Chapter 2

Data Protection Law: Journey Till Now and the Road Ahead

Somesh Tiwari
Managing Partner
Vardharma Chambers
New Delhi, India

Abstract

Technology is the most imperative tool in the 21st century, it is everywhere. It has made humans efficient like never before. The benefits of using technology are abundant but the less talked and the left-out question in this world where technology is so pierced into human life. Is our data safe in the hands of people who are controlling technology? Data privacy and its protection is one of the most important challenges that we face today, yet it is recently that we have started to talk about it. Part I of the present chapter deals with the genesis of privacy as a concept and how Indian judiciary has been the torch bearer on this topic, it also gives a chronological order on how the privacy has evolved in India. As privacy is an imperative matter, The Government of India have come with a legislation called the 'Personal Data Protection Bill, 2019' which tried to encapsulate the major problems that the public at large faces, but the Bill has not yet been passed by the parliament. Part II of the chapter explains this aspect. In this paper, an attempt has

been made to explain the variety of challenges that India is facing into making data protection law a reality. Also, a view has been presented on how other countries apart from India have been tackling this problem, and what the future holds for us in the realm of data protection.

***Keywords*:** Data Protection, Privacy, Genesis, Technology, Judiciary.

I. Introduction

Technology is the most imperative tool in the 21st century. It has made humans efficient like never before, the benefits of using technology are abundant but the less talked and the left-out question in this world where technology is so pierced into human life is – Is our data safe in the hands of people who are controlling technology. In an era of liberalization, privatization and globalization, the role of technology has become indispensable to achieve planned economic goals of the country. However, it is also true that it has become a challenging task to the law enforcement agencies to counter technology driven crimes that are emerging now. Data privacy and its protection is one of the most important challenges that we face today, yet it is recently that we have started to talk about it.

The chapter discusses about the genesis of privacy as a concept and how Indian judiciary has been the torch bearer on this topic, it also gives a chronological order on how the privacy has evolved in India. As privacy is an imperative matter, The Government of India have come with a legislation called the 'Personal Data Protection Bill, 2019' which tried to encapsulate the major problems that the public at large faces, but the Bill has not yet been passed by the parliament. In this chapter an attempt has been made to explain the variety of challenges that India is facing into making data protection law a reality. Also, a view has been presented on how other countries apart from India have been tackling this problem, and what the future holds for us in the realm of data protection.

II. Genesis of the concept of Privacy Concept and Indian Judiciary

The Indian Constitution leaves room for judicial interpretation because the right to privacy was not explicitly mentioned in the constitution, the right to privacy is included in the scope of the fundamental rights according to the legal interpretation of those rights. Although the Indian Constitution does not expressly guarantee the right to privacy, this area of law has developed since it was interpreted in accordance with Article 21.

(i) Role of Indian Judiciary

Indian judiciary, particularly Supreme Court of India has interpreted Article 21 i.e. right to life and personal liberty in a liberal way to include right to privacy within it. For example, the Apex Court in **M. P. Sharma and Others vs Satish Chandra case**[1]considered whether or not the "right to privacy" is a basic right in this case for the first time. It was argued that the search and seizure warrant issued in accordance with Sections 94 and 96(1) of the Code of Criminal Procedure violated the individual's right to privacy. The Hon'ble Supreme Court ruled that no constitutional clause is violated by the ability to search and seize property. According to a report, the state's legal right to search and seize property is mandated by the need to maintain social security. It was claimed in this judgement that the constitution's makers did not specify or foresee the right to privacy as a basic right, analogous to the 4th Amendment in the United States.

Also, in **Kharak Singh v. State of Uttar Pradesh and Ors.**[2] the issue raised was "whether the right to privacy was inclusive of Article 21." The question posed was whether Article 21 of the Indian Constitution was violated by a domiciliary visit for night surveillance against the accused. The Hon'ble Supreme Court ruled that such a visit violated Article 21.

However, the majority of justices believed that because Article 21 does not include any provisions for privacy, the right to privacy cannot be regarded as a fundamental right. Additionally, they claimed that the right to privacy is not a guaranteed right and that such surveillance does not infringe Article 19(1)(d). Therefore, monitoring the suspect's movements does not contravene any basic rights guaranteed by Part III of the constitution. Although Hon. Mr. Justice Subbarao held the minority position that privacy is a crucial component of human liberty.

Recently, the Supreme court in **Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. Case**[3] rendered a landmark decision in this matter, concluding that Articles 14, 19, and 21 of the Indian Constitution guarantees and/or enshrine the right to privacy. The Kharak Singh and M.P. Sharma ruling was overturned by this judgment.

In this case, the "Aadhar Card Scheme" was contested because it was arbitrarily collecting and it was alleged that it was exploiting people' biometric data for other reasons, which violated their right to privacy. The petitioner stated that Article 21 of the Indian Constitution should include the right to privacy because it is a basic right. In response, the respondents argued that the Constitution merely recognises personal liberty and that it has partially granted persons the right to privacy.

