RE-THINKING DATA LOCALISATION IN INDIA: GAPS IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Khushi Sharma, Christ (Deemed to be University), Delhi NCR

ABSTRACT

This paper examines the evolution and need for Data Privacy in India, recognizing data as the new Oil, which significantly impacts the lives of individuals across the country. With the increasing reliance on data, efficient legislation addressing data privacy concerns has become imperative. The paper traces the evolution of data privacy through case laws and a comprehensive analysis of the legal framework in India, while comparing it with globally renowned legislations such as the General Data Protection Regulation (GDPR). It thoroughly examines the GDPR and respected legislations of various jurisdictions to study diverse approaches on the topic. It elucidates key principles such as transparency in data collection, processing, and storage, as well as accountability and ethical handling of data.

Additionally, the paper explores the emerging issues of Data Localization and cross-border data transfers, highlighting their potential benefits and challenges. It further proposes recommendations for strengthening India's data privacy framework to better align with global standards while addressing the unique challenges faced by the nation. In conclusion, the paper critically analyzes the existing loopholes in current data privacy legislation, the importance of transparency and user consent, and evaluates Data Localization as a policy in India, offering insights into its future implications.

Keywords: Privacy, Localization, Encryption, Consent, Legislation

INTRODUCTION

India is among the most recent countries to pass legislation regarding data privacy. Privacy is the basic freedom from unreasonable interference and to be left alone without arbitrary intrusion, it is a way to protect ourselves and safeguard our own space. Whereas, data privacy or digital privacy is regarding the personal information we share online. Data privacy is a sub-part of privacy that protects our data shared with private entities from misuse. Looking back even the mere concept of privacy was first recognized globally in the United Declaration of Human Rights in 1948 through Article 12[1]. With the first time privacy as a concept was introduced and recognized by the world, countries started becoming vigilant about it and drafted provisions to improve privacy in their respective countries. OCED (Organization for Economic Co-operation and Development) in 1980[2] first time formulated guidelines regarding the protection of privacy and transborder flows of personal data. With this, the basic foundation of privacy in the digital sector was laid and has been going through transformation since then. A major transition came into being when the European Union in 1995 passed Directive 95/46/EC[3]. It sets up a framework for the collection and processing of personal data. It aims to process data fairly and lawfully, at the same time prohibits special categories of data collection such as health information, sex information and political opinions etc. With this, frequent regulations from different corners of the world were set up resulting in widening the scope of data privacy and the emergence of data localization.

Data localization, also known as Data Residency law requires data to be stored, processed and collected within that country before being transferred overseas. Data can only be transmitted when that particular country or entity fulfils the required privacy and protection laws. Data localization is comparatively a newer concept to protect the security, integrity and personal information of the users residing in a particular country. After all, 'Data is the new Oil'. The General Data Protection Regulation (GDPR)[4] is the globally most reputed and landmark guideline on Data Protection and Data localization. It covers the rights of the data subject, controller and processor, transfer of personal data to third countries, remedies and penalties,

[1] Nations U, "Universal Declaration of Human Rights" (*United Nations*) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed August 17, 2024
[2] "OECD Privacy Principles" <http://oecdprivacy.org/> accessed August 17, 2024
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[4]'(*General Data Protection Regulation (GDPR)*, 22 April 2024) <https://gdpr-info.eu/> accessed 17 August 2024

provisions on specific processing situations and cooperation and consistency.

INDIAN CONTEXT ON PRIVACY

In India, the right to privacy became a fundamental right after being included in Article 21[5], the Right to Life and Liberty in 2017 after a long debate passing through several cases. It was a prolonged journey of right to privacy getting the status of fundamental right under the ambit of the Right to Life and Liberty. Life and Liberty itself is a very broad concept, no person should be deprived of his life or personal liberty except as per the procedure established by law. This is the most important right provided to the citizens which contains their basic rights to live a healthy life and the privileges or liberties they enjoy being the citizen of the country. There are several cases explaining and broadening the definition while including various rights under the ambit of life and liberty, and eventually right to privacy was also added.

