Page 166 - 186 **DOI:** *https://doij.org/10.10000/IJLMH.113781*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 6

2022

Data Privacy: The Way Forward

FAHAM AHMED KHAN[1]

ABSTRACT

There has been rapid technological advancement in the 21st century. The advent of technologies like the internet, smartphones, artificial intelligence and mobile applications have enhanced the standard of living and reduced the distances between people. A lot of the new technologies require that the users input their personal data in order for them to function smoothly. The data requirements often mandate that the user needs to share certain sensitive and personal information which if misused can cause great harm to the user. The developers of the technologies are at an advantage since they can force the users to forcefully agree to the sharing of data in order to properly access their technology. This has raised serious concerns about the privacy of the data of the users and their safety. Therefore, the development of an effective legal and regulatory framework needs to ensure that the development of new technology does not compromise the data privacy of the general population and make them vulnerable to the leakage of their data. The European Union introduced the GDPR, which is said to be a watershed moment for Data Privacy and more accountability for corporations. The paper analyses the regime for data privacy prevailing in different Jurisdictions across the world. It also seeks to provide suggestions as to how the regime can be further strengthened so that the users do not have to face adverse consequences for using modern technology.

Keywords: *Data Privacy, Data Protection, Data Regulation, GDPR, PIPL, Right to Privacy.*

I. INTRODUCTION

(A) Data Protection and Data Privacy

With the advent of technological advancement and extensive development and use of artificial intelligence in almost all fields of our lives, the question of data privacy has become more pertinent than ever. The postulation of the term "data privacy" has always been confused with "data protection".[2] In a true sense, both these concepts have different meanings and scopes. "Data Privacy" can be understood based on information related to "private life". However, all the information related to "private life" does not come under the scope of data privacy. Data

[1] Author is a Candidate of Master of Law at University of Cambridge, Cambridge, U.K.

[2] Cindy NG, *Data Privacy: Definition, Explanation and Guide,* VARONIS (Apr. 18, 2019), https://www.varonis.com/blog/data-privacy/.

 [ISSN 2581-5369]

Privacy covers the information which is of a past event and obtained systematically, i.e. with authorisation and consent.[3] Some of the common information included under the ambit of data privacy are credit card numbers, birth dates, government identification cards, bank account details, medical history and more. Data privacy primarily identifies the sensitivity of the data and the onus is upon the organization to ensure that the data is only accessed by authorized personnel who will not misuse the information.

On the other hand, "data protection" covers all the breaches of information, including the rights to privacy and private life.[4] It is a reference to the mechanisms and strategies which are applied to ensure that the integrity and privacy of data are protected. It seeks to protect private information from unauthorized access. It prevents data theft and mitigates the harm in case there is an attempted data breach. Data privacy seeks to ensure only authorized access while data protection prevents any kind of unauthorized access and has a larger scope.

(B) Data Privacy Legislation in Modern Times

In recent times, with the right to privacy gaining importance all around the globe, data privacy laws have started being integrated into all legal systems. It will not be a long shot to say that given the importance of data in today's era, data privacy has become one of the yardsticks to judge the democratic efficacy and effectiveness of the governance of a nation.

Even though data privacy/right of privacy is an essential part of every legal system, has been dealt with in different limbs of right in different countries, which makes it a relatable right rather than a non-derogable one.

Using this disquisition, the conundrum of this right in respect of different nations, considering the developmental and economic base of the various nations is tried being analytically dealt with. Further, a comparative analysis is drawn between laws existing in countries like the US, India, European Union – these countries in particular because of their developmental scale and timeline along with the level of technological advancement. Concluding the disquisition, specific steps and measures are recommended suitable to improve the position of data privacy laws in India.

---

[3] *Rotaru v. Romania*, App no 28341/95, ECHR 2000-V, p. 44*; Segerstedt-Wiberg and Ors. v. Sweden*, App no 62332/00, ECHR 2006-VII, p. 72.

[4] Forbes Technology Council, *Data Privacy vs. Data Protection: Understanding the distinction in defending your data,* FORBES (DEC. 19, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#7ca6a8f450c9.

II. DATA PRIVACY LAWS

(A) Global Context

Data privacy law has always been a bone of contention in almost every nation alike simply because it entails a delicate balance between 2 opposing interests, i.e. the interest of the government in the data versus the individual right of control over one's data. The significant areas of conflict between these two interests garnered international attention in 2013, with the Global surveillance disclosure in the USA by Edward Snowden, an ex-NSA employee.

In today's time, not only does it remains to be an ethical issue but has instead become a legal issue, with more than 80 countries recognizing the Right to privacy as an inalienable pillar of a democratic setup. However, the question regarding the contours of this law remains unanswered- whether the individual privacy can give way to national interest like in the situation of a terror threat or whether the needs of intelligence bureaus in regard to the defence of the country can be justification enough to overpower the individual right.

Moreover, with the recent event of data breaches from Facebook coming to light, the protection of personal data and the consequent right thereof is also under the scanner vis-à-vis these technological giants.

In a global context, most countries differ on socio-economic fronts, and therefore, the laws and their application also vary. For instance, in the USA, 6,219,819,956 cases of breach of data or data theft have been recorded since 2013, which is the highest among all countries. However, despite this, the United States does not have one particular law dealing with data privacy and its protection. Consequently, most of the laws dealing with the subject matter are overlapping, and, at times, even contradictory. For Instance, the data collected in Health Sector is governed and protected by Health Insurance Portability and Accountability Act whereas Family Educational Rights and Privacy Act cover the records of health of student immunization which will often contradict the data covered under the Children's Online Protection Act. The above example clarifies that the lack of a federal statute regarding the protection of data privacy creates much confusion within the sectorial legislation.

