Page 255 - 264 **DOI:** *https://doij.org/10.10000/IJLMH.113602*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Privacy and the Development of Personal Data Protection Legislation

NIKHIL R VASISHTA[1]

ABSTRACT

This paper delves into the pivotal aspect of privacy under Article 21 of the Indian Constitution and also the development of Personal Data Protection in India. In the backdrop of various socio-legal changes that are brought into light, data privacy is a reckoning area in the era of digital economy. The absence of such legislation today is unimaginable and untenable; however, India is in the lime-light of great strides continually made in the field of Data Protection and Privacy. There have been a lot of recommendations, not only to protect the privacy of the individual but also to secure the interest of the businesses alike. There is still a lot left to be included in the bill on how it stands today. But, in the field of technology which is ever growing, the law governing it is in need of persistent change. Therefore, an analysis is needed of the same at regular intervals to keep up with changing circumstances and also check the effectiveness of implementation.

Keywords: *Data Protection, Privacy, Article 21, GDPR, Personal Data, Sensitive Information, Profiling.*

I. INTRODUCTION

India is yet to have a standalone legislation with respect to the Personal Data Protection to secure the rights of the people. The Information Technology Act, 2000 has rather a paltry inclusion of Data Privacy.

Personal Data is defined under Article 4(1) of the General Data Protection Regulation (GDPR):

Personal Data is any information which is related to an identified or identifiable natural person. Only where the processing of personal data is in question, there is applicability of GDPR.

The personal data may include reference to the identity of the person directly or indirectly such as: Name, Identification number, location data, online profile as to the physical, physiological, genetic, mental, cultural and social identity of the person.

Article 4(1) of the GDPR gives a very wide interpretation to the term Personal Data, where it begins with the terms “any information” and is upto to the discretion of the court to decide on

[1] Author is a student at BMS College Of Law, Affiliated to Karnataka State Law University, India.

 [ISSN 2581-5369]

case-by-case basis.

This has been the very basis for the Personal Data Protection Bill, 2019 where it states that whereas the right to privacy is a fundamental right, it is necessary to protect personal data as an essential facet of informational privacy.

Section 3(28) of the Personal Data Protection Bill, 2019 describes Personal Data as:

"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;

Profiling in this circumstance shall include any forms of processing of Personal Data that analyses or predicts aspects concerning behaviour, attributes or interests of data principles as defined in s3(32) of the Personal Data Protection Bill.

II. INTERNATIONAL CONCEPTS OF PRIVACY

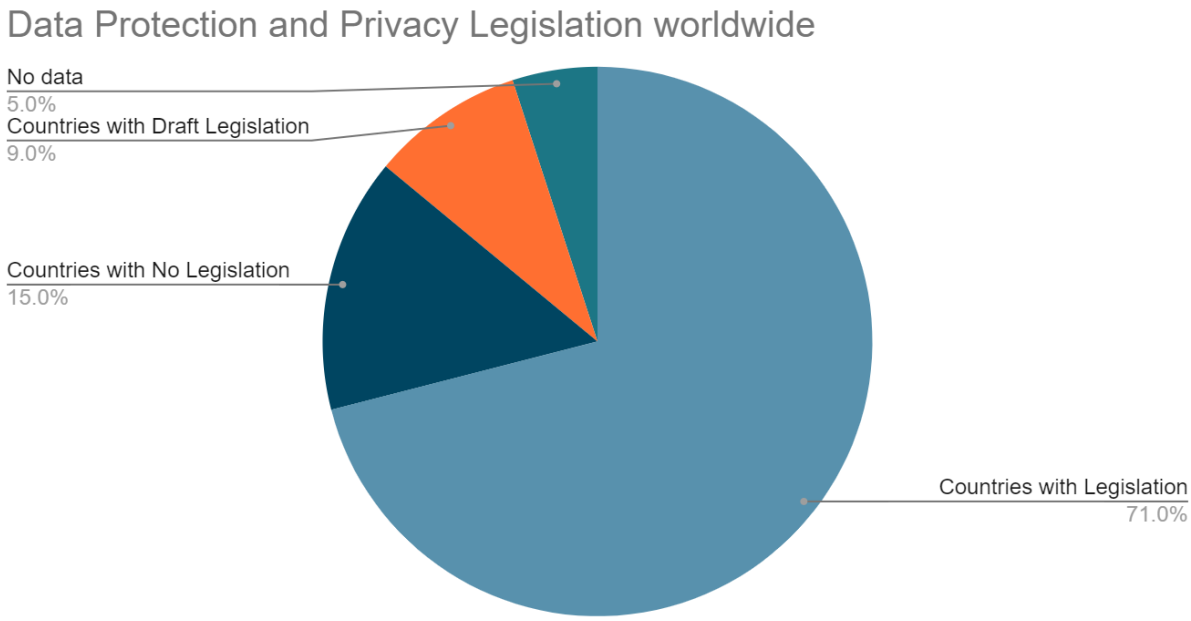
Article 8 of European Convention on Human Rights[2] states "Everyone has the right to respect for his private and family life, his home and his correspondence; there shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals or for the protection of the rights and freedoms of others.

