IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE PRIVACY & DATA PROTECTION CONUNDRUM IN INDIA: CONTEXT &CONCERNS

[1]ShubhankKhare, [2]Kamlesh Jain

[1]Assistant Professor, [2]Assistant Professor

[1]Department of Law

[1]Prestige Institute of Management and Research, Indore, Madhya Pradesh

Abstract:Data is the new oil for the 21st century. With everything growing us at a rapid space, with everything using some amount of data or information, the choice of making information selectively disclosable becomes pertinent. Right to privacy or right to be forgotten is one such privilege that enables that choice. The extension of right to privacy is data protection. Data protection is a mechanism to protect the privilege of privacy that has been guaranteed to every person in India by virtue of SC's decision in *Puttaswamy case* which held that right to privacy is an inherent right under Article 21 which relates to right to life and personal liberty. The ultimate law of the nation in India is the Constitution. Constitution of India is an ever-evolving document, adaptive to the changing conditions of the world around it. This is an unarguable reality that cannot be refuted. In India, there is particularly no specific legislation that relates with privacy or data protection in comprehensive manner. The existing framework is through combination of various pre-existing legislations such as Information Technology Act, 2000. However, the amendment to the Act in 2008 didn't effectively deal with the issue of data protection as whole but in bits and pieces. The Personal Data Protection Bill, 2019 based upon EU's General Data Protection Regulation 2018 is a step in positive direction. However, there are various concerns such as blanket exception to state actors that hasn't been addressed. This article shall deal with the concerns of the privacy and data protection discourse in India with the context of recent changes in the privacy jurisprudence.

Keywords:Data, Privacy, Data Protection, Personal Data Protection Bill, General Data Protection Regulation

INTRODUCTION

Data collecting for several purposes has grown commonplace in recent years. Google collects data from people who go to the right websites and learn something new. Facebook also collects data and allows people to communicate and share it. This isn't just a one-person problem. Users' economic habits may be gleaned from their data, which can then be utilized by businesses to better their operations. As a matter of course, firms must implement data protection standards and implementations.

The idea of personal privacy is not a relatively new one in India. The ancient Indian knowledge system, which is based on all of the literature from Upanishad, mandates meditation, which must be done in an environment free from any interruption from the outside world. Both the estates as well as the 'Arthashastra' demonstrate a sufficient care and reverence for the individual's privacy right.[1] The Ramayana

[1]Anjali Kumari, "Need of Privacy Law in India" *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/need-of-privacy-law-in-india/ (last visited June 10, 2022).

as well as other great literatures grow in a specific way, and one of those ways is how they describe the usage of curtains. Everyone has a private existence, which they should keep to themselves since others would think they are insane if they share it.

The ultimate law of the nation in India is the Constitution. Constitution of India is an ever-evolving document, adaptive to the changing conditions of the world around it. This is an unarguable reality that cannot be refuted.

In addition to a number of other basic rights, it acknowledges the privacy rights to be inherent of the many rights that fall within the purview of Article 21. Pursuant to Article 21, *"no individual shall be deprived of his life and personal liberty except according to the method prescribed by law,"* which means that no one may be killed or have their freedom taken away without following the rules. Since the right to privacy is connected to an individual's life and liberty, Article 21 guarantees protection for this fundamental human right.[2]

Article 21 of the Constitution guarantees a person's privacy right, also known as the right to be left alone, according to a decision made by the Supreme Court in the case *R. Rajagopal v. State of Tamil Nadu*[3], famously called the "Auto Shanker Case." In this case, the SC made it clear that this right exists. The privacy of an individual, their family, their education, their marriage, their children, and their unborn children is one of the many privileges that are given to a person.[4]

The idea of data protection is the most important aspect that is coextensively associated with the Right to Privacy. This relationship is extensive.[5] Since, in the modern day, a person is more likely to be found on the internet, in social media, and in cyberspace than even in his actual presence or rather existence, the relevance of data protection has become more significant and necessary. According to a Research, the advancement of legislation will be based solely on *Artificial Intelligence* (AI), which will bring more new obstacles and obstructions in the way of the Right to Privacy and Data Protection in India as well as the rest of the world, which will have a significant impact on the future of technology[6]. For example, the "*Digital Footprint*" of any moment is the precise reproduction of a person on the servers that may be retrieved from a backup for the purpose of law enforcement investigations.[7] We can see how technology can invade on your privacy and produce errors in your life.