The nine-judge Constitutional bench was set up and it decided this case unanimously. It was held by the Hon'ble Supreme Court that the right to privacy is intrinsic of the right to life and personal liberty enshrined under Article 21. It also is a part of rights guaranteed under Part III of the Constitution of India. It was also said that it is an obligatory duty of the State to protect the privacy of its citizens. Hence, the 'Aadhaar Card Scheme' was held liable for violating the right to privacy of the citizens.

This decision of the Supreme Court empowers the citizens to seek judicial relief in case their data privacy rights are breached. Also, this judgment

affects the rules and regulations set by tech companies in India. The Supreme Court in its Puttaswamy judgment, 2017 declared privacy a fundamental right. This set the government in motion to take steps to bring a new data protection legislation for the country. The report has emphasized that interests of the citizens and the responsibilities of the state have to be protected, but not at the cost of trade and industry. The Committee was constituted by the union government in July 2017, to deliberate on a data protection framework. The Committee has also proposed a draft Personal Data Protection Bill[4].

III. Journey so Far: The Proposed Legislation on Data Protection in India

The absence of data protection law in India has posed several challenges relating how to protect privacy of the individual on the one hand and interest of the data processor on the other hand. Before enacting a comprehensive law on protection of personal data, the government took following initiatives.

(i) B.N. Srikrishna Report

The report of BN. Srikrishna ensured extensive deliberation on a data protection framework in India. This committee was constituted by Government of India in July 2017 and headed by retired Supreme Court judge BN. Srikrishna. This was a significant step in the direction of framework an important and required law on data protection.

(ii) Provisions of Data Protection Bill

Following are the significant provisions of the Data Protection Bill -

a. Individual Consent:[5]

The proposed Bill significances individual's consent as the cornerstone of data sharing, grants users' rights, and places duties on data fiduciaries

(all those entities, including the State, which determine purpose and means of data processing).

The legal basis for processing personal data shall be consent. Although the law will use a different framework for consent, the data fiduciary will still be responsible for any harm done to the data principal.

The Data Protection Bill specifies terminology like data principal, data processor, data breach and sensitive data, etc. and asks for privacy by design on the part of data processors.

b. Data Protection Authority[6]

A Data Protection Authority (DPA), an independent regulatory organisation tasked with the effective execution of the legislation, would be established as a result of the data protection law.

The key responsibilities of the DPA are as follows: legal matters, policymaking, and standard setting, monitoring and enforcement, research and awareness inquiry, grievance handling and adjudication.

c. Personal data[7]

The law will apply to both public and private organizations handling personal data. If personal data has been used, shared, revealed, gathered, or otherwise processed in India, the law will have jurisdiction over such processing. The Bill has provisions relating to handling of personal data. The Bill covers several categories of information within the purview of sensitive personal data such as Passwords, financial information, health information, official identifiers, sex life, sexual orientation, biometric and genetic information, and information revealing a person's caste, tribe, religion, or political affiliations. The DPA will, however, be given the residuary authority to notify additional categories in compliance with the standards established by law.

Additionally, personal data collected, used, shared, disclosed, or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals do not present in India.

d. Right to be forgotten[8]

The right to be forgotten refers to a person's capacity to restrict, delink, erase, or rectify the exposure of inaccurate, humiliating, irrelevant, or out-of-date personal information online.

e. Cross border data transfer[9]

Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee.

Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data).

f. Data of minors[10]

The Committee has made specific reference to the need for distinct and stricter standards for safeguarding children's data, and it has recommended that businesses be prohibited from processing data in ways like behavioral tracking, targeted advertising, and any other processing that is not in the child's best interest.

The fact that youngsters are unable to completely comprehend the repercussions of their behavior provides the foundation for such discriminatory treatment. In the digital era, where data collection

and processing are usually opaque and bogged down in complicated consent forms, this is only made worse.

The committee suggests giving the Data Protection Authority the authority to identify websites or online services that process a significant number of children's personal data as guardian data fiduciaries.

The committee noted that this approach, of placing the onus of properly processing the data of a child on the company, is preferable to the existing regulatory approach which is based solely on a system of parental consent.

