Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Evolution of Data Privacy Regime in India

Apoorva[a]

[a]Faculty of Law, University of Delhi, Delhi, India

Received 19 February 2023; *Accepted* 07 March 2023; *Published* 11 March 2023

Debates over data privacy have gained momentum since Europen Union passed its data protection law in 2014. It has inspired other countries to establish similar data protection laws. With the rise in technology, several concerns associated with data privacy have evolved. Private entities and governments are deeply involved in data collection for their vested interests. Thus, individuals must be aware of the importance of data privacy in the 21st century to prevent the misuse of their data. At the same time, the need of the hour is that India enacts a comprehensive data privacy framework that can deal with all the issues and concerns surrounding data privacy, such as informed consent, data localization, the right to be forgotten, and so on. The present paper traces the journey of the status of the right to privacy and data privacy in India through various case laws as well as existing statutes. It also analyses challenges in the current legislative framework relating to data privacy.

Keywords: *data privacy, personal data, consent, right to be forgotten.*

INTRODUCTION

In modern times, we are surrounded by data. It plays an enormous role in our everyday lives. For example, when we search for something on Google or while entering our card details for online shopping, it all adds to the vast pool of collective data. However, in this age of the digital economy, data has become a commodity. Data brokers collect the personal information of

individuals, create an in-depth profile by processing them and sell them to advertisers. Thus, it has become a massive business worth roughly US$ 200 Billion[1]. The collection of data is not just limited to business. Governments across the world are involved in mass surveillance of their citizens in the name of welfare purposes. It also has become a tool to spy on other countries. Among all these, the individuals are, ultimately, the sufferers. Their privacy is being jeopardized, even without their knowledge and consent. Thus, a need arises to govern the collation, access, analysis, processing, and use of an individual's personal information by a third party.

PRIVACY: MEANING

The expression 'privacy' means the state of being free from interference in one's personal life and affairs. The right to be let alone by others is an important element of privacy. It does not mean that the person is withdrawing from society. It is an expectation that society will not interfere in the choices made by him as long as it does not harm others. At times, two competing but equally important freedoms come in conflict with each other: the right to free speech and expression and the right to privacy. One person's right to be informed, derived from the right to free speech, may violate another person's right to privacy. Thus, the law of privacy aims to balance and harmonize these competing freedoms. In Mr. X v Hospital Z's[2] case, the petitioner filed a case of the violation of his right to privacy on the ground that the hospital informed his fiance that he is HIV positive due to which his marriage was called off. The court held that the right to privacy is not infringed on the disclosure of certain information if it protects the rights and freedoms of others. In the instant case, the court held that the hospital was validly justified in disclosing the petitioner's HIV status because his fiance has the right to be informed, who otherwise would have contracted such a deadly disease. The privacy claim is derived from two sources:

[1] Shimon Brathwaite, 'What does a data broker do?' (*Security Made Simple*, 1 February 2023) <https://www.securitymadesimple.org/cybersecurity-blog/what-does-a-data-broker-do > accessed 17 February 2023

[2] *Mr. 'X' v Hospital 'Z'* Civil Appeal 4641/1998

- The Common law principle of tort where an individual can claim damages for unlawful intrusion in his privacy by another person;
- Constitutional law wherein an individual is constitutionally protected against unlawful interference from the State, implicitly guaranteed under the Right to life and personal liberty under Article 21 of the constitution.[3]

EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

Under the Indian constitution, we do not find any express mention of the right to privacy. The first attempt to include the right to privacy as one of the Fundamental Rights of the Constitution of India came from the Constituent Assembly debates. Few members introduced proposals to recognize the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. The Fourth Amendment Rights guaranteed under the American Constitution inspired them. However, all such proposals got defeated on the grounds of being restrictive on the investigative powers of the police authorities.

MP Sharma v Satish Chandra (1954)[4] was one of the earliest cases which dealt with the issue of the right to privacy. It challenged the constitutional validity of search and seizures on the ground that it infringes on the right to privacy. The court dismissed this contention and ruled that since the Constitution makers did not explicitly recognize the right to privacy within the Fundamental Rights, the power of searches and seizures can not be curtailed on this ground. Similarly, in Kharak Singh v State of Uttar Pradesh (1962)[5], the Supreme Court held that the right to privacy is not guaranteed under the Indian Constitution. However, the dissenting opinion of Justice Subbarao recognized the right to privacy as a crucial element of personal liberty.