It started from the M.P. Sharma v. Satish Chandra case[6], wherein the Supreme Court denied the right to privacy being protected by the Constitution of India. In the case, the government of India ordered an investigation into a company on the allegation of embezzlement of funds and fraudulent transaction violative of the Indian Criminal Code, 1860. The District Judge ordered the search and seizure of the property which is challenged as being violative of Article 19(1)(f) and Article 20(3) of the constitution. The petitioner challenged that the conducted investigation was unreasonable and harmful to the reputation of the company and that the search was a substitute for forced surrender, therefore a form of forced testimony which is prohibited according to the constitution. The petitioner relied on the Fourth Amendment of the United States Constitution, which protects its citizens from unreasonable seizure to safeguard their privacy and security. In the judgement, the court refused to adopt the principles of the Fourth Amendment of the United States Constitution and dismissed the allegation stating that the Right to Privacy is not part of the Constitution of India.

Kharak Singh v. State of U.P[7]., where Kharak Singh was discharged from the charges of dacoity due to lack of evidence. Uttar Pradesh Police Regulation, chapter 20 gives police the power of surveillance on criminals or suspects who are likely to be habitual criminals. The power was challenged in the court as being arbitrary, unconstitutional and violative of rights guaranteed

[5] Constitution of India, Article 12
[6] M.P. Sharma v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300
[7] Kharak Singh vs The State of Uttar Pradesh & Others, (1964) 1 SCR 332

by Article 19(1)(d) and 21 of the Constitution. The judgement upheld regulation 239 and denied that the Right to Privacy is protected by the Constitution of India. Whereas, the minority opinion recognized privacy being an important part of personal liberty under Article 21. However, both the cases, M.P Sharma and Kharak Singh were overruled by the Supreme Court in the landmark K.S. Puttaswamy case.

K.S Puttaswamy case[8] is where the Right to privacy was officially held to be part of Article 21 in the Constitution of India. The issues before the court were whether the Right to privacy is a fundamental right as it has not been expressly said in the constitution and whether the Right to privacy is absolute as affirmed in many previous judgements constitutionally. The right to privacy was held to be an element of human dignity and an inalienable natural right that will fulfil the aim of the welfare state as mentioned in the Constitution. The Supreme Court also laid down the test of proportionality where there has to be a rational connection between the object and means laid down to achieve it, it should at least satisfy the basic test of 'fair, reasonable and just' procedure under Article 21 of the constitution. The bench also recognized seven types of privacy through various examples, one of which was informational privacy, the privacy of a person linked to their use of the internet must also be recognized. Thus, Data Privacy finally got recognition and legislation protecting the same was the need of the time.

NEED FOR DATA PRIVACY

In the digital age where everything is going through a digital transformation, information keeps on increasing which in turn concerns us about our data. The development of technology and the internet has various implications for individual life. Not all developments tend to have a positive impact, which risks people's identity and sensitive information. The continuous growth of technology forces us to share our basic information with intermediaries to have access to various platforms. The power and impact user data can hold, and what its misuse can lead to can be well analyzed through the Facebook and Cambridge Analytica Scam, 2018[9] and Equifax Data Breach, 2017[10].

[8] Justice K.S.Puttaswamy (Retired). vs Union of India And Ors., 2017, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

[9] Confessore N, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" *The New York Times* (April 4, 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed August 17, 2024

[10] Electronic Privacy Information Center, "EPIC" (*Equifax Data Breach*) <https://archive.epic.org/privacy/data-breach/equifax/> accessed August 17, 2024