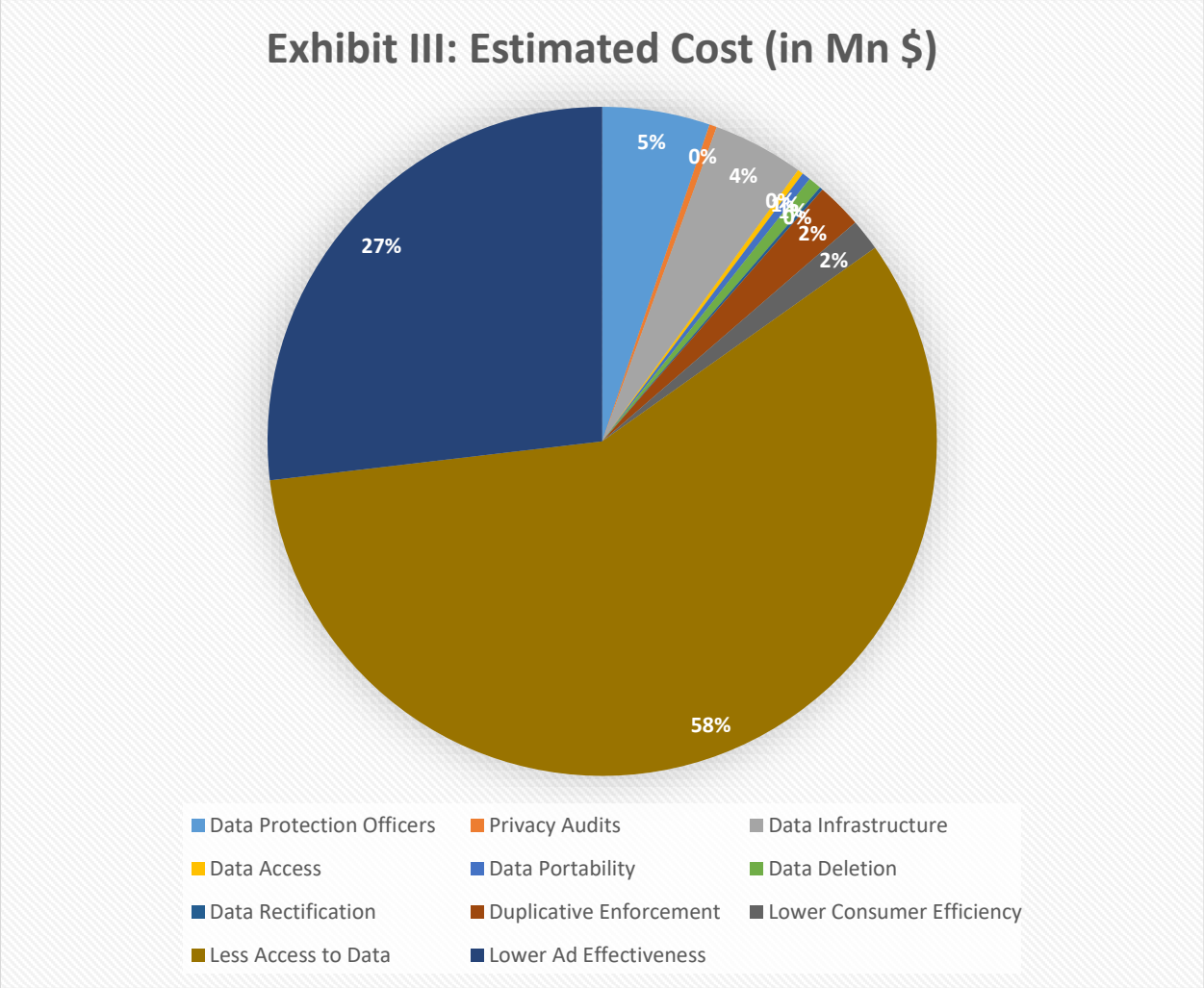
U.S Supreme Court has, on multiple occasions, attempted to define the basic right of privacy within the domain of the Bill of Rights and also suggested an amendment to the U.S Constitution. However, no substantial impact could be made on the legislature. Justice Douglas asserted in the case of *Griswold* v. *Connecticut*[5] that the right to privacy should come into the

[5]*Griswold v. Connecticut*, 381 U.S. 479 (1965).

 [ISSN 2581-5369]

ambit of the Bill of Rights, but the case was decided with a seven to two ratio. U.S. Supreme Court has never held in their ruling that the right to privacy is precisely under the domain of their fundamental rights.

After the revision of the General Data Protection Regulation (GDPR), the demand for a Federal Statute dealing with data privacy has gained momentum, but no positive sign has yet been seen. The reason for not having a federal statute can also be the cost of transition. The U.S. is one of the prime countries having advanced digital technologies, and the rules governing the data are specific to the sector. Therefore, the transition of all the data under one Federal Statute will lead to a higher financial burden.



The above pie graph is the representation of the distribution of the expenses which are likely to be incurred by the U.S to formulate a Federal Statute in line with the European Union GDPR. The Information Technology and Innovation Foundation did this study. The total accumulative estimated cost for transforming the whole data regime of the U.S. under one Federal Law is $122 billion per year. In terms of privacy alone, compliance under GDPR will cost the United

States $440 mn.[6]

The financial burden on the US economy is one of the critical factors for not introducing a single Federal Statute for Data Privacy Law despite having the most severe breaches and thefts of data. Here, it is pertinent to note the effect of not recognising the basic and inalienable right to privacy under the Fundamental Rights of the Constitution. If this right had been granted the status of a Fundamental Right under the U.S. Constitution, then the State would have been under a higher legal obligation to protect the data privacy of its subjects. Practically, for the US to be compliant with GDPR[7] is very costly; instead, Congress can come up with its national legislation focusing on serving the citizens and protecting data privacy which will not be that burdensome.

