Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 3, 5785–5790

# Right To Privacy In India: The Technical And Legal Framework

Dr. G. Mallikarjun, B. Md. Irfan

*Asst. Professor of Law, Dept., of Law, Nalsar University of Law, Hyderabad.*
*[2]System Analyst, IT Dept, Nalsar University of Law, Hyderabad.*

**Abstract**

'Data Protection' and 'Privacy' of the individuals are inseparable and inalienable. If key data belonging to an individual or an organization is not secured and is easily accessible to the public, it raises concerns of intrusion of privacy. Thus**,** personal data of every individual should be protected and should not be made accessible to the public. Data protection is a method of legally safeguarding an individual's or any organization's information in the virtual world of communication and the internet. With the passage of the Information Technology Act of 2000 and a subsequent revision, India has officially recognised the need of data privacy protection. Considering that India's existing laws on data protection and other related issues, such as the IT Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Laws of 2011, fail to provide adequate remedies, the Personal Data Protection Bill 2019 was introduced in the Lok Sabha on December 11, 2019, and has since been passed. The privacy of the individual, in the present digital world, is continuously at stake on account of the various e-surveillance methods, interception of digital communication, and the collection of personal data in various forms at various stages by various agencies. Therefore, the author in this paper makes an attempt to highlight the issues like surveillance, censorship and the interception of digital communications and its effects on the right to privacy and to what extent the present Bill will protect the personal data and safeguard the privacy of the individual.

## Introduction:

### Right to Privacy vis-à-vis Protection of Personal Data:

Since personal information can be accessed by a variety of people and for a variety of purposes in the digital age, it is extremely difficult to maintain privacy and protect personal data. For example, by the state for surveillance or even by private business entities for the revenue generation.People's personal information, such as their name and contact information as well as their likes, dislikes, habits, and hobbies, as well as their medical and financial histories, are all publicly available on the internet, and companies like these take use of this to increase their profits. In addition to this information which is voluntarily put out on the internet, there are some other ways to access the personal data of an individual without the knowledge and the consent of the said individual using a number of techniques like data mining, clustering, geotagging and geocoding. The information which is collected can used to send unsolicited business advertisements or be used for their personal ends.

In fact, with the advent of the 21st century, with an increase in technological development, privacy concerns against new technologies seemed to multiply.As a result, it is possible to say that new technologies make personal data more accessible and communicative. Therefore, it is critical to have a powerful and reliable data protection regulatory framework in order to ensure consistency between innovation and the preservation of privacy.. When it comes to personal data, there are always tensions between what should be kept private and what should be made public. Privacy is one of those legal

concepts that can take on a wide variety of appearances depending on the context, the time of day, the issue under discussion, and even who is bringing the case.

**Principles of Data Protection**

As the amount of data being created and stored continues to expand at unprecedented rates, the need for data protection is becoming more critical. When it comes to data security, we're talking about preventing sensitive information from being lost, damaged, or accessed by unauthorized parties. In today's highly advanced and frantic new world, it is critical to save and retain all of your important data. Data is becoming more valuable as new technologies emerge and new use cases are established, resulting in a greater need to preserve and safeguard this information. Protecting data and making it accessible in any situation is the fundamental goal of information security measures. Both data backup and business continuity/disaster recovery are technically referred to as "data protection" (BCDR). It's becoming increasingly difficult to protect data in two ways: through acquisition and through management. We're talking about two distinct but intertwined concepts here: lifecycle and data management. Life cycle management is an automated procedure that moves critical information between online and offline storage. It's a complete approach for measuring, cataloguing and protecting information assets against operating and user errors, malware and viral attacks, system failures or breakdown and interruption.

**Data Storage and Protection: Technological Frame work**

Data backup plays an important role in ensuring that data continues to remain available. To this end, a number of storage technologies are available. These include the creation of a backup copy of a disk or an alternative tape based device whose purpose is to copy specific information to an offline storage device for storing it securely. Although this mechanism has the drawback of being time consuming and slow, it offers strong protection as it is portable and naturally available offline making it safe from network based attacks.

