defined in the law.

US Model- The right to privacy referred to as Liberty Protection seeks to protect everyone’s personal space from governmental entities. The regulation has been inadequate in parameters like accountability and regulation. It allows for data collection as long as individuals are not informed. Regulations and control for government are well defined whereas, for the private entities, only sector-specific norms are in place.

China Model- Personal Information Protection Law (PIPL) in effect from 2021, is similar to the EU's GDPR in giving individuals rights to share, correct, and delete their data. It impacts companies' power to deal with and transfer data and provides overarching powers to the

government to collect and regulate private entities. It also discusses stringent penalties in case of breaches and defaults conducted and even suspends operations in cases of non-compliance. Cross-border transfer of data can only happen with internal security review and requires approval from several authorities.

IN FOCUS: THE CLOUD AGREEMENT

As it is known, presently deliberation is going on for formulating a comprehensive data protection law in India. With the proposed Data Protection law, the government plans to address the challenges associated with the digital world. In march 2018 US government passed an act called the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). This law serves two major purposes:

1. Clarified that the US government could make orders regarding the production of electronic evidence in the "possession, custody or control'' of the US service providers, regardless of where such evidence was stored.
2. Allows the US government to enter into executive agreements with the foreign government allowing foreign law enforcement agencies to have access to communications content directly from US service providers.

In simple terms, CLOUD Act speeds up the access to electronic information held by service providers in the US ranging from terrorism and violent crimes to sexual exploitation of children and cybercrime to the foreign partners to whom such information is critical. The US government has for the first time agreed with the UK government under the CLOUD law in 2019. It has also signed an agreement with Australia in 2021 and is in talks with the European Union (EU) as

well. Earlier to avail such secured information from US service providers, the foreign government had to enter a Mutual Legal Assistance Treaty (MLAT), a lengthy and error-prone process. With the coming of the Data Access Agreement, the UK government will be able to procure information and evidence held by the service providers. The agreement relates to the prevention, detection, investigation, or prosecution of serious crimes and the retrieval of data more quickly than before.

The following are the two requirements of the CLOUD Act:

1. Clear mandates and procedures for government access and effective oversight

2. Commitment to free and open data

Before entering into the executive agreement CLOUD with the U.S. government, domestic laws and commitment to international laws are examined. The most prominent laws that govern the digital space in India are discussed below. And India's position with the requirements of the CLOUD act is also analyzed.

The Information Technology Act 2000 (IT Act) and its Rules pertain to data interception, monitoring, and decryption in electronic form. Through this Act federal and state governments seek interception, monitoring, or decryption of any electronic data. The government does so to safeguard the "sovereignty and integrity of India, the security of the State, and public order, or to prevent incitement to an offense relating to these specific grounds".

The Criminal Procedure Code 1973 (CrPC) applies to criminal investigations and includes access to any evidence. This route is available to both court and police officers to compel the production of data. Under Section 91, police officers in charge at particular police stations have

the power to seek the production of any document from the person who has possession. Similarly, Courts can order the same through summons. Police officers issue orders to tech companies for retrieving email and other data. The Court under the law can issue search warrants if "has reason to believe that a person may not comply with the order issued under Section 91". The law " allows the court to issue general warrants to allow police officers to seek information when it is unknown in whose possession such information may be". Mostly this legal route is used by police officers without securing Court orders. The process can fail to meet the requirements of the CLOUD Act of clear mandates for access. Orders issued by police officers can be challenged before courts. It is difficult to say it would meet the standards of independent oversight stated under the CLOUD Act. Other significant safeguards like restrictions around the use of the collected data, who can use or view such data, retention periods, and other organizational and technical safeguards are required.

The **IT Act** has some of the safeguards mentioned above. However, its review committee and its procedures and independence have been pointed out by privacy advocates.

Further taking into consideration the second requirement of the CLOUD Act which is a commitment to the global free flow of information and open internet, few difficulties exist. For instance, **the Reserve Bank of India (RBI)** which regulates the financial sector in India requires payment companies to secure data locally. It also requires that data must be detected from foreign servers if taken outside. Such hard data localization norms become impediments to the second requirement of the CLOUD agreement.

Before entering into a bilateral agreement, it is essential to understand the already existing pact between the US and UK governments. For the first time, the bilateral agreement has been signed

between the US and UK governments, compelling US technology companies like Facebook, Twitter, and Google to provide data content that included emails, texts, and direct messages to UK's Law Enforcement Bodies when required. The agreement requires the UK companies to do the same. Now both nations would not have to follow the cumbersome procedures of "mutual legal assistance" which consumes a period of six to twenty-four months. The new system, however, prioritizes speed over safeguarding and raises concerns over protecting human rights considering the privacy hijack in terms of handling sensitive personal data by tech companies. Governing bodies of both countries, the US Department of Justice (DOJ) and the UK Serious Fraud Office (SFO) can request data on child sexual abuse, terrorism, and other serious crimes from the respective companies in the countries. As per the agreement, private litigants will not have access to the data. While making bilateral pacts to ensure cooperation in the transmission of data, one must be cognizant of the relationship between the powers of the state and laws to protect the fundamental rights of the citizens. Evidence of the large use of IT systems is visible in causing cyber attacks. However, terms such as 'serious crimes', 'national security', or 'prevention' of criminal acts are capacious and thus need to be established explicitly. This makes abuse of clauses stated in such agreements for meeting one's purposes and harming the democratic ideals of other parties uncomplicated. As an example, laws against the concept of hate speech in one country may constitute a restriction on freedom of speech in another country. Moreover, the US Supreme Court has time and again claimed that its laws are for domestic land, however, CLOUD Act may seem to subvert this assertion. The agreement also builds grounds for forming one large database. Besides, problems that are global need supra-regional agreement for adequate solutions. Consider an example of climate change, for assuring environmental protection will need resolutions of every nation. One such international treaty for the right to

privacy and cyber security is the Cyber-Crime Convention developed under the UN Special Rapporteur.

CONCLUSION

It must be admitted that a positive transition in privacy law formulation is noted. The deliberations on the bill have been conducted that included not only legal professionals, policymakers, and some politicians, the law has been made accessible to every citizen considering its impacts. Large-scale surveys outlining online habits, preferences, behaviors, and digital literacy levels would help policymakers make well-informed and intelligent decisions.

Bibliography

https://indianexpress.com/article/technology/tech-news-technology/digital-personal-data-protection-bill-2022-released-8276193/

https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece

*ORF_Report_DataProtection-CloudAct.pdf (orfonline.org)

A comparison of data protection laws: India | Asia Business Law Journal