Recently, the *Narcotics Control Bureau* (NCB) has been investigating many Indian celebrities on drug charges after retrieving their old deleted communications dating back three years. Nonetheless, since it was done by the Investigating Authorities, it was lawful; however, in all other situations, save for the voluntary

[2]SonamRawat, "Revisiting Right to Privacy in Indian context" *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/revisiting-right-to-privacy-in-indian-context/ (last visited June 10, 2022).
[3]1994 SCC (6) 632
[4]Vijay P Dalmia, "Data Protection Laws In India - Everything You Must Know - Data Protection - India" *Mondaq.com*, 2017*available at*: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (last visited June 10, 2022).
[5]Shiv Shankar Singh, "PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT," 53 *Journal of the Indian Law Institute* 663–77 (2011).
[6]Atul Singh, "DATA PROTECTION: INDIA IN THE INFORMATION AGE," 59 *Journal of the Indian Law Institute* 78–101 (2017).
[7]*Ibid.*

agreement, such an act amount to contravention of privacy right of a person, which from the year 2017 is considered as a fundamental right and is guaranteed by Constitution of India under Article 21.

I. JOURNEY OF PRIVACY RIGHTS

The ultimate law of the nation in India is the Constitution. Constitution of India is an ever-evolvingdocument, and adaptive towards conditions of the world around it. This is an unarguable reality that cannot be refuted.

In addition to a number of other fundamental rights, it acknowledges privacy right as among the various rights that falls within the purview of Article 21. Pursuant to Article 21, "no individual shall be deprived of his life and personal liberty except according to the method prescribed by law," which means that no one may be killed or have their freedom taken away without following the rules. Since the privacy right is part and parcel of individual's life and liberty, Article 21 guarantees protection for this fundamental human right.

Article 21 encapsulates privacy rights, also known as the right to be left alone, according to a decision made by the Supreme Court in the case *R. Rajagopal v. State of Tamil Nadu*[8], also known as the *"Auto Shanker Case*." In this case, the SC made it clear that this right exists. The privacy of an individual, their family, their education, their marriage, their children, and their unborn children is one of the many facets of Article 21[9].

Further, SC in*State of Maharashtra v. Madhulkar Narain*[10], decided that a lady has the same access to the right to private as any other person, and that no one has the right to breach her privacy.

Article 21 of the Constitution protects citizens' rights to life and liberty, including their right to privacy, and the government should not use this power unless there is a public interest, emergency, or danger to the public[11], according to the SC's decision in *People's Union for Civil Liberties v. Union of India*[12], which is also called "Phone Tapping Case." In this case, the court held that telephone tapping is a serious infringement of right to privacy. The Indian Telegraph Act of 1885 and the Information Technology Act of 2000 both give the government the authority to conduct surveillance activities under certain conditions. Those criteria must be in the best interests of India's *"sovereignty and integrity, the security of the state, good relations with foreign countries, public order, or the prevention of encouraging someone to commit a crime"*. These arguments are founded on the Constitution of India's provision of reasonable limits to freedom of expression, which may be found in the document.[13]

---

[8]

[9]YashrajBais, "Privacy and Data Protection in India: An Analysis" *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/privacy-and-data-protection-in-india-an-analysis/ (last visited June 10, 2022).

[10] AIR 1991 SC 207

[11]NiveditaBaraily, "An Analysis of Data Protection and Privacy Laws in India" *International Journal of Law Management & Humanities*, 2021*available at*: https://www.ijlmh.com/an-analysis-of-data-protection-and-privacy-laws-in-india/ (last visited June 10, 2022).

[12] AIR 1997 SC 568

[13]Abraham, "Data Privacy: Finding the Right Balance Between Data Personalisation and Consumer Privacy" *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/data-privacy-finding-the-right-balance-between-data-personalisation-and-consumer-privacy/ (last visited June 10, 2022).

It was noted by the SC in *R.M. Malkani v. State of Maharashtra*[14] that the court would not accept measures for the protection of citizens being jeopardized by allowing the police to continue in an illegal or irregular way[15]. Tapping someone's phone is ainfringement of their privacy right as well as their freedom of speech and expression. In addition, the government is not permitted to place prior restraints on the dissemination of defamatory information pertaining to its officials; if it were to do so, it would be in contravention of Articles 21 as well as 19(1)(a) of the Constitution[16].