The parental concern is prone to circumvention. It risks encouraging children to lie about their age, without achieving the intended purpose of protection.

g. Exceptions[11]

In cases of public welfare, law and order, emergencies when the person cannot provide consent, employment, and justifiable purposes, the state may handle data without the user's consent. Some requirements of the proposed data privacy law may not apply to the processing of data for particular purposes, such as the security of the State, judicial processes, research, and journalistic purposes. To prevent potential abuse, the law must, however, include sufficient security measures.

h. Data Storage[12]

The Bill includes provisions requiring a copy of personal data to be kept on file in India. The current world of commerce and trade depends on cross-border data flows. Investments and transactions (like outsourcing) might be hampered by restrictions or uncertainties on these flows (in data businesses). India must strike a balance between its demand for

commercial facilitation and its desire to maintain its sovereignty as a global hub for both.

i. Appellate Tribunal[13]

To hear and decide any appeals against a DPA order, the Central Government must either create an appellate tribunal or give authority to an existing tribunal.

j. Penalties[14]

Infractions of the data protection legislation may result in penalties. If the amount of the fine exceeds the maximum limit that has been set, it will be increased by a percentage of the previous financial year's total worldwide turnover. It is worthy to mention here that the above stated committee has suggested a penalty of Rs. 15 crore or 4% of the total worldwide turnover of any data collection/processing entity, for violating provisions. Failure to take prompt action on a data security breach can attract up to Rs. 5 crore or 2% of turnover as a penalty. Further, the penalties paid by violating entities in this case will be deposited to a Data Protection Fund, which will, among other purposes, finance the functioning of the Data Protection Authority.

k. Impact on Allied laws[15]

The committee has observed that the Aadhaar Act is silent on the authority of the Unique Identification Authority of India (UIDAI) to impose sanctions against violating businesses operating within its ecosystem. To strengthen data protection, the Aadhaar Act has to be changed. The Report also suggests changes to the RTI Act, citing the possibility of private harm from the release of public authorities' information.

l. Obligations on Fiduciaries and rights to principles are the two underlying themes of the Bill[16]

The obligations would include "purpose limitation," which states that data will only be used for explicit, legal purposes, and "collection limitation," which states that only the data required for the purpose will be collected and will only be kept for as long as it is reasonably required for the purpose.

A data protection impact assessment is started before new technologies are implemented, data policies are verified by a data auditor, and they have data protection officers. The Bill lays out requirements for fiduciaries to guarantee no harm to the user, with transparency and security protections. The Act would apply to data processors who are not physically present in India as well as those who conduct business there or engage in other activities like profiling that might endanger the privacy of data principals in India.

IV. Personal Data Protection Bill, 2019

The PDP Bill proposes a significant shift in India's data collection and processing procedures. So far, both the private sector and the government have functioned in a largely uncontrolled environment, free of checks and balances and processes to protect citizens' privacy interests. according to Section 3(28) of the PDP Bill means "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling. The key notion behind deciding what personal data is the identifiability of a natural person.

(i) Features of the Bill

The PDP Bill aims to strengthen data processing and privacy in a manner similar to the GDPR of the European Union.[17] The PDP Bill proposes the establishment of a Data Protection Authority (DPA)[18], similar to those found among European Union countries, and specifies the types of sensitive personal data that must be protected. The PDP Bill establishes the term "data fiduciary" and imposes specific requirements on them about how they collect, deal with/process, and retain personal data. It holds them responsible for upholding their commitments in relation to personal data processing performed by them or on their behalf.

If the PDP Bill becomes law, businesses will be required to inform customers about their data gathering activities and obtain their consent. They would have to gather and store proof that such notice was given, and approval was given. As a result of the PDP Bill giving customers the ability to withdraw their consent, firms would have to devise ways to allow consumers to do so. After their data has been processed for the purpose for which it was intended, consumers have the right to access, correct, and erase it under the PDP Bill. As a result, businesses would have to devise means for customers to do so.

The PDP Bill allows consumers to transmit their data to other firms, including any inferences formed by businesses based on that data. All businesses would have to devise mechanisms to enable customers to do so. The PDP Bill mandates that all firms adopt organizational changes to better secure data. This includes privacy-by-design principles (a business model in which privacy is a primary issue), security precautions, and so on. The PDP Bill mandates data localization, mandating companies to keep specific types of data on Indian servers solely. In this way, it establishes the following three-tiered structure:[19]

(ii) Major Provisions of the Bill

The major provisions of the Bill are as follows -

a. **Personal data**: Personal data that is not designated "sensitive" or "critical" is not subject to localization or data transfer limitations. No transfer limitations would apply if this type of personal data was stored wholly outside of India.
b. **Sensitive personal data**: "sensitive personal data" may be sent outside of India, but it must still be stored there. "Special categories of personal data" include health, religion, sex life, political convictions, biometric, genetic, and financial information, among other things. Passwords, for example, have been eliminated from the definition.
c. **Critical Personal Data:** The Bill allows the government to designate some types of personal data as "critical personal data" that cannot be transferred outside of India. The Bill, however, allows transfers to nations or organizations that are assessed to provide a sufficient level of protection (and will not jeopardize the State's security or strategic interests).
d. **Miscellaneous Provisions of the Bill:** The PDP Bill establishes a right to be forgotten, allowing a data principal to limit or prevent the continued disclosure of his personal data by a data fiduciary where such disclosure has served the purpose for which it was collected or is no longer necessary for that purpose; was made with the data principal's consent and such consent has since been withdrawn; or was made in violation of the provisions of this Act or any other law in force at the time.