In Govind v State of Madhya Pradesh[6], the Court for the first time gave limited recognition to the right to privacy. The privacy claims may be accepted subject to the laws with the compelling public interest. R. Rajagopal v State of Tamil Nadu (1994)[7], also known as the 'Auto Shankar

[3] *R. Rajagopal v State of TN* (1994) SCC (6) 632
[4] *M. P. Sharma and Others v Satish Chandra, District Magistrate, Delhi & Ors* (1954) AIR 300
[5] *Kharak Singh v The State of UP & Ors* (1963) AIR 1295
[6] *Govind v State of Madhya Pradesh & Anr* (1975) AIR 1378
[7] R. Rajagopal (n 3)

case', was the first case where the court considered the question of the right to privacy in the backdrop of the freedom of the press. In this case, the issue was whether a publisher has a right to publish another person's autobiography without his consent under the freedom of the press protected by Article 19 and whether it violates his right to privacy. The court observed that a person has a right to safeguard his privacy and no person has a right to publish anything related to his life. But this is subject to the exception that when the matter is already in the public record, the right to privacy does not subsist. Hence, no consent of the person concerned is required as far as the publication is based on public record.

Justice K.S. Puttaswamy (Retd.) v Union of India (2017)[8] is a landmark case wherein the nine judges bench considered all the judgments to date to decide the question about privacy vis-a-vis fundamental rights. It held that the right to privacy is a natural right, inherent in a human being. Safeguarding the privacy of an individual is important as it is fundamental to human dignity. Privacy has two aspects: negative and positive. In its negative aspect, the State is restrained from interfering with an individual's life and personal liberty. The positive aspect directs the State to take all necessary actions possible that can protect one's privacy. The judges also touched upon the concept of "reasonable expectation of privacy" which was first discussed in the American case Katz v United States[9], and adopted in India by Justice Lahoti in Distt. Registrar & Collector v Canara Bank[10]. This concept means that an individual can not expect the same level of privacy in all places. His expectation vis-a-vis privacy must be reasonable, depending on whether he is in a private or public space. In the most intimate space, an individual has the right to be let alone, free from societal expectations and judgments. However, it does not mean that a person has no right to privacy if he is in a public place. At the same time, the court laid down that the right to privacy is qualified. It is dependent on the reasonable restrictions provided by a law, which must be just, fair, and reasonable. The court laid down three parameters on which a law interfering with the right to privacy must be tested to ascertain its reasonableness:

[8] *Justice K.S.Puttaswamy (Retd) v Union of India and Ors* WP (Civil) No 494/2012
[9] *Katz v United States* [1967] 389 US 347
[10] *Distt. Registrar & Collector v Canara Bank* Civil Appeal 6350-6374/1997

- Legality, requiring the existence of law, since the right to life and liberty guaranteed under Article 21 can not be taken away except according to a procedure established by law;
- Need, necessitating that the purpose of the law restricting privacy must be legitimate, reasonable, and not arbitrary, as required under Article 14;
- Proportionality, ensuring that the object sought to be achieved must be proportional to the means adopted to achieve them.

On this basis, the court overruled the judgment of the MP Sharma case fully and the Kharak Singh case partially wherein it decided that the right to privacy is not part of any fundamental rights.

DATA PRIVACY

Puttaswamy's case[11] recognized various facets of privacy, including informational privacy. It means that every individual should have the right to control the dissemination of information personal to him. A person may want to limit access to his affairs relating to his private life. Unauthorized access and use of such information may violate his informational privacy. It is also known as data privacy or data protection. If a person is identifiable through any information related to him collected by a third party, then it refers to his data. Businesses gather huge amounts of data for products, services, advertising, marketing, and even developing artificial intelligence-based applications. It poses a massive risk of a breach in people's data privacy. Therefore, building a robust data privacy regime is essential because people need to trust that their data will not be misused so that they can engage online and utilize the full benefits of digital technologies. One of the earliest regulations for data privacy came from the Organization for Economic Cooperation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. It laid down various non-binding principles like:

- Personal data collection should be fair and just;

[11] *Justice K.S.Puttaswamy (Retd)* (n 8)

- Disclosure of such personal data collected should be with the consent of the individual concerned as well as by the authority of law;
- The purposes of personal data collection should be specified and should be relevant to the purposes for which it is utilized.