Moving further toward the situation in **China**, the law has recently gone through a significant overhauling. The changes were in light of a few contemporary data misuse threats like in the case of the Zao App controversy or the Alibaba Credit system facility. The former was a local version of the Face-swap app by means of which the person's face could be superimposed on that of any celebrity. However, the problem arose with the terms of the app which basically allowed the company to use any image created by the app. In the latter controversy, the company rolled out an online credit scoring service in which the users of Alibaba were enrolled by default. The function used private information like transaction history, and social media presence among other factors to arrive upon conclusions.

Both of these instances were dealt with very strictly, and a dire need was felt to introduce reforms in the already existing privacy laws in the country. Previous to this, there was no comprehensive law dealing with the issue but rather a web of laws dealing with the issue including the Cyber-security Act, 2017, Criminal Law, 2015, Consumer Protect Act, 2014 and Decision on Strengthening Protection of Network Information 2012.

As an aftermath of the abovementioned instances, the Cyberspace Administration of China notified new rules in 2019, which June 2019 titled Data Protection Regulatory guidelines. In addition to this, the CAC along with the Ministry of Public Security, the Ministry of Industry and Information Technology and the State Administration for Market Regulation, have launched a national campaign to inspect smartphone apps to determine if they illegally or

[6]Alan McQuinn& Daniel Castro, *The cost of an Unnecessarily Stringent Federal Data Privacy Law*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.
[7]General Data Protection Regulation, (EU) 2016/679 (GDPR).

 [ISSN 2581-5369]

excessively collect users' information.[8]

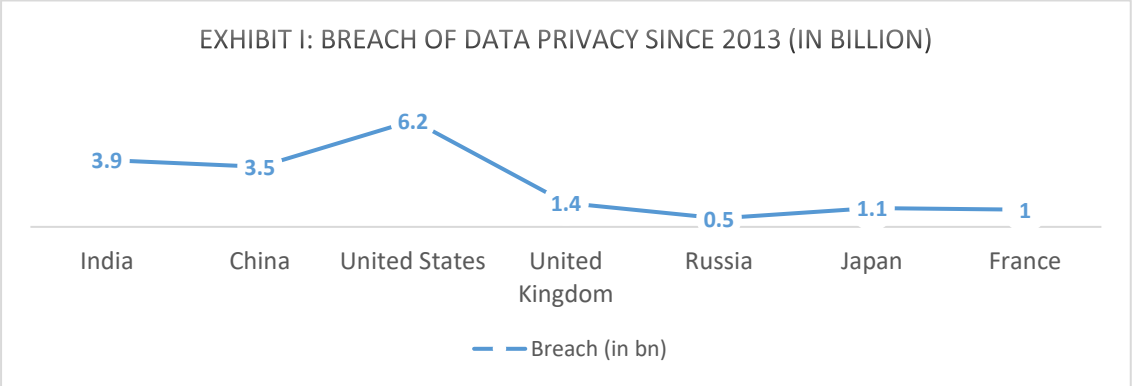
In the case of the United Kingdom, along with most European Union Nations has adopted the General Data Protection Regulations, issued in April 2016 as the basic law along with a few minor modifications to suit the needs of the nation. The salient feature of the GDPR is the establishment of the Supervisory Authority in every nation, which will be coordinated by the European Data Protection Board to facilitate easy and uniform data protection laws in all countries.

Smaller countries like Thailand also are taking the menace of data breaches seriously. As of 2019, the government is drafting a comprehensive law on the point titled "The Personal Data Protection Bill". However, till its promulgation, the data privacy is protected by the provision of the Constitution, the Credit Bureau Act 2002, the Child Protection Act 2003 and the National Health Act 2007 working together.

Therefore, in conclusion, it can be stated that the inherent right of privacy is embedded, in one form or the other, in the respective Constitutions or laws of the different jurisdictions which define the nature of this specific right. However, it is essential to also look at the need of having such a right in the first place.

