Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Data Privacy Laws in India

Ahmed Ziya Siddiqui[a]

[a]Dogra Law College, Jammu, India

Received 24 June 2022; *Accepted* 12 July 2022; *Published* 17 July 2022

Everything in the modern world is connected to the internet. Whenever data is provided to a service provider or a firm then there is a great risk of misuse of that data. The State[1] or a firm has no business knowing what we eat, what we search for, what we wear, and which religion we follow. Talking about accountability when we need any information from the government we use the Right to information act, 2005[2] but if an individual wants to save his privacy from an unnecessary intervention then he has the Right to privacy[3] granted by the constitution of India. This right can be used against the state, journalists, and even our neighbours but that doesn't mean it is absolute there are reasonable restrictions. Talking about data privacy online we need to make a comprehensive law, which should deal with the diverse aspects of data security as the right to privacy or intellectual rights this will reduce the happenings of data theft or unauthorised access and it will attract more and more foreign firms/entities to our nation, which would be a boost to our nation's IT industry.

Keywords: *state, government, privacy, right to information, right to privacy, constitution, data privacy.*

INTRODUCTION

There are things on the internet we quite don't understand yet, such as the Dark web, while we are still figuring the internet out we can say Data privacy on the internet is a hoax. Before we

[1] Constitution of India, 1950, art.12
[2] Right to Information Act, 2005
[3] Anusha Misra, 'Different aspects of Right to Privacy under Article 21' (*IPleaders*, 6 December 2021) <https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/> accessed 22 June 2022

go into data privacy on the internet in India we should know about the history of privacy in India through Landmark judgements which play an important role in the current data privacy debate in India.

- In the case of***. P. Sharma and Others v Satish Chandra***[4]*,* the court held that "for the security of the State was provided overriding powers of search and seizure. The court further said that in the Indian Constitution, there is no mention of a right to privacy.
- In the case of ***Kharak Singh v State of Uttar Pradesh***[5]*,* the issue of state surveillance as against the right to privacy was brought before the court. The judge bench held that "Domiciliary visits were unconstitutional but other regulations such as suspicion and tracking were deemed valid. The court also said that the right to movement under article 19(1)(D)[6] infringes with physical restriction." Justice Subba Rao was of a different opinion from the other judges and quoted a statement that changed data privacy in India for the future he said "Anybody can enjoy the freedom of movement anywhere for personal purposes, if the movement is being tracked then how free is it?"
- In the famous ***People's Union of Civil Liberties (PUCL) v Union of India***[7]**,** section 5(2)[8] of the Indian Telegraph Act, 1885 (the Act), which violates the right to privacy, was challenged as being unconstitutional by the People's Union of Civil Liberties (PUCL). This was in response to a report by the Central Bureau of Investigation (CBI) on the phone tapping of politicians that revealed several procedural errors in the phone tapping carried out by Mahanagar Telephone Nigam Limited (MTNL) at the direction of government officials. In this judgement, the Supreme Court ruled that phone tapping without the necessary precautions and without obeying the law violated people's fundamental right to privacy.

[4] *M. P. Sharma And Others v Satish Chandra* (1954), AIR 300
[5] *Kharak Singh v State of Uttar Pradesh* (1963), AIR 1295
[6] Constitution of India, 1950, art.19(1) (d)
[7] *People's Union of Civil Liberties (PUCL) v Union of India* AIR 1997, SC 568
[8] Indian Telegraph Act, 1885, s 5(2)

- In the landmark judgement of ***Justice K. S. Puttaswamy (Retd.) and Anr. v Union Of India***[9], The Bench's decision provided a fresh perspective on people's rights to privacy according to Articles 14, 19, and 21[10] of the Indian Constitution, the right to privacy was deemed to be a fundamental right. The Honourable Court upheld the Aadhaar Act and struck down the Act's unlawful provision. The Court ruled that Part III of the Constitution gives protection of privacy which is to be protected under, Article 21[11] i.e. Right to life and personal liberty, requires that the right to privacy of all individuals be maintained. The bench overruled the earlier landmark judgments of the Supreme Court such as Kharak Singh vs State of UP[12] and M.P Sharma vs Satish Chandra[13] in which the Right to Privacy was not held to be a Fundamental Right of the citizens under the Indian Constitution.

In this article we will talk about how the landscape of data privacy in India changed over time and what are the issues, meaning of data privacy, the need for protection of data, and the way forward.