Facebook and Cambridge Analytica Scam, 2018

Cambridge Analytica firm exploited the personal data of 87 million Facebook users without their consent. It all started with a research firm namely, Cambridge Analytica which partnered with a U.K.-based academic, Aleksandr Kogan who was using Facebook data for his research. Kogan developed a simple quiz called " This is your digital Life", it asked simple personality questions similar to many quizzes now available online. But it required logging in with your Facebook account, which gave Kogan access to your Facebook profile and data such as your birthdate, location and friends network. Quiz results and Facebook data were used to develop a psychometric model and then combined with the voter records, he sent them to Cambridge Analytica. His app also grabbed the personal data of your Facebook friends and compiled similar profiles of them. In a few months, 270,000 people took the survey and the data of 87 million users were harvested. The parent company of Cambridge Analytica, SCL called itself a 'global election management agency' and was reported for its involvement in disinformation campaigns social media branding and voter targeting. Allegedly, US polling and voting data were transferred to Russian intelligence services by Cambridge Analytica's contractor. SCL's work in the political world primarily revolved around gaining public opinion and manipulating viewpoints and political will. The same involvement was found during Trump's political campaign. Kogan claimed that the research was for academic purposes. Facebook states that there is no data breach as no passwords were stolen and no systems were infiltrated but rather was a breach of trust between Facebook and its users.The Impact was that the scandal revealed a gross violation of privacy. People entrust social media platforms with their data, but the trust was shattered. The personal data of a user is very integral part of a person which is shared with a platform. The scandal was a breach of Integrity. The aftermath revealed that approximately 75% of the users changed their settings and disabled or deleted accounts. Cambridge Analytica allegedly used the data to manipulate the 2016 U.S. presidential elections and the Brexit vote. Personality profiles were used to identify people's viewpoints, opinions and points through which they may be manipulated in a particular direction. It posed concern regarding democratic process manipulation. The scandal led to better regulations and safeguarding norms. One of the results was GDPR (General Data Protection Act) in Europe.

Equifax Data Breach, 2017

The Equifax data breach is one of the biggest data leaks in History, exposing the personal

information of 147 million U.S. citizens, which is 40% of the population. It all started in March 2017, The United States Computer Readiness Team warned about Apache Struts 2 vulnerability and that if the companies don't address it then an attacker may exploit it. Apache Foundation Software released a patch for the vulnerabilities, and Equifax administrators were told to apply the patch to any affected system, the employee who was told to do so didn't do it. Initially, 3 servers were breachers by the attackers, which doesn't seem to harm much. But then, the attackers were able to gain access to multiple servers containing information of hundreds of people. The attackers to remain unnoticed encrypted the data they were moving making it difficult to spot for the administration. It affected approximately 147 Million U.S. citizens and compromised their data such as names, addresses, date of birth, social security number and driving license number. A small subset of records of about 2 lakh people, also included credit card numbers. Who was responsible for the Equifax data breach? The data was not breached to sell on the dark web, rather it was hacked by Chinese state-sponsored hackers whose purpose was to espionage. Similar big breaches were identified: the 2015 U.S. Office of Personal Management and the 2018 hack of Marriott's Starwood hotel brands. All of this was done to gain insight into U.S. government officials and intelligence. In February 2020, the United States Department of Justice charged four members of the Chinese military with the attack. A congressional inquiry was launched into the breach and the CEO of Equifax resigned amid the fallout. Equifax agreed to a $700 million settlement with the Federal Trade Commission and others over the breach. The new regulation was enacted for the consumer to freeze their credit cards for free. A credit freeze, also known as a security freeze restricts access to consumers' credit files, making them hard to access. The Equifax data breach was an alarming wake-up call about the risk we hold while sharing our sensitive information with large credit reporting agencies. It prompted calls for safety regulations for the consumers while entrusting personal information to companies required essentially in our daily lives.

With the above two case studies, we can understand the grave impact data breaches exert and it may range from the apps we use to the credit cards we swipe.

WHAT IS DATA LOCALIZATION

Data localisation is comparatively a more recent concept to protect a country's sovereignty, integrity and security. It essentially means to localize data within a decided boundary. Before understanding data localization and what cross-border transfer of data is, let's first slide to the

very root of the concept. Where is your data stored?

Whenever you surf online, visit a website or accept cookies, you are leaving your digital footprint online. It is a unique set of traceable activities, actions, contributions and communications done on the Internet. This is called Digital Footprints. Digital footprints can be of two types; active digital footprints and passive digital footprints. Active digital footprints are the intentional actions you take online such as posting your photo, commenting on a post or sharing a file. These actions have been done through your will and consent which has your opinion, and interest underneath it. Passive digital footprints are the unintentional actions you take online which are done by you but you didn't mean to leave your mark. Such as just reading a blog that leaves a browsing history, IP address etc. When you share your data with others such as personal information, photos, or files you are leaving your trace online. The data can be accessed, tracked and analyzed. Now whenever you share your data online, where is it stored?