The PDP Bill mandates that data fiduciaries notify the DPA of any breach of personal data they process if the breach is likely to cause harm to any data principal. "Significant data fiduciaries" will have additional

responsibilities under the Bill, such as conducting data audits and hiring data protection officers. The Bill allows the Central Government to declare any social media intermediary (such as Facebook) with subscribers over a certain threshold as a significant data fiduciary:

The PDP Bill offers the Central Government vast powers to exempt any government agency from the Act's application. The government can access any anonymized or non-personal data from data fiduciaries and processors under Section 91[20] of the PDP Bill. The PDP Bill gives the DPA the authority to punish any business that does not follow the Bill or the DPA's or the Government's rules. The maximum penalty that can be levied is 150 million Indian rupees (about $2.1 million), or 4% of the company's global turnover in the previous financial year.[21]

V. Joint Parliamentary Committee's Report and Suggestions on 2019, Bill

There are certain shortcomings with this proposed Bill of 2019 which were highlighted by the report released by the Joint Parliamentary Committee[22]. The proposed suggestions are as follows:

(i) Difficulties in discerning Personal and Non-personal data

It is difficult to discern between personal and non-personal data, according to the JPC, because the Data Protection Authority (DPA) will manage various types of data at various security levels. According to the committee, the PDP Bill should cover both categories of data until a separate framework to distinguish between personal and non-personal data is implemented.

The report stated, "*As soon as the provisions to regulate non-personal data are finalised, there may be a separate regulation on non-personal data in the Data Protection Act to be regulated by the Data Protection Authority*,"[23]

(ii) A mirror copy of sensitive and critical data should be localized

The JPC recommends that, in addition to the provisions under Clauses 33 and 34 for cross- border data transfer, the government take concrete steps to ensure that a mirror copy of sensitive and critical personal data already in the possession of foreign entities be brought to India in a timely manner[24].

(iii) Data Localization

The central government has been given orders to take precautions and secure sensitive data held by foreign firms. According to the JPC, a copy of such data must be brought to India in a timely way. The central government has also been required to verify that all local and foreign entities meet the new data localization laws. In the coming days, the government has been requested to create and issue a complete data localization strategy.[25] The report suggest the following for data localization.

(iv) Data Localization Norms

"Normally, the imposition of data localization norms can be attributed to mitigation of certain risks in cross-border flow of data and address strategic objectives. These include:

a. **National security and law enforcement**: In a hostile country, the data can be a tool for surveillance and manipulation of consumer behavior/opinion. Timely access to personal information by law enforcement agencies is also one major requirement.
b. **Privacy**: Better informational privacy can be ensured with appropriate data protection regulations within the country.
c. **Employment generation**: Data localization can provide a great boost to the data economy in the domestic market with the

emergence of the data centers and other associated industries, which have the potential to create significant employment opportunities.

d. Bargaining power: With strong presence on the internet and mammoth generation of consumer data, India can be in better position to bargain with other countries for encouraging data-based innovation for providing digital services and impetus to the digital economy."

(v) Data Breaches

Clause 25(3) should include a 72-hour reporting timeframe for data breaches, according to the committee. The committee requested that the DPA follow particular guiding principles while creating data breach legislation. It has been suggested that the authorities ensure the privacy of the data principals. The data fiduciary will bear the burden of proving that the delay was reasonable if the data principle has experienced inconsequential or material harm as a result of delayed reporting, according to the study.

The data fiduciary is liable for any harm caused to the data principal as a result of a late complaint. According to the study, fiduciaries would also be required to keep track of all data breaches. A data fiduciary must not keep personal data for longer than is necessary and must erase it once processing is completed. Because the government will also become a data fiduciary, the report suggests that in the event of a breach or a crime, the head of the department in question conduct an internal inquiry first. This procedure is designed to ascertain who was responsible for the specific crime, after which liability can be determined.

(vi) Social Media and Intermediary Liability

With the revelations of the Facebook Files, social media platforms have become a prominent focus of discussion in technology policy. The JPC

Report has been impacted by this, with various new insertions in the Draft Data Protection Bill, 2021. To begin, we'd like to emphasize that, while data protection laws are crucial tools for regulating data flows to giant digital platforms, they are distinct from broader social media regulation, which requires its own statute (e.g., the UK's Online Harms Whitepaper). "Social media platforms have been designated as intermediaries in the IT Act, and the Act has not been able to regulate social media platforms adequately," according to the JPC Report and that "the current Bill is about personal data protection, and social media regulation is an entirely different aspect that requires detailed deliberation". Despite these observations, the report goes on to suggest major changes to social media regulation.