PRIVACY OF DATA

Data privacy, in its broadest sense, refers to the freedom a person has to choose for themselves how, when, and to what extent others are given access to personal data. One's name, address, phone number, and online or offline conduct are examples of personal information. Just as someone may prefer to exclude persons from a private conversation, many online users wish to regulate or avoid some sort of personal data collecting.

The value of data privacy has grown along with Internet usage throughout time. To deliver services, websites, software, and social media platforms frequently need to gather and preserve personal data about users. However, some services and applications might be beyond what users had anticipated in terms of data collection and utilisation, giving users less privacy than they had expected. Other apps and platforms might not have proper security measures in

[9] J*ustice K. S. Puttaswamy (Retd.) and Anr. v Union of India* (2017) Writ Petition (Civil) No. 494/2012
[10] Constitution of India, 1950, art.14, art.19, and art.21
[11] Constitution of India, 1950, art.21
[12] Kharak Singh (n 5)
[13] M.P. Sharma (n 4)

place to protect the data they gather, which could lead to a data breach that breaches user privacy. Thus, Data protection is the process of protecting important information from corruption or loss. Data is the wide collection of information that is stored on a computer or on the web. The extent of data security increases as the quantity of data created and stored continues to grow at unparalleled rates.

According to the economic times, the number of internet users in India is expected to boost by 45% in the next 5 years to 900 million in 2025, as reported by IAMAI-Kantar ICUBE 2020 report. One of the important sources of gaining profits is the large collection of data about individuals online. You might have noticed how we get ads from shopping sites related to our recent searches. It is also a possibility that our personal data is not safe online and we may suffer an invasion of privacy Businesses, Governments, and political parties find it useful as it can be used as a tool by them to present ads in the most convincing ways to an individual online.

LAWS OF DATA PROTECTION AROUND THE GLOBE

- European Union (EU): The General Data Protection Regulation[14] (GDPR) is a legal body that sets procedures for the accumulation and processing of private information from people who live in the European Union (EU). The main objective of the General Data Protection Regulation (GDPR) is to give an individual authority over his/her data.
- United States of America: US has acts like the US Privacy Act, 1974[15], Gramm-Leach-Bliley Act[16], etc. to protect the personal digital data of individuals from invasion online.

INITIATIVES IN INDIA

Information Technology Act, (2000)[17]: This act ensures security against certain violations regarding data from computer systems. It has provisions that help in preventing the

[14] Jake Frankfield, 'General Data Protection Regulation (GDPR)' (*Investopedia*, 11 November 2020) <https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR)%20is%20a%20legal%20framework,the%20European%20Union%20(EU)> accessed 22 June 2022

[15] US Privacy Act, 1974

[16] Gramm-Leach-Bliley Act, 1999

[17] Information Technology Act, 2000

unauthorised use of computers, computer systems, and data stored in them. The Information Technology (IT) Act, 2000, which is amended from time to time, oversees all activities related to the use of computer system resources. It also covers all 'intermediaries' which play a role in the use of computer resources and digital records. The role of the intermediaries has been framed in 2011- The Information Technology (Intermediaries Guidelines) Rules, 2011, separately.

- Intermediaries according to the IT Act 2000: As defined in Section 2(1) (w)[18] of the IT Act 2000Intermediaries include telecom service providers, network service providers, social media, Internet service providers, and web hosting platforms it also includes search engines, online payment platforms, and auction sites, online shopping sites and even cyber cafes. It includes any individual who manages an electronic record on behalf of another.
- Importance of intermediaries under the law: Intermediaries are directed to maintain and control specified information in a particular way and format prescribed by the Centre for a certain duration of time. Violation of this provision is punishable with a term of three years in prison and a fine. The intermediary and any individual who is in charge of a computer resource should provide technical support by ensuring access to the resource involved. If there is a failure to provide this support, the individual may be punished with a prison term of up to seven years, along with a fine.
- Supreme courts stand on the IT act: In the case of ***Shreya Singhal v Union of India***[19], the Supreme Court interpreted the provision about intermediaries and said that the intermediaries are supposed to act only upon receiving actual knowledge of the passing of the court order asking them to specifically remove or disable access to certain material.