In addition to these methods however, an organization can use a technology known as a "mirror" which creates an "image" of a specific site or file so as to make it available in more than one location. In any case, the practice of data backup on the cloud is gaining increased acceptance and is now commonplace. Often, backup data is moved to a cloud-based repository or to a public cloud. Local discs and libraries can be replaced or protected data can be added to these backups. The process of creating data backups is an extremely important function to effective protect data. Current technological advancement has meant that backup has moved from an independent activity to an integrated component of other activities to conserve storage as well as reduce expenses. Modern backup data protection involves the use of a built-in system that adds or exchanges backups and protects against potential problems.[1]

In the current day and age, data is all pervasive and has become an indispensable component in almost every activity. Data is generated and shared as a consequence of most of our day to day activities including traveling, ordering food or even purchasing anything. This places a high value on this data which is not often recognized and several persons and organizations have found ways to utilize this data which highlights the need for data protection and digital privacy.

**Right to Privacy in India: The Legal Framework**

Constitutional texts across the world provide for privacy protection in one form or the other. The most notable examples of these are the US Constitution's Fourth Amendment,[2]On the International Covenant on Civil and Political Rights and on the European Covenant on Civil and Political Rights (Article 17 and Article 8).

[1]*Ibid.*
[2]The Constitution of the United States. amend. IV.

Human Rights.[3] Even at its lowest point in American constitutional jurisprudence, the right to privacy was said to be a part of the Bill of Rights' penumbra, if not an integral part or a substantive right on its own.[4]

In India, however, privacy jurisprudence has taken a different line of evolution altogether. While it has been dealt with in a wide variety of constitutional as well as sub constitutional contexts [5], the fact remains that on its own, privacy is almost alien to the Indian judicial imagination. While other jurisdictions can claim to source the right to privacy from a concrete text, India cannot. The best way out of this quagmire so far has been an expansive interpretation of Article 21, which mandates that the right to life and personal liberty can only be taken away by a lawfully established procedure. Indeed, Indian law has a fairly rich history of attempting to create a somewhat robust right to privacy from Article 21. The first real "privacy" cases in Indian constitutional law relate to the police surveillance of individuals with criminal records ("history sheeters"). In **Kharak Singh v. State of Uttar Pradesh**,[6] the petitioner claimed that police surveillance, and specifically night-time house visits, of history sheeters was violative of Article 21. Citing American jurisprudence extensively, the Supreme Court held that a right of privacy was implicit in Article 21's guarantee of personal liberty.

Next in line was **Gobind v. State of Madhya Pradesh**,[7] in which the Supreme Court encountered another instance of visitation and harassment by the police against a history sheeter. Gobind is an important case to understand the Article 21and how it articulates the right to privacy in the context of use of internet. This is because the ruling in Gobind directly challenges the foundations of the most invasive elements of India's national security apparatus. One such feature is the retention of communications metadata by service providers for a period of two years.[8] Another is Netra, a mass surveillance programme that gives security agencies the ability to collect and store all communications data (as well as metadata) flowing through India's internet infrastructure. Gobind, by following the tradition of Kharak Singh before it, laid down strict limitations upon the targeted surveillance of an individual by police officers. If targeted surveillance of an individual based on a probable cause or a criminal record requires such standards to be followed, there can be no question that even more stringent due process constraints must be in place for the collection and storage of data en masse from every single internet user in the country.

Thus, at first glance, it would seem that Kharak Singh and Gobind have established a right to privacy within the Indian constitution through the Article 21 route. However, my thesis is that such a right, even if it does exist, isn't nearly robust enough to stand the test that pervasive internet surveillance poses. I argue that this is because of the inherent limitations that plague the Article 21 articulation of the right to privacy, and that these limitations have been highlighted by the manner in which the Supreme Court has treated the ways in which the right to privacy can be infringed upon by the state.