The companies you share your data, depending upon the scale of operation, and level of sensitivity of data, store user-uploaded data in some of the common methods like file storage, databases, content delivery networks and cloud storage. Among all, cloud storage is the most famous, widely used method used in very high-scale operations that need high security. Many companies retain cloud storage services to store their data, like Amazon, Microsoft, Google and IBM, which are the top players in the market. More than half of the world's data is controlled by these four major corporations. After understanding that you leave your trace online, intentionally or unintentionally and that footprint can be well traced and recognized because your data is stored by the companies in the back-end somewhere in the world. But where?

Companies operating in multiple countries globally have huge amounts of data that should be stored, processed and transferred in compliance with law[11]. For years, companies have taken a uniform approach across geographies to manage the data. But, now that countries across the globe are passing various legislations and a plethora of overlapping regulations to control data. This forces companies to think locally rather than globally, it is time-consuming to compile with rules and regulations of each country and sometimes confusing because of overlapping

[11] "Localization of Data Privacy Regulations Creates Competitive Opportunities" *McKinsey & Company* (June 30, 2022) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities> accessed August 18, 2024

legislations. Currently, data localization regulations are in place in 75% of all countries. Significant ramifications arise for an organisation's IT infrastructure, data governance, and data architectures, in addition to their interactions with regional regulatory bodies. Localization regulations are primarily meant to stop cybercrimes, boost local economies and possibly most importantly address growing privacy concerns.

Localization mandates the storage and processing of data in a geographical boundary and imposes restrictions on the cross-border transfer of data. The stringency of data localization may vary from country to country, to balance localization and privacy of data and growth in the IT sector. Data processing means information processing, where meaningful and usable data is filtered out of the collected raw data. It facilitates decision-making and increases the value of information in the end. Whereas, data storage is where the processed data is kept and stored. The localization laws mandate storage of data should be stored in a country from where it has originated before its cross-border transfer or transfer of its replica. Data localization can be further sub-categorised into two categories: absolute data localization and relative data localization. Absolute data localization creates a whole barrier to sharing data outside its jurisdictional limits. For example, Starbucks India cannot share its customer data outside India if absolute data localization is imposed. Whereas relative data localization imposes some pre-conditions, and compliance and defines the data which can be transferred trans-border. For example, Starbucks India to share its customer data outside India has to remove extremely sensitive data and keep original copies of data in India to transfer data cross-border.

The increasing demand for data localization is underscored by mounting global privacy concerns, state-sponsored hacking targeting sensitive information of foreign nations, the need to safeguard against data breaches, bolstered security and sovereignty, protection against data misuse, and the elevation of the value of user consent.

General Data Protection Regulation (GDPR)

GDPR is a landmark legislation by the European Union, a step ahead towards better data privacy laws. In GDPR, a controller or processor of data in a protected area who wants to transfer data has to pass a check of requirement which is known as ‘essentially equivalent’. The receiving country or the data revising data must have essentially equivalent laws. Regarding the same, the Court of Justice of the European Union (CJEU) two important cases

i.e., Schrems I[12] and II[13] come into play. In both cases, CJEU concluded that the US data protection laws which allow indiscriminate and general surveillance were not 'essentially equivalent' to European Union data protection laws.

Schemes I case, The matter involved a challenge to the Irish Data Protection Commission's decision not to investigate a complaint made by Max Schrems. He had requested the Data Protection Commission to halt the transfer of data from Facebook Ireland to Facebook Inc. due to concerns arising from the Snowden disclosures. Mr Schrems feared that his data could be accessed by U.S. intelligence authorities, potentially leading to a violation of his EU data protection rights. At that time, Facebook's legal basis for data transfers was the U.S.-EU Safe Harbor Framework under the EU Data Protection Directive. The Irish High Court subsequently referred the case to the Court of Justice of the European Union, and CJEU invalidated the US-EU Safe Harbour arrangement. The reasoning behind it was that the US-EU Safe Habour arrangement did not provide adequate protection for the sharing of personal data and that the transfer of data to the US is unlawful as it does not equal protection. This case led to a re-evaluation of data protection laws in the US, raised concerns with US surveillance agencies and paved the way for the formation of the EU-US Privacy Shield.