The JPC Report has identified and remarked on a number of issues with social media, including "the predominance of fraudulent accounts" and "instigated individuals all over the world to plan, organize, and carry out revolutions, protests, riots, and spread violence." The JPC Report suggests the following modifications in response to these concerns:

Publishers: The Committee's main worry was that the IT Act had labeled social media sites as 'intermediaries'. In this regard, the Committee believes that social media platforms should not be identified as such because, in essence, they act as content producers, with the capacity to choose who receives the content and control access to any content placed on their platform.

Verification: A method might be established whereby social media platforms that do not function as intermediaries are held liable for content posted by unverified accounts on their networks. The social media intermediary must verify the account once application for verification is submitted with all required papers.

Local office: "Moreover, the Committee also recommends that no social media platform should be allowed to function in India unless the technology's parent business has an office there.

Social Media Regulatory Body: "Further, the Committee recommend[s] (sic) that a statutory media regulatory authority, on the lines of Press Council of India, may be setup for the regulation of the contents on all such media platforms irrespective of the platform where their content is published, whether online, print or otherwise."[26]

VI. Miscellaneous Legislations relating to Data Privacy

Information Technology Act, 2000 and the relevant amendments empowers individuals to sue a company for damages caused by its failure to develop and maintain "reasonable security measures and procedures" to protect sensitive personal data or information under Section 43- A, (IT Act, 2000). The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Act Rules) define sensitive personal data or information as personal information relating to: "Passwords, Financial information, such as bank account or credit card details or other payment details, Physical, physiological, and mental health condition, Sexual orientation, Medical records and history and Biometric information." [27]

Section 43-A provides compensation in the event that a body corporate that owns, controls, or operates a computer resource and possesses, deals, or handles any sensitive personal data or information is negligent in implementing and maintaining reasonable security practices and procedures, resulting in wrongful loss or gain to any person. Non-digital data is not mentioned in this section. Data saved on any electronic

device or in a relevant file system (such as a salesperson's diary) should be covered by data protection legislation.[28]

Data kept on non-electronic media is not protected by this provision. Furthermore, while the part mentions sensitive personal information, it does not compare it to personal information, which is on a whole different level. In essence, there appears to be no distinction between what is traditionally deemed personal information and sensitive personal information under this clause.[29]

Information disclosed in violation of a legitimate contract is punishable under Section 72-A. Anyone who acquires access to any material containing personal information while providing services under a legitimate contract and reveals that material to anyone else without consent or in violation of the contract will be penalised. The problem with this clause is that it lacks a definition of personal information, which, when combined with the provisions of Section 43- A, which refer to personal sensitive information, causes some inherent ambiguity between different sections of the IT Act. While the clause makes it illegal to break a person's confidentiality, it does not provide any compensation to the victims of such a breach. That is arguably the most essential solution in the context of violation of privacy. The section is very specific in that it only applies to personal information gathered within the terms of a service contract. Personal information can be gained in a variety of ways, and all such personal information must be protected.[30]

While these improvements give some protection against privacy intrusions, they are by no means comprehensive. It is critical to clarify terminology such as "personal information" and "sensitive personal information." In terms of collection, use, and disclosure, sensitive personal information must be handled with greater caution. It's also critical to make sure that data saved on non-electronic media is covered

and secured. More crucially, while the new provisions in the IT Act 2008 offer a foundation for data protection in the country where none previously existed, a full-fledged data protection legislation must contain regulations on data collection, control, use, and destruction. To have an effective data protection regime in India, several fundamental aspects must be addressed.

VII. Changes Incorporated into Draft Data Protection Bill, 2021

Following suggestions have been offered by the JPC:

(i) Incorporation of Non-Personal Data[31]

One of the most significant revisions recommended by the JPC was to expand the Bill's scope to cover all types of non-personal data, as per Clause 3(28), which states that it includes "data other than personal data." The committee advised this because, in their opinion, it is highly challenging to discern between personal and non-personal data, which might even impact privacy. Additionally, a separate statute will need to be introduced in order to govern non-personal data if it is not included by the data protection Bill.

(ii) Social media terminology change

The word "social media intermediaries" has been changed in the Draft Bill, 2021 to "social media platforms," which is defined under clause 3(44) of the Draft Data Protection Bill, 2021, as any platform that aims to facilitate online interaction between various users. This change was made to make these platforms accountable for any content they host.

However, including these social media companies within the ambit of "platforms" will still not provide a viable solution to the issue of data privacy. Classifying these social media platforms strictly as

an "intermediary" or strictly as a "platform" will not be as effective because a middle ground has to be found wherein as per the varying circumstances, these companies can be legally exempted or be held liable for the content posted by their users.