a. Need for Data Privacy Laws

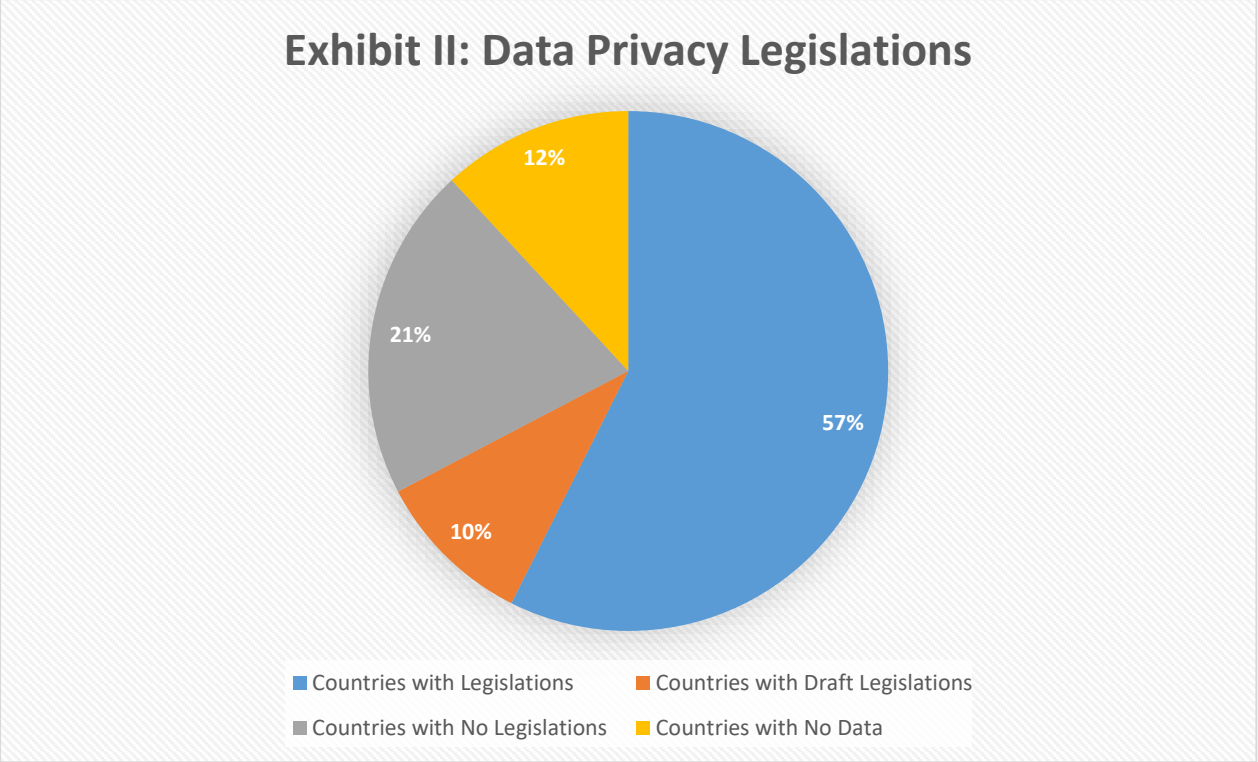
The progress in the development of the digital space in the last two decades has been enough to spark debates about the need for data privacy laws. As we move towards an era of complete digitization where we conduct several of our essential act ivities online, the question regarding the need for data privacy laws becomes more pertinent. The statistics which highlight the need for stringent laws related to data privacy have been discussed. It cannot be denied that strong legislation concerning data privacy is the need of the hour for all nations across the globe.



[8] Winston Ma, 'China Is Waking up to Data Protection and Privacy. Here's Why That Matters' (*World Economic Forum* 12 November 2019) <https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/.> accessed 1 June 2022.

Source: Varonis Data Privacy Breach Report[9]

Exhibit I, mentioned above, shows the statistics of breaches or theft of data in different countries. The data has been recorded since 2013, which projects the record of the breach that happened in the previous six years. The statistics represent that every other user of the internet is strangled into the web of breach of data privacy. Additionally, countries are moving towards a system of full digitalization, which means all the data, including personal and confidential data, is coming over the online mode. For instance, the use of mandatory Aadhar cards for different purposes. This increases the chances of breach of the private data of the users, which demands legislation for protecting the same.



Source: Data Protection and Privacy Legislation Worldwide[10]

Exhibit II represents the percentage of countries having data privacy legislations, drafts etc. As per the report released by United Nations Conference on Trade and Development, now there are only 58% of the countries have adopted legislation for protecting the right of data privacy while 10 % of countries are still deliberating on their draft bills. At present, almost 21% of the countries have not concretely understood the need for data privacy legislation, while 12% of

[9] Rob Sobers, *The World in Data Breaches,* VARONIS (Jul, 16, 2018), https://www.varonis.com/blog/the-world-in-data-breaches/.
[10] *Data Protection and Privacy Legislation Worldwide,* UNCTAD, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

countries do not have any data to protect in the first place.[11] This is concerning keeping in mind the fact that the outreach of the internet and modern technology is global. The data of the users is an important source which can be used to influence multiple facets of their life. In such a scenario it is essential to ensure that there is proper legislation for the protection of data so that the organizations collecting such data have a legal obligation to protect the same. A joint global effort will be important to ensure data privacy and ensure that users feel safe sharing sensitive data on the internet.

III. INDIAN VIEW ON THE RIGHT TO DATA PRIVACY

The Right to Privacy including Data Privacy has been attached to the Fundamental Right to Life enshrined under Article 21 of the Constitution of India. The famous ruling of *K.S. Puttaswamy (Retd.) v. Union of India* was instrumental in identifying the need for "*strong data privacy measure to prevent theft and abuse"*.[12] Before this pronouncement, merely two legislations on data privacy were in force, which was utterly insufficient for providing adequate data security. These legislations were:

- *Information Technology Act, 2000*
- *Information Technology (Reasonable Security Practices & Sensitive Personal Data or Information) Rules, 2011*

Realising the concerns raised by breaches of data privacy, India has made significant headway in the direction of data privacy by introducing a new Personal Data Protection Bill. However, the Apex Court of India has set a benchmark for the protection of data privacy. Article 21 of the Indian Constitution lays down the fundamental right to life and personal liberty which can be restricted as per the procedure established by Law. That law must also pass the threefold test laid down in K.S. Puttaswamy which includes:

- Prescribed by Law
- Legitimate Aim
- Necessary in a democratic society
- There should be sufficient measures taken for the protection of citizens from the adverse consequences which can result from the abuse of such powers.

Another impact of categorising the Right to Privacy under the Fundamental Rights is the

[11] *Ibid.*
[12] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, para 245

 [ISSN 2581-5369]

protection of basic structure doctrine. Fundamental Rights are an inherent part of the basic structure which cannot be amended by the legislature using its constituent powers. All the rights enshrined in Part III of the Constitution are protected under the basic structure doctrine. Recognising the privacy aspect with the right to life also brings with it all the consequences attached to a Public Interest Litigation under Article 32 of the Indian Constitution. Another major question which has been raised due to the inclusion of this right as a fundamental right is the waiver of the Right to Privacy. As a matter of right, fundamental rights cannot be waived but there are several exceptions (where the Government seeks the data) when this right has been waived. The Apex Court in *K.S. Puttaswamy case* referred to the judgment in *Behram Khurshed Pesikaka v. State of Bombay*[13] and held that Fundamental Rights could not be waived. Therefore, there needs to be a strict threshold upon the state while asking for the data of the citizens for its functions.