Schremes II, case was subsequent to Schremes I which was brought to challenge the new EU-US Privacy Shield. The CJEU invalidated the EU-US Privacy Shield stating that it does not provide an adequate level of protection. It further stated that the Standard Contractual Clause (SCC) can be used if the data controller, data receipt and data protection authority of the EU member state finds the level of data protection adequate. In the cases, Schremes I and Schremes II pointed out the inadequacy of US data protection laws and high-level surveillance of US authorities. The alternative mechanism for the transfer of data was Chapter V of GDPR, Standard Contractual Clause (SCC) where the exporter of the data has to assess the data protection compliance and rules and regulations of the receiving country.

GDPR was formulated by the European Union for the protection of data and its free movement. The single compiled rules would remove the unnecessary burden for companies to compile with multiple guidelines. According to the general principle of Transfers under Article 44 of GDPR, transfer between protected areas to third countries is prohibited subject to the

[12] Case No. C-362/14, Schrems v. Data Protection Commissioner
[13] Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

conditions laid down in the article. The European Data Protection Board (EDPB) is an independent European body established by GDPR composed of representatives of national data protection authorities of EU countries to ensure consistent data protection application in all European Union countries. In cases where data has to be transferred within EU countries, GDPR does not lay down any additional requirements with respect to GDPR. The relationship between a data processor and the data controller is governed by an agreement that is subject to minimum criteria laid down in Article 28 of GDPR.

The European Data Protection Board in 2021 guidelines of the interplay between the application of Article 3 and the provisions on the international transfers of Chapter V of GDPR lays down three criteria for the transfer of data.

(i) A controller or a processor is subject to the GDPR for the given processing.

(ii) The controller or processor discloses by transmission or otherwise makes personal data, subject to this processing, available to the other controller, joint controller or processor.

(iii) The importer is in a third country or is an international organization, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

In the case of non-EU data transfers, GDPR mentions specific situations when data transfers can be allowed. The European Union based on their adequacy decision can allow the transfer of data, The adequacy decision is based on a thorough assessment of the third country on their data protection levels. The European Commission has so far recognized Andorra, Argentina, Canada, Faroe Island, Guernsey, Israel, the Isle of Man, japan, jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, United States and Uruguay for providing adequate protection. The main aim of the legislation and of the EUPB is that the data transferred is safe and sufficiently protected. Not being recognized in adequacy decision does not close the door for data transfer, one can use any alternative of any of the following:-

1. Standard Contractual Clause:- It is standardized terms and conditions that facilitate the protection of data and appropriate safeguarding measures. As of now, two standard contractual clauses have been issued by the European Commission, one for controllers

and processors within the European Economic Area (EEA) and one for the transfer of personal data to countries outside of the EEA. They are pre-approved by EUPB ensuring compliance with the GDPR.

2. Binding Cooperate Rules (BCRs):- It is used when data has to be transferred from one company to another, irrespective of the territory it can be transferred based on Binding Cooperate Rules. It is useful as the same level of data security is maintained throughout the entities.

3. Derogations for specific situations:- According to Article 49 of GDPR, in the absence of an adequacy decision or any proper safeguards (including Binding cooperate rules), the transfer of data may take place based on the derogations on a case-to-case basis.

The overall purpose of the cross-border transfer of data and GDPR regulations is to protect the data by maintaining "essentially equivalent" protection of data from the transferring country to the receiving country.

INDIAN LEGISLATION

The paper lastly analyses Indian legislation on Data Protection, focusing specifically on data localisation. The very first Indian legislation that focuses on data protection came in 2023, which is the Digital Personal Data Protection Act (DPDP)[14]. Before the implementation of this legislation, the previous draft of the 2019 DPDP was a topic of debate in the country, the 2019 draft presented some strict data localization laws which apparently were deleted in the 2023 legislation. India mainly follows sector-specific data protection and localization laws such as:-

- The Information Technology Act, 2000[15] and the Information Technology (reasonable security practices and procedures and sensitive personal data and information) Rules, 2011[16], Rule 7 talks about the transfer of data where sensitive personal data or information may be transferred across India or any other country that ensures the same level of data protection.

[14] The Digital Personal Data Protection Act 2023
[15] The Information Technology Act 2000
[16] The Information Technology (reasonable security practices and procedures and sensitive personal data and information) rules 2011, 7

- Unified Access license for telecom service providers, 2004[17] mandates local storage and local processing of subscribers' information and prohibits the transfer of information related to the subscriber.