Article 12 of Universal Declaration of Human Rights (1948)[3][4] states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."

Article 17 of International Covenant on Civil and Political Rights[5] states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation"

[2] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, Available at https://www.echr.coe.int/documents/convention_eng.pdf (last visited Sep 16, 2022).
[3] Universal Declaration of Human Right, Dec. 10, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights (last visited Sep 16, 2022).
[4] Ibid.
[5] International Covenant on Civil and Political Rights, Dec. 19, 1966, No. 14668, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

A significant number of nations around the world, upto 71% already have legislation in place of data protection and privacy with also another 9% of countries having draft legislation.[6]



Source: United Nations Conference on Trade and Development on Data Protection and Privacy worldwide. The dataset is as of 14/12/2021.

The above infographic shows a wide enforcement of the Data Protection laws around the world i.e., 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. Africa and Asia show different levels of adoption with 61 and 57 percent of countries having adopted such legislations. The share in the least developed countries is only 48 per cent.[7]

The International privacy laws for data protection generally follow, or are guided by, the five global privacy principles of:

1. Notice – To make people aware of the type of data that's been collected and stored and it creates a right over such data.

2. Choice and consent – providing people with choices and consent around the use, storage, management and collection of personal information. Today, in many websites we see the pop-up of cookies being asked when one enters any website.

3. Access and participation – For people to know who is accessing the personal information and in what way they are being used. The people can actively request for their data to be removed.

[6] Data Protection and Privacy Legislation Worldwide | UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Sep 16, 2022).
[7] ibid

4. Integrity and security – ensuring that the data is secure and that there is no unauthorised access.

5. Enforcement – ensuring that the service, site, solution and platform are aligned with some form of regulation that enforces compliance.

The European version of the Data Protection Law, the GDPR, is widely used as a benchmark in the formation of new Data Protection Laws around the globe. GDPR made a big case for the protection of the data securely and the compliance was also duly ensured. Non-compliance to the GDPR would be met with Dawn Raids, Hefty fines and the damage to the reputation of the entity. The enforcement of GDPR created a seismic global shift in how countries, organisations and individuals viewed data privacy and saw a rapid global move towards more rigorous controls and protections.[8]

In the United States, there is no federal law on Data Protection but the states have their own version of laws at a basic level. While many states have already implemented the laws, many states have yet to finalise the draft legislation. Among the states, the state of California with the California Consumer Privacy Act (CCPA) is said to be having great privacy rights and data protection. This created a new obligation on businesses to disclose the type of data that the business collects about the consumers and the reason to which they are selling, collecting and sharing personal information. It also gave rights to the people to opt out of the data being collected and sold to third parties and also request access to data and thereby deletion of the same.[9]

Canada, has implemented the Personal Information Protection and Electronic Documents Act (PIPEDA) that is framed with reference to GDPR. The Act entails the 5 global privacy principles as mentioned above and offers a great deal of choice and consent to the people. However, on 17/11/2020, the Canadian Minister for Information, Science and Economic Development introduced a new charter, The Digital Charter Implementation Act (DCIA) to replace PIPEDA. This new charter is set to surpass the guidelines laid down in GDPR while also imposing heavy penalties on the offenders.