The state is the sole protector of the Fundamental Rights provided to the people. It is the obligation of the State that its citizen must enjoy their Fundamental Rights without any hindrance. However, the Apex Court, by recognising the Right to Privacy under Article 21 of the Indian Constitution, has defined the limits for the protection granted. For instance, Fundamental Rights cannot be enforced against non-state parties, and in cases of data privacy, incidentally, most of the breaches are by non-state parties since there are no territorial barriers over the internet. To protect the same, the need for a Personal Data Protection Bill was felt.[14]

The recognition of Data Privacy under the domain of Fundamental Rights has provided the drafters with a path to structure the right to data privacy in the new bill. Otherwise, the situation and result might have been different and contrary as previous laws are not competent enough and the new bill would be unable to properly define privacy.

The Draft Data Protection Bill was introduced in the year 2019. The Bill was not passed by the Parliament but referred to a Joint Parliamentary Committee for consideration and further amendments. There were several consultations carried out by the JPC with stakeholders. Once the process was committed, the JPC submitted its report with the finalized Data Protection Bill, 2021.

(B) Pitfalls in the legal system in the Indian context

Even though data privacy is attempted to be dealt by employing the 2019 Bill and the Apex Court has already recognised the right to privacy as a fundamental right, the menace of data

[13] *Behram Khurshed Pesikaka v. State of Bombay*, (1955) 1 SCR 613.
[14] Personal Data Protection Bill, 2019, Ministry of Law and Justice.

privacy breaches in India is far from over.

Even though 2018 has much more contemporary relevance and a more holistic approach towards the problem, it is not entirely devoid of any lacuna or difficulties. Some of the major issues that India is facing in light of recent events and the proposed law include:

- Since the law mandates storing critical data in India itself, it may adversely affect the FDI of the economy as the MNCs would now have to shell out more money to develop and maintain storage facilities in India itself.
- It gives a very widely worded exception to the State wherein in case it is related to any function of the state, non-consensual processing of personal data can also be undertaken.
- There exists overlapping of the domain, which will lead to more confusion and consequently lesser compliance. This is because the Bill is laid down as a general base, whereas sectoral guidelines will be issued separately. In the case of DISHA (applicable to the health care sector), there is a requirement of mandatory breach notification whereas according to the bill, only fiduciary notification is required.

Therefore, the need of the hour is to address the lacuna in the Bill along with dealing with all the implementational problems to effectively counter the issue at hand. The amended Data Protection Bill, 2021 provides hope in this regard. Some of the provisions have been analyzed for a greater understanding.

Data Protection Bill, 2021

The applicability of the Bill is widespread. It includes personal data processed, shared, disclosed or collected by the State, State bodies, corporate entities in India and the citizens of India. It also includes non-personal data and the data has been provided with different layers of protection as per its nature. The applicability of the law is not limited to India and applies to the data fiduciaries and processors which are located outside India. In an attempt to balance the interest of the data subjects and the fiduciaries, there is the existence of Notice of Use, Prior Consent and Limitations.

The responsibilities of Data Fiduciaries when it comes to the handling of data have been increased. They need to create “privacy by design” models. Such models should be transparent with the processes and algorithms used by them. The data subjects should be provided with comprehensive notices which possess information related to retention policies and cross-border transfers.

For effective implementation of the law, a Data Protection Authority is to be constituted. The

 [ISSN 2581-5369]

body will consist of no more than six individuals and will have the responsibility to monitor compliance with the law and its enforcement wherever necessary. To ensure the best minds in the nation from different fields, the DPA must consist of the attorney general and a director from both the Indian Institute of Management and the Indian Institute of Technology.[15] The DPA is responsible for the creation of accounting standards to be followed, fostering trust and establishing penalties for non-compliance. Every organization which is subject to the law must appoint a data protection officer to ensure compliance.

The Government has wide discretionary powers when it comes to cross-border transfers. The DPA needs to consult the Government. The approval or the rejection of the request will be dependent on the compatibility of the scheme with state or public policy. It fixes greater accountability for organizations responsible for data protection. In case there is a data breach which involves personal or non-personal data, it must be reported to the DPA by the organization within 72 hours of becoming aware of the same.

The Bill also bats for localization of data storage. It seeks to impose a mandatory requirement to process the data in India. There is still a provision which allows for the transfer of sensitive data to other countries but requires that a copy of the same be retained in India. The Government is to issue detailed localized practices after its enactment.

The Bill is a significant step taken for the protection of data privacy in India. If made into a law, it will be the third law related to Data Protection after the GDPR and the PIPL which impacts a large population. India has been regularly upgrading its infrastructure to be more digital and with the introduction of Aadhaar and Digi Locker, a large amount of sensitive data of its citizens is over the internet. Therefore, the legislation was the need of the hour particularly in the aftermath of the *Puttusamy* judgment as the lack of Privacy for data could greatly infringe the Right to Privacy of the citizens. The law is still on the table and there is room for further changes and modifications. However, considering that the EU and China have already passed similar legislations, it is expected that India will act on the same soon

(C) Data Privacy and China

Covid-19 resulted in a drastic increase in the usage of online technologies to provide businesses and services to customers. China, being the country with the largest population on the internet, felt the need for comprehensive privacy law in such circumstances. This led to the enactment of the Personal Information Protection Law (PIPL). It is the first law enacted by China for the

[15]Epiq, 'Ten Compelling Features of India's Proposed Data Privacy Law' (*JD Supra* 30 March 2022) <https://www.jdsupra.com/legalnews/ten-compelling-features-of-india-s-6127498/> accessed 1 June 2022.

regulation of online data and the protection of personal information. This was in continuance with the Data Security Law (DSL) passed by China 3 months prior to the PIPL. The DSL finds application in a large number of activities which involve data processing which includes the processing of personal information. The scope of both the laws expands beyond the territory of China.