- National Data Sharing and accessibility policy (NDSAP), 2012[18] mandates localization of all information related to government or governmental data, and allows sharing of non-sensitive data or legitimate usage. It is an important policy that ensures the security of the country.

- The Companies Act, 2013[19] requires local storage of books of accounts of companies including the papers stored in electronic mode. Though there may be some exemptions such as a company may keep a part of its register of members outside India if the company's articles authorize the foreign articles according to Article 88(4) of the Companies Act.

- The MeghRaj initiative was launched by the Ministry of Electronics and Information Technology in 2014, it is the national cloud initiative of India which mandates government applications, services and citizen data to be stored in India.

- Reserve Bank of India storage of payment system, 2018-19 requires storage of data locally, which further clarifies that the processing of data may happen outside but the final copy has to be stored within the country.

- The IRDAI (Outsourcing of Activities of Indian Insurers) regulation, 2017[20] mandates local storage of payholders accounts. Moreover, the IRDAI (maintenance of insurance records) regulation, 2015 mandates in rule 3(9) that records including electronic mode about all policies issued and claims made in India shall be held in data centres located and maintained in India.

Apart, from the sector-specific data protection and localization rules, the first legislation that particularly deals with digital personal data protection came out in 2023 as Digital Personal

[17] Unified Access License for Telecom Service Providers 2004
[18] National Data sharing and Accessibilty Policy 2012
[19] The Companies Act 2013
[20] IRDAI (Outsourcing of Activities of Indian Insurers) regulation 2017

Data Protection Act, 2023.

Digital Personal Data Protection Act, 2023

In light of the debate on data localization, the Ministry of Electronics and Information Technology presented the Digital Personal Data Protection Act in 2022 Government on July 31, 2017, formed Justice B.N. Srikrishna's committee to study issues and provide a framework for data protection. The committee submitted the draft personal data protection bill in 2018 and the government sought recommendations on the draft. Chapter VIII of the personal data protection draft dealt with the transfer of personal data outside India. The draft mandated that the data fiduciary should keep at least one copy of the personal data in the data centre located in India, further the central government shall notify categories of personal data as critical personal data which can be processed within India only. Moreover, it provides conditions for the cross-border transfer of personal data where the central government may only permit the transfer of data after ensuring an adequate level of protection. After further deliberations, the bill was approved by the Cabinet Ministry of India on 4 December 2019 and was tabled in Lok Sabha. The 2019 bill was heavily criticized for not aligning with the original draft of 2018. Justice B.N Srirkishna, drafter of the original personal data protection bill himself criticized the revised version as being dangerous and can turn India into an 'Orwellian State'. The bill removed the safeguards which means that the government can access the personal data of anyone in the name of sovereignty and security which may be dangerous, it also gave exemptions from the rule of processing to any government agency that the government may want. The bill was referred to the Joint Parliamentary Committee and after they submitted its report on the bill in 2021, the bill was withdrawn on 3rd August 2021.

The DPDP Act, 2022 reverses the course of action taken in the previously tabled bills, which followed China's approach of restriction in cross-border data transfers and high data localization. The recent DPDP Act, 2022 follows a more free-flowing approach towards data transfer. Let's understand the Key features of the DPDP Act:-

1. The provisions of the act, apart from residents and businesses also apply to non-residents processing digital personal data outside the territory of India, if the data is related to the goods or services to data principle within India.

2. The act allows the processing of personal data of data principle for a lawful purpose,

'lawful purpose' has been explained as a purpose that is not forbidden by law. – Section 4(1) and Section 4(2).

3. Data may only be processed for which the data principle has given consent and for certain legitimate uses. Further, the consent has been defined in Section 6 of the act which says that the consent should be "free, specific, informed, unconditional and unambiguous".

4. The act specifies the processing of personal data for specific usages:-

   (i) Where the data principle has voluntarily provided consent for a specific purpose.

   (ii) For the state to provide a subsidy, benefit, service, certificate, license or permit to the data principle.

   (iii) For protection of sovereignty and integrity and security of the state.

   (iv) For fulfilling any obligation under any law to disclose information to the state.