In another developing country across the world, Brazil has one of the most extensive sets of Data Protection Legislation, where the General Data Protection Law that supports a

[8] Data protection regulation around the world, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world (last visited Sep 16, 2022).

[9] Codes Display Text, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (last visited Sep 16, 2022).

comprehensive list of more than 40 data privacy laws that have been brought into force through the years. Much like GDPR, it warrants the companies to appoint Data Protection Officers and have solid security protocols in place. Lei Geral de Proteção de Dados (LGPD), a data protection law also based on GDPR came into force on 18th September, 2020. It gives similar definitions and essentially same subject data rights.[10]

III. THE GENESIS OF THE PERSONAL DATA PROTECTION LEGISLATION

With pronounced growth in the field of Technology over the yester years, there has been a long-standing wait for the change in legislation in the field of Information technology and more importantly in the field of Data Protection in India; There have been attempts made to address the question of privacy and has been a continually evolving aspect not only in India, but throughout the world. Europe has been the focal point for data protection legislations much like the General Data Protection Regulation (also commonly referred to as GDPR) which came into force on 25th May, 2018. and the UK Data Protection Act 2018 which is the United Kingdom's adaptation of the GDPR.[11] Contrarily, the Indian government has recently withdrawn the Personal Data Protection Legislation[12] after deliberating since 2018. This bill was based on the recommendations made by the committee of experts under the chairmanship of Former Justice B. N. Srikrishna in a 176-page report and presented the report and draft bill which was also vaguely based on GDPR on 27th July 2018 to the Ministry of Electronics and Information Technology (MeitY).[13] Among the recommendations, the following are considered to be substantial:

- ➔ Fiduciary relationship between the individual and service provider and obligation of the service provider to:
  - ◆ Process data fairly and reasonably
  - ◆ To give notice to the individual at the time of collecting data
- ➔ Definition of Personal Data in section 2(28):

It became very essential to determine what would be considered under the ambit of Personal Data and hence the aspects that would be bound by the act itself.

"personal data" means data about or relating to a natural person who is directly or

[10] What is the LGPD? Brazil's version of the GDPR - GDPR.eu, https://gdpr.eu/gdpr-vs-lgpd/ (last visited Sep 16, 2022).
[11] Data protection, GOV.UK, https://www.gov.uk/data-protection (last visited Sep 16, 2022).
[12] Bulletin No. 1, Lok Sabha, dated August 3, 2022, http://164.100.47.193/bull1/17/IX/03082022.pdf
[13] Data Protection Framework | Ministry of Electronics and Information Technology, Government of India, https://www.meity.gov.in/data-protection-framework (last visited Sep 16, 2022).

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;[14]

➔ Providing rights to Individuals through consent-based processing:

The individuals would have the option of giving their personal data for selling, collecting and sharing and at any time the individual has the right to access the personal information and also request for the deletion of the same.

➔ Amendments to other laws

Certain laws were needed to be amended to facilitate the implementation of the Personal Data Protection Bill.

1. Information Technology Act, 2000
2. Census Act, 1948
3. Aadhar Act, 2016
4. Right to Information Act, 2005

➔ Setting up a Data Protection Authority to ensure compliance with the bill.

➔ Transfer of data outside India: Personal data (except sensitive personal data) may be transferred outside India under certain conditions. These include: (i) where the central government has prescribed that transfers to a particular country are permissible, or (ii) where the Authority approves the transfer in a situation of necessity.