The task of the enforcement of PIPL is with the Cyberspace Administration of China along with the local and state departments of the Government. It takes several key aspects from the General Data Protection Regulation (GDPR) enacted by the European Union. The penalties imposed are as high as more than 5% of the revenue of the previous year or $7.7 million.

The scope of Jurisdiction of the PIPL is similar to that of GDPR. It has extra-territorial application and it includes any company or individual who processes the personal information of individuals in China within its ambit. It further mandates that the personal information processors which are located outside China establish an entity within China or make the appointment of representatives responsible for personal information within China under Article 53. Article 52 mandates that the contact details of the individual responsible to protect and process personal information be published if they meet certain thresholds which are yet to be defined.

Personal Information is defined under Article 4 of the PIPL as, *"various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously."*

Sensitive Personal Information has been defined as, *"The personal information that can easily lead to the infringement of the personal dignity or natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14."*

It further defines Personal Information Processing Entity under Article 73 as *"Organisation or individual that independently determines the purposes and means for the processing of personal information."*

The PIPL is similar to the GDPR to the extent that it requires that the organisations have a lawful basis for the processing of personal information. "Legitimate Interests" are not included under the lawful basis for the protection of information like the GDPR. Article 13 of the PIPL allows the organizations to access the following information on a non-consent basis. Some of the information which is allowed to be processed on a non-consent basis includes:

 [ISSN 2581-5369]

- The information which is necessary to enter into or perform a contract to which the individual is a party.
- Essential information for the fulfilment of legal responsibilities or obligations.
- Information crucial to a proper response to a public health emergency or protection of the safety of the property of the individual and their health.
- Some other situations where the disclosure of the information is mandated by law.

Any information outside the ambit of the information which can be processed without consent must only be processed after seeking due consent from the user. The essentials for consent are similar to those mentioned in the GDPR. The consent should be freely given, informed, clearly demonstrated by individual act and can be withdrawn at a later stage. There is a need for separate consent for certain processing activities under the law. The instances are mentioned below:

- If the personal information is shared with other processing entities.
- If the personal information is disclosed publicly.
- If the personal information being processed is sensitive.
- If there is an overseas transfer of personal information.[16]

Article 50 further empowers individuals to bring forth lawsuits against organizations if their requests to ensure individual rights are not paid heed to. Moreover, the burden of proof is on the entity and the individuals will be provided compensation with regard to the actual damage caused or the illegal profit obtained by the processing entities under Article 69. This further provides additional incentives for individuals to utilize their rights if the entities reject their requests.

There is a great degree of alignment between the PIPL and the GDPR when it comes to rights related to personal information. However, the language of the PIPL when addressing certain rights is relatively vague and undefined. For example, the processing entities are required to give a "timely" response to the requests. There is no specific timeline for the same. The minimum quantum of penalty to be imposed in case of violation of PIPL has not been specified. Therefore, there lies a wide discretion with the regulators in the imposition of penalties. Article 67 provides that the violations could be recorded in the "credit files" of the processing entity. This can affect their business in China and thus ensure that they remain careful.

The PIPL is a fine example of how China recognized the importance of bringing forth legislation for data protection. The increased usage of the digital space in the aftermath of Covid-19 was

[16]Xu Ke and others, 'Analyzing China's PIPL and How It Compares to the EU's GDPR' (*Iapp* 24 August 2021) <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/>.

recognized by China and realizing the importance of the protection of the data and privacy of its citizens, it enacted the PIPL. The United States of America on the other hand still lacks comprehensive legislation for data protection. As discussed earlier, it relies on several laws for data protection but there are several grey areas due to the lack of comprehensive legislation.

(D) General Data Protection Regulation (GDPR) – The first comprehensive legislation for Data Protection

The GDPR was the first comprehensive law for the security and protection of data. It was drafted by the European Union and came into force on 25th May 2018. Its applicability is not limited to the EU and applies to entities all over the world as long as their target audience is in the EU or the data collected is of the residents of the EU under Article 3. A breach of the GDPR regulations can result in the imposition of heavy fines. Two of the largest corporations in the world Google and Meta were fined 150 million Euros and 60 million Euros respectively for the breach of the regulations. They had violated the regulations since they did not make the process of refusal of cookies convenient for the users and it hinted at coercion into acceptance. The timeline for the payment of the fine was three months, failing which there will be an additional penalty of a hundred thousand Euros per day of the delay. They also need to ensure that they provide a simpler mechanism to refuse cookies.[17] This shows that the implementation of the GDPR is in full force and is only bound to grow with time.

It is based on the European Convention on Human Rights, 1950 which provides that, *"Everyone has the right to respect for his private and family life, his home and his correspondence."* This right was often violated in the digital space since it was still under development. The development was expedited by an incident in 2011, where Google was sued by a user for scanning her emails. This led the data protection of the EU to declare the need for *"a comprehensive approach on personal data protection."*[18]

There are a large number of key legal terms which have been concisely defined under the GDPR. The PIPL of China and the Data Protection Bill of India have also taken some of their definitions from the GDPR. For example, personal data is defined as, *"any information that relates to an individual who can be directly or indirectly identified."* This can include names, addresses, gender, biometrics, cookies and more. Even pseudonyms can be classified as personal data if one's identity can be deciphered from it. The entity which decides the need and

[17] Reuters, 'Google Hit with 150 Mn Euro French Fine for Cookie Breaches' (*The Indian Express*7 January 2022) <https://indianexpress.com/article/technology/tech-news-technology/google-hit-with-150-mn-euro-french-fine-for-cookie-breaches-7711091/> accessed 1 June 2022.