(iii) Defining 'damage'

The JPC report also discusses the issue pertaining to the breach of data and its disclosure and reporting mechanisms. It puts forth a number of rules, one of which specifies a time limit of 72 hours for reporting a violation. In accordance with this, organizations will also need to properly justify any delays in disclosing security breaches. The Data Protection Authority (DPA) only required to be notified by the data fiduciaries in the event that any "damage" was caused, according to the 2019 Bill. The most recent iteration of this definition of "damage" has been updated to include psychological manipulation in addition to the loss of reputation or any type of financial loss. Additionally, this proposal suggests making it essential to notify all data breaches, whether or not any harm was done.

(iv) Obtaining consent:

The express consent requirement and giving consumers the choice of supplying or not disclosing their personal data were two more changes included in the proposed Legislation. According to the JPC committee's suggestion, the individual will be permitted to exercise their right to privacy even if they opt not to divulge their personal information. However, as all rights are subject to a few reasonable limitations, efforts have been made to define the conditions that permit the non-consensual processing of personal data. Non-consensual use is permitted where" such processing is required," according to an earlier version of the 2019 Bill that deals with data protection. However, the 2021 draft of the Bill

fails to incorporate the procedural safeguards provided in the landmark judgment of **Justice K.S. Puttaswamy v. Union of India (2017)**[32] which requires the presence of "proportionality" and "legitimate purpose". The 2021 Draft Bill provides that non-consensual usage can be allowed whenever it "can be reasonably expected" thereby failing to incorporate the procedural safeguards laid down in the aforementioned case.

(v) Storing of data within the boundaries of the country

The JPC report recognised the significance of data localization and asserted that all sensitive information pertaining to national security, personal information, economic activity, etc. must be kept inside the boundaries of the country. The committee even made recommendations for the actions that should be performed to transfer all of the sensitive data that has been held abroad and bring it back within the country's boundaries. However, there have been some discrepancies over the legal bases for the transmission of this data. In the 2019 draft of the Bill, it was provided that the transfer of sensitive data can be restricted if it is against the public or the state policy. But there is no information available as to what all can be included within the definition of public and state policy, and this could lead to the arbitrary use of powers that have been assigned to the DPA.

(vi) Mandatory appointment of the data protection officer

The JPC changed the draft and mandated the appointment of a Data Protection Officer for all notable data fiduciaries. The committee said that the role of a data protection officer should only be filled by someone who has a senior or significant managerial position inside the organisation. This is done to make sure that whoever is chosen to serve as the DPO is familiar with how the business operates.

(vii) Hardware and software testing and certification

The Committee also took into account the consequences of data breaches brought on by the technology and software used for data gathering and storage. It opined that certain basic minimum criteria need to be set that need to be fulfilled before the approval is granted for the hardware or the software. The JPC advised that the DPA create a framework for monitoring and make sure that frequent testing is done to maintain the data secure.

VIII. Roadblocks and Challenges

There exists a number of challenges regarding data protection in India:

(i) Question of government controlling and accessing public data

While some national security issues may need the state's access to and maintenance of public data records, it is critical that the Bill does not place citizens' right to privacy ahead of the country's security interests. The government will have the power to gather and exploit public data as it sees fit, thanks to an intentional elevation of national security over the right to privacy.

(ii) Effective restraints on large corporations

In 2018, the Central Bureau of Investigation filed a case against the British data analytics firm Cambridge Analytica for allegedly obtaining and exploiting the personal data of 6.1 million Indian Facebook users[33]. The business allegedly utilised the information to sway Indian elections. As a result, imposing effective limits on huge firms' data mining tactics should be a major legislative priority.

(iii) The importance of people's right to privacy

Any data privacy and protection law must be based on the Supreme Court's 2017 decision on the right to privacy. In August 2017, a nine-

judge Constitution Bench of India's Supreme Court declared that the right to privacy is "intrinsic to life and liberty" and hence fundamentally guaranteed by the Indian Constitution's many fundamental freedoms. The government must strike a compromise between the protection of personal data and the nation's national security concerns.

(iv) Cyber-attacks and surveillance prevention

According to government data presented in Parliament, India reported 1.16 million cyber security cases in 2020, which is three times more than in 2019. Several nations have recently been accused of using Pegasus spyware[34] for spying purposes. It is unknown whether the spyware was deployed by the Centre or if it was employed by a third party in India. Data security and privacy issues posed by current surveillance technology must be considered in the Bill.