[18] Information Technology Act, 2000, s 2(1) (w)
[19] *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167/2012

ISSUES RELATED TO THE IT ACT

1. Every user might not understand the terms and conditions or the implications of giving consent. When a user gives consent the data aggregators have access to a wide range of personal data under these broad terms and conditions.
2. The IT Act does ensure data security but does not put enough focus on the privacy of data. While entities take measures to protect data, they don't have strong rules that respect users' preferences on how her private data should be accessed.
3. Provisions regarding data protection under the IT Act do not have any authority over the government agencies. This shows that governments are storing large amounts of personal data and forms an enormous void for data protection.
4. This act is becoming obsolete as it was legislated in 2000 and further amended in 2008 whereas the technology has advanced a lot since then digitally. Thus, the current data protection authority seems ineffective in handling threats arising from new developments in data processing technology.

PERSONAL DATA PROTECTION BILL (2019)[20]

This bill was first introduced to the Parliament in 2019 and was referred to the Joint Parliamentary Committee for examination at the time. It was drafted after a landmark Supreme Court verdict that declared 'Right to Privacy' a fundamental right in the famous ***Puttaswamy judgement***[21] in August 2017. It is also referred to as the "Privacy Bill" and plans to safeguard individual rights by handling the accumulation, processing, and movement of personal data, which can be used to identify the individual. The Bill is itself progressive legislation on how various corporations and institutions use the Digital data of an individual inside India. Through this bill, we may see a massive and meaningful modification to personal data protection in India. The proposed methodology that the bill seeks to implement is as follows.

[20] Personal Data Protection Bill, 2019
[21] Justice K. S. Puttaswamy (Retd.) and Anr. (n 9)

- This bill will help define roles. The Bill has such a framework that it will help codify relationships between Corporations, states, and Individuals as one between Individuals whose information is being collected and individuals who are processing the data so that privacy is guarded by arrangement. Also, the Bill aims to apply the data protection regime to both private and Government commodities across all sectors.
- This bill Ensures Data Privacy. The Bill ensures that data principles will preserve security to protect digital personal data and also fulfill a mandatory set of data protection guidelines and accountability and transparency measures. Thus it provides Scrutiny over these entities and upholds users' interests and privacy.
- The bill Puts emphasis on the Rights of the Citizens over their private data and ways to exercise those rights. For example, an individual will be able to acquire details about the kind of private data that a commodity has about them and how the commodity is using that data.
- The bill seeks to establish a Regulator. A powerful and independent regulator is known as the Data Protection Authority (DPA). It will scrutinize and overlook the activities of data processing and ensure their compliance with the regime. More importantly, the Data Protection Authority (DPA) will also act as a redressal portal through which users can bring action against the entities when they do not comply with their obligations.

Issues related to the bill

Some provisions in the bill question the effectiveness of the regime. These could contradict the main objectives of the bill by giving an edge to the government agencies and diluting user data safeguards.

There is a Scope for Loopholes, for instance, under clause 35, any government agency can be exempted by the Centre from complying with the Bill. With this Government agencies will get the power to process data without following any safeguard norms under the bill. This will create severe privacy risks for users and will make them feel that their data is not really secure.

The concept of Consent may get compromised. Users may find it difficult to implement various safeguards of data protection such as remedies and rights in the bill. For instance,

there are threats of legal consequence for users who revoke their consent for the data processing. This means the users will be under constant fear of legal consequences even if they want to opt out of a data processing activity.

CONCLUSION

The Bill creates two universes, one for the private sector where it would apply strictly and one for the Government and its agencies where it has some exemption and escapes. This bill provides immunities to the 'state' and its agencies, which is outside the legal authority and contrary to the Fundamental Right to privacy as laid down in ***Puttaswamy Judgment***[22]. Clause 35 of the bill is open to being misused by the government as it gives them unqualified powers. There should be Social audits that could keep a check on activities of processing data and will help maintain the integrity of private data. Protecting data from the very institution that creates it, including the political and administrative leadership, should be a key component of our data policy.

For public data to be genuinely relevant, an independent mechanism of review and verification is required, especially when the data is strongly related to people's access to crucial public services. Since it cannot be independently evaluated by a body for data protection, the promise of privacy preservation through anonymization methods in this scenario offers little hope. The Data Protection Law needs to be put into action right away and effectively in these situations. Data is a significant resource in the current digital era that shouldn't be left unregulated. In light of this, India should establish a strong data protection regime. In conclusion, it is time for the Personal Data Protection Bill, 2019, to undergo the necessary revisions. It must be rewritten with a focus on user rights and a strong emphasis on privacy for users. To safeguard these rights, a privacy commission would have to be created. While enhancing access to information, the government would also need to preserve the privacy of its residents. Additionally, given that recent technological advancements have the potential to render the law obsolete, it is also necessary to address these advancements.

[22] *Ibid*