[18] Ben Wolford, 'What Is GDPR, the EU's New Data Protection Law?' (*GDPR.eu* 7 November 2018) <https://gdpr.eu/what-is-gdpr/>.

the method for the processing of data is known as the data controller. A third party which processes data for a data controller is defined as a data processor. There are special rules for such entities under the GDPR. These definitions provide clarity to the role.

The GDPR also provides an expansive definition of consent under Article 4(11). It provides that, *"Consent must be unambiguous, freely given, specific and informed."* Article 7(32) provides that consent is not constituted through pre-ticked boxes, silence or inactivity. This definition bodes well for the rights of the users as their consent will be given easily and they will have greater freedom of providing their consent after understanding its implications.

Article 5 of the GDPR lays down the *"Principles relating to processing of personal data."* It provides the following criteria for usage of personal data:

a. "processed lawfully, fairly and in a transparent manner in relation to the data subject;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to the implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

This is to ensure that the process of data collection and storage is fair and transparent. It also intends to limit the usage for a specific purpose and only collect the data which is required. The

 [ISSN 2581-5369]

data should be accurate and once its usage is completed, it should be erased expediently. This ensures that the integrity and confidentiality of the data are maintained. If the measures are not complied with, the controller is helped responsible, thus providing for greater accountability. Article 6 further specifies the situations where the processing of data is allowed.

There must be a justified reason for the usage of data. It requires the unambiguous consent of the user and a need to use the data. The data can be processed for fulfilling legal obligations and medical purposes. A task which is in the interest of the public is also a valid reason to collect data. There is some scope of discretion in the clause where a legitimate interest will also be enough to process personal data. This also has the rider that the *"fundamental rights and freedoms of the data subject"* cannot be compromised in any case.

If a Data Controller is a public authority or monitors people systematically and regularly on a large scale, there is a need for the appointment of a Data Protection Officer (DPO). In other cases, the appointment of a DPO is not necessary but can be beneficial. It allows the organisation's personnel who understand the applicability of the GDPR and assist it to undertake practices which further comply with the regulation. The data subjects have a great deal of privacy rights assigned to them under the GDPR. This includes the right to be informed, the right to restrict, the right to object and more.

The principles of the GDPR apply to the processing of data. It provides for data integrity, protection from unlawful processing, accountability, transparency and fairness. It has specific conditions which need to be fulfilled by the corporation processing and using the data. Such conditions are absent in acts of other countries such as the Information Technology Act, 2000 in India. The security measures which are to be adopted under the GDPR are elaborate and seek to ensure the security of data. The measures like the appointment of a data security officer, conducting privacy impact assessment and maintenance of records of processing are well-thought and aim for the provision of a robust mechanism for security.

The mechanism is so rigid that even a method of data transfer can be deemed invalid. This was seen in the case of *Data Protection Commissioner* v. *Facebook Ireland and Maximillian Schrems.*[19] The Court held that even if data is transferred and processed by authorities of the third country in question for the purposes of public security, defence and State security, such data cannot be precluded from the scope of GDPR. The data can only be transferred to a third country for the purpose of processing if the process complies with the GDPR.

The penalties under the GDPR are significant and as seen with the fines imposed on Google

[19] *Data Protection Commissioner* v. *Facebook Ireland and Maximillian Schrems,* C-311/18.

 [ISSN 2581-5369]

and Facebook, the amount of penalty can even affect deep-pocketed corporations. It is comprehensive legislation for dealing with data privacy and the world's first legislation to do the same at this scale. It has set the benchmark and will greatly assist the enactment of similar legislation across the globe.

(E) Data Privacy and US Law

The US Supreme Court in the case of *Carpenter* v. *United States,*[20] the US Supreme Court ruled that *"The Government needs a warrant to access a person's cellphone location history. The court found in a 5 to 4 decision that obtaining such information is a search under the Fourth Amendment and that a warrant from a judge based on probable cause is required."* It held that in order to access detailed personal and sensitive information about a person using a method which provides great surveillance needs a proper warrant and the data of citizens in such cases must be protected from warrantless intrusion by the Government. The counsels argued and the Courts recognized that the old rules allowing for warrantless searches of physical information like traveller's luggage, the trunk of the car and more cannot be compared to the kind of information which is stored in electronic devices. Therefore, such information should be granted greater protection. This was a significant decision the USA does not have a central law for data privacy, unlike the EU and China.

However, it possesses several state and federal laws which are used to protect the privacy of the citizens. The oldest law related to the personal data of the citizens was the US Privacy Act, 1974. It included certain rights and restrictions related to the data held by the Government agencies of the USA. It provided the citizens with to access the data stored by the Government and correct any errors. The principles of data minimization were reflected in the law. The least information had to be collected for the specific purpose. The data is not accessible to everyone in the agency and only the ones who need to know are given access. The sharing of information is only allowed in certain cases.[21]

The Health Insurance Portability and Accountability Act, 1996 (HIPAA) was enacted to regulate the health insurance sector. The legislation included certain key elements linked to data privacy. It has a privacy rule where the health information can be shared with spouses and other family members only after obtaining consent from the individual. It provides healthcare providers to use patient data for the "treatment, payment, and health care operations." However, the usage of the data for marketing purposes or selling requires the consent of the individual.

.[20] *Carpenter* v. *United States,* 138 S. Ct. 2206.

[21]Andy Green, 'Complete Guide to Privacy Laws in the US | Varonis' (*www.varonis.com* 2 April 2021) <https://www.varonis.com/blog/us-privacy-laws#eu-vs-us>.