   (v) For compliance with any judgement, decree or order.

   (vi) For responding to a medical emergency of the data principle or any other person.

   (vii) For taking measures to provide medical services or treatment for public health.

   (viii) For ensuring safety during any disaster or breakdown of public order.

   (ix) For the purpose of employment for safeguarding the employer from loss or liability.

5. The bill establishes rights and duties of the data principle such as getting a summary of personal data that is to be processed, identities of the data fiduciary and processor with whom the data has been shared and any other information related to the personal data. The bill provides the right to data principle for any correction, completion, updating and erasure of the personal data for which the consent was given previously.

6. Chapter IV, special provisions is the only part that deals with the cross-border transfer of data. Section 16(1) of the act states that the central government by notification can

restrict the transfer of personal data to any country. Section 16(2) further gives the green flag to sector-based restrictions, protections and transfers that provide a higher level of security.

7. The act provides for exemptions from the obligation of law for consent and notice requirements in various cases such as processing of data for enforcing a legal right, processing of data for investigation or prosecution of any offence etc.

8. In addition, the act completely exempts processing of personal data:-

   (i) In the interest of sovereignty and integrity of India, security, and maintenance of friendly relations with the foreign states.

   (ii) Data processing for researching, archiving or statistical purposes.

   (iii) The government may exempt data fiduciaries from some provisions.

   (iv) The central government before the expiry of five years from the date of commencement of data may exempt any data fiduciary from the provisions of the act for a specified period of time.

9. The act establishes the Data Protection Board of India, the board is established mainly to oversee inquiries and breaches and to mitigate, resolve and impose penalties in case of data breaches. The board is allowed to impose a monetary penalty of up to 250 crore rupees. And the appeals of the board will go to TDSAT.

10. Lastly, Section 37 of the act allows the central government, upon the reference of the board, may block public access to any information that enables data fiduciaries to carry out activities within the territory of India. The blockage should be based on two criteria:- (a) a monetary penalty has been imposed by the board in two or more instances, and (b) the board has advised for the blockage in the interest of the general public.

ANALYSIS AND WAY FORWARD

Throughout the paper, we have discussed in detail data privacy and the inception of its recognition in India, the need for data privacy which is explained through two famous data breaches, data localization as an important part of privacy, thorough analysis of General data

protection regulation focused on data localization as a part of the international context and lastly Indian sectorial data localization laws and its first flagship digital personal data protection act. Data localization's main purpose is to enhance and improve data protection and privacy, hence it can be called as a part of data privacy. Data localization in India mainly exists in sectorial form which is again supported in the latest DPDP act as mentioned in Section 16(2). The DPDP act, 2023 takes a different turn from its previous draft of 2018 which is provided by strict, specific and broad data localization laws. Though the DPDP Act will now be the basis of ensuring data security in the country, some provisions of the act are still debatable.

The act fails to explicitly classify between personal and critical or sensitive personal data and rather takes a more unified approach which may be the grey area when questioned. Moreover, it also fails to address the right to be forgotten which is recognized in international legislation, precisely in Article 17(2) of GDPR. The act in many ways has gone against the original draft formulated by the Justice B.N. Srikrishna Committee. Section 17(5) of the act is a problematic provision where the government before the expiry of five years from the commencement of the act can exempt any data fiduciary which will not be subject to the provisions of this act. This is a very wide discretionary power given to the government without any pre-conditions or requirements for the application of the provision or for the selection of such data fiduciary. Further, the 2023 act completely reverses the regulatory design of the previous draft which called for the constitution of DPA. The DPA was more or less in line with the GDPR and worked independently from the government with more powers. Whereas, the new act proposes the creation of DPB which has less power than the latter and is not free of governmental intervention.

The missing link still remains in Indian legislation which is lacking behind in framing detailed localization laws when the globe is moving towards the same. Even though India has sector-based localization laws they may not be as sufficient as it looks, sectorial laws may not ensure efficient enforcement, accountability and transparency. Consistency in-laws might be beneficial to better data protection and harmonization. Data localization comes with many benefits and drawbacks, which have to be addressed and solved through deliberations and comparative studies. For now, as the world is moving forward towards detailed data localization laws and adopting different approaches to localization, India needs to fill this missing link to enhance its data protection laws.