A significant transformation in the existing data privacy laws occurred with the introduction of the General Data Protection Regulation (GDPR) in 2018 by the European Union (EU), replacing the earlier Directive 96/46/EC. It lays down a comprehensive framework for regulating data privacy within the EU. It is one of the strictest data privacy laws applicable to even those companies ('data processors') that do not operate within the EU, the simple condition being that they process personal data relating to a citizen or resident in the EU. It gives several rights to 'data subjects' (the person whose data is processed) so that their data privacy is effectively safeguarded like the right to be informed, right of access, right of rectification, right to erasure, etc. Also, the penalty for violation of GDPR rules is severe. Data principles under GDPR provide fairness, transparency, and lawfulness in the processing of personal data, data must not be processed for unauthorized purposes, it must protect the confidentiality of data subjects, and so on.

DATA PRIVACY FRAMEWORK IN INDIA

India does not have single comprehensive legislation dealing with data privacy. There are numerous sectoral rules and regulations, but they are fragmented. The Information Technology Act, of 2000[12], including all its amendments (hereafter referred to as 'IT Act'), attempted to address this issue. Section 43A[13] of the IT Act provides compensation for negligent handling of personal data. If a company possessing and handling any sensitive personal data or information (SPDI) is negligent in implementing and maintaining reasonable security practices and procedures, which causes wrongful losses or wrongful gain to any person, then it is liable to pay damages by way of compensation to the affected person.[14] Section 72A of the IT Act stipulates

[12] Information Technology Act 2000
[13] Information Technology Act 2000, s 43A
[14] Information Technology (Amendment) Act 2008, s 43A

criminal punishment if an intermediary discloses to any third party the personal data of a person without his consent or in a breach of a lawful contract.[15]

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") lays down minimum data protection standards for sensitive personal data. Rule 3 defines "sensitive personal data or information" as including passwords, financial information, sexual orientation, medical records and history, biometric information, and any such information provided to or received by the companies processing such data. Rule 4 mandates companies to publish a privacy policy on their website regarding sensitive information collected under rule 3, the purpose of such collection, and reasonable security practices and procedures. Rule 5 provides that companies shall obtain consent in writing before collecting such information. Prior consent is required for the disclosure of sensitive personal information to third parties (Rule 6)[16].

ANALYSIS OF LIMITATIONS OF EXISTING DATA PRIVACY FRAMEWORK

The existing laws and rules governing data privacy are vague and inadequate. It does not cover all dimensions of data privacy in the context of rapidly changing technologies. Banking, telecommunications, insurance, and other sectors have separate rules governing sensitive personal information. All these fragmented laws and regulations must be consolidated to create comprehensive privacy legislation. Section 43A does not apply to the public sector. It only applies to the body corporate. The government has been launching various data-driven schemes such as the AADHAAR, DigiLocker, and National Population Register that require collecting a vast amount of sensitive personal data like biometric information. There is a need for regulation of such sensitive information, otherwise, it may have serious privacy breach concerns. The definition of sensitive personal data or information is limited. It does not cover electronic communication like emails, browsing, chats, or social media. With the growing nature of data, there is the evolution of new data sources and forms, rendering the existing privacy framework

[15] Information Technology (Amendment) Act 2008, s 72A
[16] Ministry of Communications and Information Technology (Department of Information Technology) Notification 2011

ineffective. The requirement of prior written consent under the Data Protection Rules is not enough. Consent must be informed, explicit, freely given, and include other modes of obtaining it. Moreover, as the Data Protection Rules apply only to sensitive personal data and information, the precondition of consent narrows down.

LATEST DEVELOPMENTS IN DATA PROTECTION BILLS

In 2017, the Ministry of Electronics and Information Technology constituted a committee of experts on a data protection framework, under the chairmanship of Justice B.N. Srikrishna. Based on the recommendations of its report, a draft Personal Data Protection Bill, 2019 was introduced in Parliament. It introduced the terms Data Principals, Data Fiduciaries, and Data Processors. Individuals whose data is processed are data principals and data fiduciaries are entities processing such data. Data processors are organizations processing data on behalf of data fiduciaries. It applies to the government, private actors incorporated in India, or any individual or group of persons processing personal data within India. It is also applicable to data fiduciaries or data processors incorporated abroad if they are involved in data processing relating to any business activity in India, or any venture of providing goods or services to data principles in India. However, it does not apply to anonymized data, that is, data that has undergone the process of anonymization after which a person can not be identified by such data, except as provided under Section 91.[17] This bill was withdrawn owing to widespread criticism from various stakeholders. The tech companies dissented against the requirement of data localization provision. Data localization norms mandate storing of all personal data of Indians within India, and various safeguards to be followed for transferring data abroad such as consent of data principals, compliance with the laws, publishing privacy policy, etc.