Similarly, the Children's Online Privacy Protection Act (COPPA) prohibited the collection of all kinds of information from minors under the age of 12 without parental consent which can be verified. It states that the originating website operator must take *"reasonable steps to release children's personal information only to companies that are capable of keeping it secure and confidential."*

Similarly, the state of California enacted the California Consumer Privacy Act, 2018 (CCPA). This was to provide privacy protections to the consumer on the internet as well. Till date, it is the most comprehensive data privacy legislation related to data on the internet in any part of the USA. It allows the consumers to access the information held by businesses and necessitates that they are provided with an opportunity to opt-out. They can request the deletion of their personal request information. If the consumers end up being victims of a data breach, they are also provided with a right to sue. The definition of personal data which is, *"information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,"* is similar to that under GDPR and is very comprehensive.

It also introduces *"probabilistic identifiers"* which mean, *"the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to the categories enumerated in the definition of personal information."* This allows certain other data which is not specifically personal data to be qualified as an identifier and be given protection under the act. The law is largely influenced by the GDPR and other states like Massachusetts, New York, Maryland and Hawaii also have similar data privacy legislation largely based on the CCPA.

Therefore, it can be seen that the USA has federal level laws for certain sectors like healthcare which protect data privacy. However, it still lacks comprehensive legislation related to data protection at the national level. There is a lack of uniformity and consistency in the application of laws which still allows corporations to take advantage of the loopholes in the data privacy law. This is apparent with companies like Google and Meta offering much stricter policies in Europe compared to the USA where they still make use of the leniency of the laws. Thus, a comprehensive data protection law is the need of the hour for the USA.

IV. CONCLUSION AND RECOMMENDATIONS

"Data privacy" is an extension of the right to privacy. Right to Privacy is a conundrum of rights as it is not fixed under one domain. Under the international regime, the Right to Privacy has been given the status of a basic human right. Under national laws, countries usually differ in

providing the status as can be seen from the above examples. India declares privacy a part of the Fundamental Right to Life, whereas the U.S. deals with the Right to Privacy as a Legal Right provided by Fourth Amendment but not as a separate Fundamental Right.[22] This grant states to get a waiver of this right to procure data from the people.

However, the question here is why data privacy needs to be categorised? The Constitution of any country is the grundnorm which forms the basis for the nation's legislative, administrative and judicial framework. No law can be in contravention of the Fundamental Rights enshrined in the Constitution. Therefore, defining the status of the Right to Privacy as a Fundamental Right will help the nation in formulating a systematic structure for the national legislation on Data Privacy.

Further, having Analysed the data privacy laws of countries like India, the USA, the EU and China, it is pertinent to mention that the laws have taken a very dynamic nature and are continually evolving to not only fit the society in a better way but also to keep up with the newer and novel challenges that the development in technology poses such as the incessant development in the field of artificial intelligence among others. It is noteworthy that not only the developed countries like the UK and USA but also the developing countries like India and Thailand are continually trying to deal with the problem of data breach. China too has joined the bandwagon and has beaten the USA in the introduction of a comprehensive law for data protection.

However, despite having proper laws in place to deal with the problem of data breach, the instances of such crimes taking place are just increasing. Since all the countries have a different socio-economic background, states of technological development, demography as well as political setup, there can be no one-stop solution to the problem of data privacy breach. However, specific standard measures can be taken to effectively handle the menace mentioned above, especially in a developing country like India. The measures include:

- Countries need to categorise the status of the Right to Privacy / Data Privacy as a right.
- Having an independent and dedicated institution explicitly dealing with the problem of Data privacy in each country like the CAC established in China.
- An international body, made on the model of EDPB of the European Union to effectively deal with any data privacy breach on a global or inter-country level.

[22] Fourth Amendment to the U.S. Constitution. 1791.

 [ISSN 2581-5369]

- To ensure mass support and more compliance, simplification of the law along with awareness drives should be undertaken. Something like this was attempted by Google which offered free online courses to one and all on GDPR, Data privacy law compliance etc.
- The more developed the country, the higher the need to protect its data. The same difficulty is equally applicable in the implementation of a consolidated law on a subject throughout the jurisdiction.
- A comprehensive, inter-sectoral analysis of the law should be done to ensure maximum implementation without any lapses.
- The exemptions that are culled out in the law should be narrowly worded and strictly interpreted so as to give maximum benefit to the citizen.
- A uniform model of protecting data privacy is needed, if not in compliance with GDPR.

European Union GDPR is acting as model legislation for most nations, but any legislation has to be implemented considering the factors peculiar to that nation. Every nation cannot adopt a stringent law as EU GDPR; instead, countries have to come up with their own laws for protecting the breach of data privacy. The prime example of this situation is the United States, where the transition to the law in compliance with GDPR is costing a huge estimated burden on the economy. China on the other hand has been successful in adapting some of the best features of GDPR and including them in the PIPL. It has ensured that the provisions are not blindly copied and meet the needs of the country. It still attempts to maintain a certain level of uniformity for easier compliance.

The least uniformity which can be maintained is to recognize the right to data privacy as a Fundamental Right, thereby giving citizens open avenues to approach and fight for their rights. However, the scope of the term data privacy needs to be explicitly defined as it will decide the future of various other aspects. For instance, "data privacy" covers all the information of private life but in the case of the Head of the State, the private life of the Head of the State is also a national security concern.

The statistics presented in this disquisition are to help the readers to analyze the factors important while deciding the status of the right to privacy, including data privacy. Instances of identity theft, cost of transition to be GDPR compliant, and statistics about the states having data privacy legislation, project the conclusion that there is a dire need for a data privacy law in every state suited for the circumstances of the country. Therefore, this conundrum of the status

of data privacy right needs to be settled to give a proper structure to the upcoming laws and recognising the same as a Fundamental Right is the best way forward.

*****

 [ISSN 2581-5369]