The biggest limitation of an Article 21 right to privacy is that the provision and its jurisprudence are fundamentally at odds with the framework of the privacy debate. In today's world, privacy has been couched as an individual, collective or human right that states have an obligation to protect, except when faced with grave national security concerns. The privacy v. security debate is of such a nature that states, when violating the privacy of their

[3] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 1950, art.8.
[4] *Griswold v. Connecticut*, 381 US 479 (1965).
[5] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 for example, discusses the right to privacy in the context of civil wrongs committed by private parties against one another, rather than in the context of constitutional commitments of a state towards its people.
[6] 1964 SCR (1) 332
[7] (1975) 2 SCC 148
[8] AnirudhRastogi, *Cyber Law: Law of Information Technology and Internet* 212 (LexisNexis 2014).

citizens, routinely get away with heavy-handed tactics in the name of the "national interest" (or some equally vague variant of the term).

The manner in which Article 21 has been en-capsuled has led to real consequences in the privacy context, where in the ability/power of state to restrict or abridge the privacy of citizen and the consequences thereof. In **Gobind vs. State of M.P.**,[9] the Supreme Court laid down the test of compelling state interest or compelling public interest. In theory, this was an attempt to borrow an American constitutional principle[10] and adapt it to the Indian context in order to emphasize that a "compelling" public interest required to take away an individual's privacy would be a higher threshold than the state interest or public interest thresholds present in Article 19(2) or Article 19(5). Further, the American doctrine of compelling state interest was accompanied by a requirement that any infringement upon the right be tailored as narrowly as possible. Thus, an overbroad measure (the monitoring of all internet traffic within the country, for instance) would immediately pose a constitutionality problem within this test.

**The Growing Need for Novel Policy**

India does not have a complete law that deals with data protection and privacy. Existing policies and regulations are, in fact, part of its core. These industry rules are a related provision of that IT Act, 2000 and thus provide the rules governing the collection process, the use of such confidential information and sensitive confidential information or the date by the companies' organization within India.

The government is regulating the development of some comprehensive laws that help regulate privacy and data protection. Additional efforts are needed in the process initiated by a team formed by a privacy expert led by Justice A.P. Shah, a judge of the Delhi High Court, presented his full report on October 16, 2012.

The government then appointed a single expert commission under the leadership of Justice Srikrishna who was the previous judge of the Last Resort in India, reviewing issues related to data retention in India and specific recommendations needed to benefit the Central Government on the principles to be considered for data protection in India in the framework of the proposed data protection bill.

There are other important legal provisions that focus on and regulate privacy protection and the provision of personal data

However, data protection in India was achieved through the provision under various laws and regulations apart from provisions of the constitution,[11] such as the following:

• **Information Technology Act, 2000 -** (aIt is illegal for companies that deal with sensitive personal information, such as credit card numbers or health records, to profit improperly or unfairly from that data. In accordance with Section 72-A, any service provider that discloses personal information about a person without their consent or in violation of a legally binding contract is subject to criminal prosecution.

• **Telegraph Act, 1885** –The Central Government of India and the Provincial Governments of India are governed by Sections 5 and 24 of the Indian Constitution, respectively.

• **Telegraph Regulations, 1951-** For the issuance of disconnection orders, Law 419-A sets up specific processes and criteria.

• **Unlawful Activities Prevention Act, 1967 -** If the responder is not given a copy of the restraining order, the illegal communication cannot be used as evidence.

• **Access to Information Act, 2005 –** According to Section 8 (1 (j) of the Privacy Act, personal information that is not related to any public

[9] Su*pra* n.12.

[10] *See, eg.,Grutter v. Bollinger*, 539 US 306 (2003).

[11] Constitutional protection in respect of the right to privacy as a fundamental right under Part III of the Constitution as opined in the case of *Justice K.S. Puttaswamy vs. Union of India* (2017) 10 SCC 1.

service or interest, or that could result in illegal access to any privacy, is exempt from disclosure..

**• Postal Act, 1898 –**

Section 26 governs the acceptance of postal products by the Indian government at both the federal and provincial levels.

**• Criminal Procedure Code, 1973 -** Section 91 regulates access to stored content.

**• Wireless Telegraphy Act, 1933 -** Wireless networks that are established, maintained or operated for the aim of blocking, monitoring, or intercepting communication are illegal under Section 3 of the Act.