(v) Data leaks

The past few years have also been victims of several major data leaks. In 2020, IRCTC's data leak revealed the personal information of millions of Indian citizens on the dark web. The information included their full names, mobile numbers, e-mail IDs, dates of birth, marital statuses, and cities of residence. Similarly, the data of 45 lakh passengers was leaked on Air India's passenger system service provider SITA, including information about the passport and credit card details. Outlook India reported data localization issues, given SITA is based out of Geneva, an aspect PDP Bill would raise. An 8.2 TB data leak also revealed such sensitive information at Mobi Kwik, with the KYC documents, Aadhar card and passport details of 10 Crore people on sale on the dark web. In an even worse turn, Domino's India's data leak led to the information being on the surface web, accessible to anyone with a search engine.[35]

IX. Global Legislations Relating to Data Privacy

This Part shall specifically deal with legislations at the global level:

(i) U. S. Fourth Amendment

Stated in the U.S Constitution, the Fourth Amendment provides that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The secretary of State Thomas Jefferson on 1st March 1792 declared this Fourth Amendment.

The focal aim of this provision is to guarantee people's right to privacy and secure them from unreasonable interference by the State. Not all search and seizures are protected by the law but only those which are initiated by the government or an unwarranted search.

With a few exceptions, a search or seizure without a warrant is generally unjustified and illegal. A law enforcement official must show probable cause that a search or seizure is warranted in order to obtain a search warrant or an arrest warrant. The totality of circumstances will be considered by a court-authority, generally a magistrate, in deciding whether or not to issue the warrant.

If an officer has probable cause and obtaining a warrant would be impractical in the given context, the warrant requirement may be waived. For example, an Ohio court concluded in *State v. Helmbright*[36], that a warrantless search of a probationer's person or residence is not a violation of the Fourth Amendment provided the officer conducting the search has "reasonable reasons." to believe that the probationer has failed to comply with the terms of his probation.

The Fourth Amendment's applicability in electronic searches and seizures[37] has gotten a lot of attention in recent years from the courts. With the rise in use of computers and the internet, there has been an increase in the quantity of crime committed electronically. As a result, computers, hard drives, and other electronic devices are frequently used to store evidence of such crimes. Electronic devices are subject to search and seizure under the Fourth Amendment.

In many electronic search situations, the question is whether law enforcement can search a company-owned computer that an employee uses for work. Despite the fact that the law is split, the majority of cases rule that employees do not have a genuine expectation of privacy when it comes to information saved on company-owned computers. The Supreme Court expanded this lack of expectation of privacy to text messages sent and received on an employer-owned pager in the 2010 decision of *City of Ontario v. Quan*[38].

(ii) European Union- General Data Protection Regulation[39]

The General Data Protection Regulation (GDPR) is the world's most stringent privacy and security law. Despite the fact that it was designed and passed by the European Union (EU), it imposes duties on organizations anywhere that target or collect data about EU citizens. On May 25, 2018, the regulation went into effect. Those who break the GDPR's privacy and security regulations will face severe fines, with penalties ranging in the tens of millions of euros.

The GDPR signals Europe's hard stance on data privacy and security at a time when more individuals are committing their personal data to cloud services and data breaches are becoming more common. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium- sized enterprises (SMEs).

"Everyone has the right to respect for his private and family life, his home, and his communications," says the European Convention on Human Rights, which was adopted in 1950. The European Union has worked to assure the protection of this right by legislation based on this foundation.

The EU recognized the necessity for updated protections as technology advanced and the Internet was developed. As a result, in 1995, it passed the European Data Protection Directive, which established minimum data privacy and security criteria on which each member state's implementing legislation was based. However, the Internet was already transforming into the data Hoover it is today. The first banner ad emerged on the internet in 1994. The majority of financial institutions offered online banking in the year 2000. A Google customer filed a lawsuit in 2011 after the corporation scanned her emails. Two months later, the European Commission's data protection authority determined that the EU required "a comprehensive approach to personal data protection," and work on updating the 1995 directive started.

After passing via the European Parliament in 2016, the GDPR became effective in 2016, and all enterprises were obliged to comply by May 25, 2018.

X. Data protection principles

The main Data Protection Principles are summarized -

(i) Transparency, fairness, and lawfulness – Processing must be legal, fair, and transparent to the data subject.

(ii) Purpose limitation: Data processing shall be limited to the legitimate purposes notified to the data subject when the data was obtained.

(iii) Minimize data collection and processing – Only gather and process as much data as is absolutely necessary for the objectives stated.

(iv) Accuracy — Personal data must be accurate and up to date.

(v) Limitation on storage – You may only keep personally identifying information for as long as it is required for the intended purpose.

(vi) Integrity and secrecy – Processing must be carried out with the utmost security, integrity, and confidentiality (e.g., by using encryption).

(vii) Accountability — It is the responsibility of the data controller to show GDPR compliance with all of these criteria.

XI. Conclusions and Road Ahead

The changing digital world has forever changed how personal data is acquired, kept, and used for a variety of purposes, both known and unknown. Personal data protection is more voluntary than required in the absence of organized and comprehensive data privacy regulations. With the introduction of the Data Protection Bill and its several versions, India has adopted a careful approach to establishing itself as a "nation intent on constructing a solid data privacy framework" that will help enhance global trust and make India a desirable investment destination.