➔ Offences and Penalties: Under the Bill, the Authority may levy penalties for various offences by the fiduciary including:

- failure to perform its duties,
- data processing in violation of the Bill, and
- failure to comply with directions issued by the Authority.

More recently, another report of the Joint Committee of the Parliament (JCP) has suggested 81 amendments and 12 major recommendations, which practically meant overhauling the bill.[15]

[14] Supra note 2.

[15] IT Ministry will soon come up with new version of Data Protection Bill, says Union Minister Ashwini Vaishnaw, https://www.aninews.in/news/national/general-news/it-ministry-will-soon-come-up-with-new-version-of-data-protection-bill-says-union-minister-ashwini-vaishnaw20220905211150/ (last visited Sep 16, 2022).

The recommendations also included expanding the scope of the proposed law to cover discussions on major topics like:

- ➔ Change in name to "Data Protection Bill".
- ➔ Inclusion of non-personal data - The bill to include both personal and non-personal data.
- ➔ A transition period of 24 months from the date of notification of the act.
- ➔ Procedure for selection of Data Protection Authority (DPA)
- ➔ Data Localisation - Introduced in the fallout of the government banning 54 Chinese apps in February 2022 for storing personal data outside the country and was considered detrimental to national security.[16]
- ➔ Social media liability - Which makes social media platforms liable to the content posted on the platform.
- ➔ Harsh penalty - fine upto 15 crore or 4% of the total global turnover of the term and/or jail term upto 3 years.
- ➔ 72-hour notification period to the data protection authorities in the case of data breach.

Many Industry analysts claimed the withdrawal was a bad move.[17] The delays in the Bill had been criticised by several stakeholders pointing out that it was a matter of grave concern that India did not have a basic framework yet to protect people's privacy.

Much recently, the IT minister was quoted saying "The Data Protection Bill was withdrawn from Parliament because that bill had become **very complex**, there were far too many amendments that had made the bill create a high degree of compliance for our start-ups and small companies."[18]

However, It is set to be back in the form of 2 new bills, The Digital Data Protection Bill and secondly The Digital India Act to replace the Information Technology Act, 2000 which are to be introduced in the winter session of the parliament later in the year.[19]

However, there are concerns being raised on the nature of the Legislation as it had become very

[16] Govt bans 54 Chinese apps over security threat concerns | Latest News India - Hindustan Times, https://www.hindustantimes.com/india-news/govt-to-ban-54-chinese-apps-that-pose-threat-to-india-report-101644814634095.html (last visited Sep 16, 2022).
[17] Withdrawal of the Personal Data Protection Bill was a bad move - The Hindu, https://www.thehindu.com/opinion/lead/withdrawal-of-the-pdp-bill-was-a-bad-move/article65750995.ece (last visited Sep 16, 2022).
[18] Ibid.
[19] Ibid.

complex and it may create a high degree of compliance issues as earlier mentioned. It is still unsure whether the bill would revert back to its foremost iteration based on the Former Justice Srikrishna committee report or whether it would adhere to the report of the Joint Committee of Parliament. In the light of this, there is an inherent need for stringent and enforceable legislation.

IV. DEVELOPMENT

The case of JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA[20] is a cornerstone of the jurisprudence of privacy law in India. In this case, the nine judges unanimously reaffirmed the right to privacy as a fundamental right of the Indian Constitution. The Supreme Court has ruled that the right to privacy is an integral part of the freedoms guaranteed by fundamental rights and an essential aspect of Dignity, Autonomy and Liberty.