The Digital Personal Data Protection Bill, of 2022 replaced the earlier one due to these issues. It applies to personal data collected online as well as data collected offline that is digitized. It introduces the concept of deemed consent wherein the data processor voluntarily gives consent and is reasonably expected to give consent for providing personal data to the data fiduciary. A

[17] Personal Data Protection Bill 2019, s 91

deemed consent also includes situations such as medical emergencies, employment purposes, court orders, or the public interest. Furthermore, the Bill gives the data principals the right to correct and erasure personal data if the purpose of processing data has ceased to exist.[18]

RIGHT TO BE FORGOTTEN (RTBF)

The right to be forgotten means the right of an individual to have his personal information removed from websites, search engines, databases, and every other public platform that hosts such information. It is a key component of one's right to privacy. The reason is that the right to control one's data is meaningless if he cannot erase his personal information which is no longer required. However, this is not an absolute right. A person can not have his personal information removed from public platforms whenever he demands it. It depends on situations, like when personal information is not required anymore for the purpose it was accessed by data fiduciaries. Moreover, his request for the removal of personal data can be denied in certain situations, viz when it conflicts with free speech, or it is to be used as a legal defense, in public health, medical emergency, or in the larger public interest. Otherwise, it would amount to rewriting one's history.

This concept gained popularity from the case Google Spain SL v AEPD and Mario Costeja Gonzalez.[19] The petitioner Mario Costeja Gonzalez prayed for the removal of the information relating to an attachment and garnishment action published against him in a newspaper in 1998 on the ground that the case is already settled. But it still shows up on Google searches which damages his reputation. The European Union Court held that a search engine can be directed to remove the personal information of an individual that is published by third-party websites to safeguard his right to privacy. Following this judgment, this concept of RTBF was incorporated under Article 17 of GDPR as the right to erasure.

In India, there is no provision for RTBF in the current legislative framework. Attempts have been made to include it within several data protection bills but they have not become laws. Due to

[18] Digital Personal Data Protection Bill 2022
[19] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] C-131/12

the absence of a legislative framework governing RTBF, several High Courts of India have given conflicting judgments on the same. In Jorawer Singh Mundy v Union of India and Ors[20], the petitioner accused under the Narcotic Drugs and Psychotropic Substances Act, 1985[21] was acquitted by the Trial Court and the High Court. Still, that particular case showed up in online searches which tarnished his reputation and hampered his job prospects. The petitioner filed a writ petition for the deletion of that case from websites like Google and Indian Kanoon. The High Court of Delhi held that the petitioner is entitled to interim relief for removal of the said judgment from online platforms till the time the case is pending in the Supreme Court, because of the irreparable harm caused to his social life and career prospects. However, in a similar case, the High Court of Madras in Karthick Theodre v The Registrar General[22] dismissed the petitioner's right to be forgotten. The court held that this right could be effectively enforced in India if data privacy legislation recognizing such a right was in place. In X v Union of India[23], the petitioner's photos were taken from her social media accounts and illicitly posted on pornographic websites without her consent, despite having the requisite privacy settings. The High Court of Delhi held that unauthorized access to photographs from a person's social media accounts and posting them on pornographic websites, despite them not being obscene or offensive, amounts to a breach of her privacy, guaranteed under Article 21 of the Constitution. In such cases, the court may direct the necessary parties to remove the offending content from all the websites as far as possible.

CONCLUSION

The collection of data is not going to be stopped shortly, rather data will be collected at unprecedented levels than ever. This poses a great risk to people's privacy being compromised. The need of the hour is that India establishes a comprehensive data protection law that addresses all the issues relating to data privacy that the modern world faces. India must develop effective tools, strategies, and policies to formulate a law that can balance the competing

[20] *Jorawer Singh Mundy @ Jorawar Singh Mundy v Union of India & Ors* WP (Civil) 3918/2021
[21] Narcotic Drugs and Psychotropic Substances Act 1985
[22] *Karthick Theodre v The Registrar General* WP (MD) No 12015/2021
[23] *X v Union of India & Ors* W P (Crl) 1082/2021

interests of individuals who want to safeguard their privacy and companies that wants to grow their business using modern technologies.