**Locating the Data Protection Bill in the Context of Privacy Considerations**

The PDP Bill has a big impact on how personal information about Indian citizens is collected and used. Because there are no rules for private or public businesses in India today. Section 3 (28) of the Bill says that "personal data" refers to information that can be used to identify or contact a person who can be found. People can use this definition to describe data that is online and off-line, as well as any combination of these characteristics with other information. The Bill is very important because it defines personal data very well.

If the GDPR and other privacy rules have made a big difference in how the Data Protection Bill, 2019, is written, that's what it looks like.

In the 1970s, there was a lot more privacy than there is now. That's why the rules aren't up to date. In the 1970s, a report called "Records, Computers, and Citizens' Rights" was written to deal with the rapid technological changes. Organization for Economic Co-operation and Development rules on protecting privacy have also been put into place for some of the most important suggestions on how to protect people's privacy, such as not collecting data without permission, making data processing visible, and giving people the right to change their data.

**Significant Features of the Bill**

Data collection and usage will be governed by this legislation. Bill proposes to establish Data Protection Authority in addition to creating rights and obligations in relation to processing personal data (DPA). The DPA is responsible for drafting and enforcing the rules of the game. The bill also provides the DPA a mandate to enforce the law and gives the central government more power to regulate itself.

A bill's most crucial feature is that it applies to all businesses in India, unless specifically exempted by law. Any business that uses automated data collection methods will be affected by this. Based on income, portable data volume, and data collecting objectives, (DPA will be able to define small firms). This may contain not only technological firms and e-commerce platforms, but also real estate companies, banking contacts, vehicle dealers, hotels, and restaurants. etc.. etc. Consent must be free, informed, and direct, with the option to cancel it; this is the most critical condition. It is illegal to process personal information without the express authorization of the data subject. In addition, the Bill says that such data can only be used "with explicit permission." If you want to collect data from someone, you must give them enough information about what data is being collected, why it is being collected, and what their rights and responsibilities as "data trustees" are so that they can give their consent. This information must be provided to the person being tracked (the "data principal").

There are several exceptions to the notification requirement, such as the provision of emergency medical or health care services in the event of an epidemic, a disaster, or a breakdown of public order. Similar exemptions to permit requirements, including credit rating and the recovery of pending debt, may also be granted by regulations.

A fiduciary duty only comes into play when the information is needed to reach the goal for which it was gathered, and in full compliance with all applicable laws and rules. So, there are rules about how and when data can be used and

stored, so that's why. In addition, businesses that use privacy by design must use business processes that can predict and avoid harm to customers, comply with transparency requirements that include measures to stop data misuse, and make sure that data isn't used without permission, as well as meet other requirements.

Even the panel that came up with ideas for a 2019 bill on intermediary responsibility has looked at it, too. Those who work for a company are being held accountable for what they do under the Bill and other laws. For example, the Intermediary Guidelines and Digital Media Ethics Code of 2021 say that media publishers and OTT providers should be in charge of the content they put on the internet. Consumer Protection (Amendment) Rules of 2021 say that e-commerce intermediaries will have to pay for what other people do when they sell and buy things from them. Under Section 79 of the Information Technology Act, they were previously free from liability for things like web hosting services and search engines, as well as e-commerce platforms and telecom service providers. But because of this new law, they could now be held liable for things like this.

There are questions about whether people can say what they want and if they can be censored. If you want to make sure that third parties who have a lot of information don't use it in a bad way, this could be a good start.

**Conclusion:**

In this present digital world, the need of protecting the individual data is very much needed. Thus, the efforts made in the Data Protection Bill are commendable in striving to establish a data protection system in India. However, some of the provisions under the Bill are not in consonance with the fundamental right to privacy. The Bill, in the present form, does not provide much protection to protect the right to privacy. Interestingly, the Bill is in its strict sense would not be able to provide the proper system of checks and balances in monitoring and protecting the data. Therefore, there is a need to recognize the privacy of citizens as the ultimate goal of data protection law.

In the end, any law is as good as the remedy it provides. None of the existing laws mentioned above provide a legal remedy for correcting unlawful state actions such as illegal intrusion / surveillance into a person’s data and this aspect must be addressed at the earliest. While there seems to be growing regulation of the online world, protection of the data of individuals must be prioritized and its misuse must be prevented without compromising on the freedom of speech.