The lawsuit began with the question of whether the right to privacy, raised in the 2015 dispute over the legal validity of the Aadhaar database, and whether the Article 21 of the Indian Constitution also confers the right to privacy. There was an argument being made as to the existence of the right to privacy as a fundamental right in the view of the 2 decisions in the cases of, MP. Sharma vs. Satish Chandra, District Magistrate, Delhi[21] was decided by a bench of eight judges, where it was argued that the Indian Constitution did not have any language like the 4th Amendment of the Constitution of the US. Kharak Singh v. Uttar Pradesh[22] was decided by a bench of six judges where Justice Subbarao was of the opinion that the Right to Privacy was not guaranteed under the constitution, however he considered that the Right to Privacy formed a part of Personal Liberty under Article 21. The state argued that both cases included remarks that the Constitution did not explicitly protect the right to privacy as a fundamental right. At the same time, the right to privacy has been recognized as a fundamental right in subsequent years of court decisions. However, these subsequent decisions confirming the existence of the right to privacy were made by Courts with smaller benches than M.P. Sharma and Kharak Singh. The case was referred to a nine-judge bench because of the precedential value of the judgement and the momentous implication that would follow due to the importance of right to privacy.

The Court unanimously stated that "The right to privacy is protected as an integral part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.". In doing so, it overruled an earlier Supreme Court decision in M.P. Sharma and Kharak Singh, where in the latter it was considered that the right to privacy was

[20] WRIT PETITION (CIVIL) NO. 494 OF 2012
[21] (1954) SCR 1077
[22] (1964) 1 SCR 332)

 [ISSN 2581-5369]

not recognized in the Indian constitution. The Hon'ble Supreme Court, while holding that the right to privacy was not absolute in nature, the judgement also gave an overview of the standard of judicial review that must be applied in cases of intrusion by the State in the privacy of an individual. It held that the right to privacy may be restricted where such invasion meets the three-fold requirement of

- ➔ legality, which postulates the existence of law;
- ➔ need, defined in terms of a legitimate state aim; and
- ➔ proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

Justice S.K Kaul added a fourth aspect to this test which mandated:

- ➔ procedural guarantees against abuse of such interference.

In addition to establishing the right to privacy as a fundamental right, the case also establishes the need to implement new data protection laws, expand the scope of privacy in the personal sphere, and promote privacy as an elemental value.

In Rayala M. Bhuvaneswari v. Nagaphomender Rayala,[23] The petitioner filed a divorce petition in the Court against his wife and to substantiate his case sought to produce a hard disc relating to the conversation of his wife recorded in the U.S. with others. She denied some portions of the conversation. The Court held that the act of tapping by the husband of conversation of his wife with others without her knowledge was illegal and amounted to infringement of her right to privacy under article 21 of the Constitution. The conversation cannot be admissible evidence under the Indian Evidence Act, 1872. The wife cannot be forced to undergo a voice test and then asked the expert to compare portions denied by her with her admitted voice. The husband was recording her conversation on telephone with her friends and parents in India without her knowledge. This is a clear infringement of rights under Article 21 of the Constitution of India.

Initially, the passing of the bill would result in a challenge to both the service provider and the enforcing authority alike with respect to the adaptation and enforcement of the act. In the long run, however, it will give rise to both advantageous and disadvantageous situations both of which should be in control. There is an inherent need for the Act to have the right balance so as to not tip to any side, maintain normalcy and serve the best interest of Individuals and their protection of their privacy.

[23] AIR 2008 AP 98

V. CONCLUSION & RECOMMENDATIONS

As the Personal Data Protection Bill in India is set to undergo major changes before being introduced to the winter session of the Parliament; The passing of the bill through the legislature is not a one-stop solution, it becomes a law that is always in need of constant updates through amendments. It has to keep up with trends in technology and rights of the citizens at large. Further, there should be no unwarranted delay in the implementation of law and setting up of agencies enabled through such law.

Though the implementation of the Personal Data Protection bill would have both positive and negative impact on business, the focus shall be on safeguarding national security as it is paramount for the government to enact such laws that protect its subjects.

The advancement of technology has enabled interaction at a global level and such technology does not exist in isolation. Similarly, the law is not to be limited to the local jurisdiction but it has to integrate with laws all around the globe, exchange ideas and discuss issues in a common forum.

*****

 [ISSN 2581-5369]