The Bill intends to promote fair and transparent personal data processing through informed permission, making ethical data usage a key component of data management. Furthermore, with the passage of the Bill, there is an urgent need to educate the next generation of India's digital users from all walks of life on their privacy rights and the redressal mechanisms that companies are required to implement. This growing knowledge will be crucial in promoting trust and openness among the general public.

On the one hand, the demand for data localization would increase compliance costs by compelling multinational firms to establish up personal data duplicates in India. On the other hand, it will progress technology and provide future investment and job prospects, transforming India into a real data sovereign nation.

In light of the Bill, we anticipate the development of a number of regulatory policies, including a framework for non-personal data, data-localization, and certification for digital and IoT (Internet of things) devices, all of which emphasize the need for a flexible data privacy framework to meet future requirements in their overarching data privacy programmes.

Endnotes

1 AIR 1954 SC 300.
2 AIR 1963 SC 1295.
3 AIR 2017 SC 4161
4 The Personal Data Protection Bill, 2019(Bill No. 373 of 2019)
5 Justice B.N. SriKrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, page no. 24, (2018), Ministry of Electronics & Information Technology, Government of India.
6 *Id* at page no. 151
7 *Id* at page no.170
8 *Id* at page no.68
9 *Id* at page no.82
10 *Id* at page no. 42
11 *Id* at page no.120
12 *Id* at page no. 83
13 *Id* at page no.159
14 *Id* at page no. 163
15 *Id* at page no. 98
16 *Id* at page no.146

17 General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the on-data protection and privacy in the European Union and the European Economic Area.

18 The Personal Data Protection Bill, 2019(Bill No. 373 of 2019), s. 41(1)

19 The Personal Data Protection Bill, 2019(Bill No. 373 of 2019), s.3

20 Section 91 of the PDP, Bill 2019: 91. "Act to promote framing of policies for digital economy, etc.", available at:http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

21 The Personal Data Protection Bill, 2019(Bill No. 373 of 2019), s.57 (2) (d)

22 Report of the Joint Committee on the Personal Data Protection Bill, 2019, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf'

23 Mohit Sharma, "Joint committee report on Data Protection Bill tabled in both Houses of Parliament | Details", available at: https://www.indiatoday.in/india/story/joint-committee-report-data-protection-Bill-tabled-houses-parliament- details-1888747-2021-12-17

24 Gulshan Rai, "Personal Data Protection Bill, 2019 - Key Highlights Of Reports Of Joint Parliament Committee (JPC)", available at:https://www.mondaq.com/india/privacy-protection/1161678/personal-data-protection-Bill-2019--key-highlights-of-reports-of-joint-parliament-committee-jpc#:~:text=Salient%20features%20of%20the%20%22Bill,on%2011th%20Dec%2C%202019&text=The%20proposed%20legal%20framework%20would,Non%20Personal%20Data%20(NPD)

25 Supra Note 8

26 Key Takeaways: The JPC Report and the Data Protection Bill, 2021 #SaveOurPrivacy, available at: https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-Bill-2021-saveourprivacy-2/

27 Supratim Chakraborty, Privacy in India: Overview, available at: https://www.khaitanco.com/sites/default/files/202101/Privacy%20in%20India%20Overview.pdf

28 Approach Paper for legislation of Privacy, available at: https://documents.doptcirculars.nic.in/D2/D02rti/aproach_paper.pdf

29 Id.

30 Id.

31 Siddarth raj choudhary," Data Protection Bill, 2021 & The Joint Parliamentary Committee Report: Key Changes, Mondaq, 25th January, 2022, available at https://www.mondaq.com/india/privacy-protection/1153588/data-protection-Bill-2021-the-joint-parliamentary-committee-report-key-changes .

32 Supra note 3.

33 Personal details of 6.1 million Facebook users in India leaked online, The Economic times, 06th April, 2021,available at https://economictimes.indiatimes.com/tech/technology/personal-details-of-6-1-million-facebook-users-in-india-leaked-online/articleshow/81916959.cms

34 David pegg and Sam cutler," What is Pegasus spyware and how does it hack phones?", The Guardian, July 18th2021, available at https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does- it-hack-phones.

35 Priyam Shukla," The state of data privacy in India amid hanging data protection Bill" The Outlook, 28th October, 2021 available at https://www.outlookindia.com/website/story/india-news-the-state-of-data-privacy-in- india/390849

36 State v. Helmbright (Judgement) (2003), United States Court of Appeals (Ohio).

37 Jonathan Kim, Fourth Amendment, Legal Information Institute (2022).

38 City of Ontario v. Quon(Judgement) (2010), Supreme court of the United States.

39 European parliament and of the council, General data protection regulation (GDPR), Regulation 2016/679 (April 27, 2016).