In the year 2017, the right to privacy was finally acknowledged as a basic human right. Previously, this did not occur.

The landmark decision made by the SC in the case of *Justice K. S. Puttaswamy (Retd.) and Another.* v. *Union of India*[17] and others establishes that the privacy right is inherentunder Articles 14, 19, and 21 of the Constitution of India.[18] This decision has been hailed as a constitutional victory. Because of technology advancements, it was argued that the state and non-state organisations may both be held liable for violating people's privacy when it comes to protecting it[19]. However, like other fundamental rights,it is not absolute in nature, and any violation of that right by governmental or non-governmental organization must pass the *"triple test of legitimate goal, proportionality"*, and legality laid down in *Maneka Gandhi* v. *Union of India*[20]. This is true whether the actor in question is the state or not.

II. PRE-EXISTING SAFEGUARDS

There is no comprehensive legislation in India that addresses issues relating to the safeguard of personal information and privacy. In point of fact, a significant portion of its foundation consists of the laws and regulations that are already in place. These industry regulations are a linked part of that IT Act, 2000, and they thus supply the rules that regulate the gathering procedure, the use of such personally identifiable information as well as sensitive classified info or the date by the firms' organizations inside India.[21] The government is now working to oversee the establishment of certain extensive regulations that will assist monitor privacy and data protection.

There are a number of other essential statutory provisions that concentrate on and govern the preservation of personal privacy and the supply of personal data. There are several rules and regulations in place in India to ensure data privacy and security, which are separate from the constitution[22].

[14]1973 SCC (1) 471
[15]B Madhana, "A Study on Law Relating to Data Protection in India" *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/a-study-on-law-relating-to-data-protection-in-india/ (last visited June 10, 2022).
[16]*Ibid.*
[17](2017) 10 SCC 1
[18]"A study on Right to Privacy in light of K.S. Puttaswamy v Union of India," *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/a-study-on-right-to-privacy-in-light-of-k-s-puttaswamy-v-union-of-india/ (last visited June 10, 2022).
[19]*Ibid.*
[20]AIR 1978 SC 597
[21]Vidhi Agarwal, "Privacy and data protection laws in India," 5 *International Journal of Liability and Scientific Enquiry* 205–12 (2012).
[22]Sheshadri Chatterjee, "Is data privacy a fundamental right in India?: An analysis and recommendations from policy and legal perspective," 61 *International Journal of Law and Management* 170–90 (2019).

In the event of improper disclosure and abuse of personal data, as well as the breach of contractual obligations in regard to personal data, the Information Technology Act of 2000 addresses the problems that are related to the reimbursement of civil redress as well as the imposition of criminal penalty.

An organization may be held accountable for damages under Section 43A of the IT Act, 2000 if it is negligent in establishing but also implementing sufficient protection requirements, ending in the wrongful loss or gain of any individual who has been harmed by the negligence. In these kinds of situations, it is essential to keep in mind that the amount of compensation that may be demanded from the responsible party is not subject to any kind of predetermined cap.

Credit card numbers and health records are examples of sensitive personal information that cannot be profitably exploited by corporations who handle it. If a service provider reveals personally attributable info in unauthorized manner or in breach of an agreement, they are susceptible to criminal punishment under Section 72-A of IT Act, 2000.

A notification on the *"Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter Rules)"* has been issued by the government. The Rules exclusively address the notion to protect sensitive personal data[23] or certain data of a person, which comprises the kind of personally identifiable information that consists of information pertaining to: -

Information pertaining to one's financial situation, including but not limited to several instruments of payments and related data -

1. The patient's physical, physiological, and mental health;
2. Subject's gender or sexuality;
3. a patient's medical background as well as records;
4. Information pertaining to biometrics.

When dealing with "Personal sensitive data or information," the body corporate is expected to follow the rules that provide the appropriate security practices and procedures that are outlined in the rules. In the event that there is a violation of the agreement, the body corporate, as well as any person may be held vicariously liable, to pay compensation or renumeration to the victim who has been adversely affected.[24]

Section 72 A of the Act can be employed to punish in cases of unauthorized access of the data or any breach of the agreement. This crime is punishable by both of these punishments.

"Data" is defined as:

> *"a representation of information, knowledge, facts, concepts, or instructions that are being prepared or have been prepared in a formalised manner, and is intended to be processed or is*

[23]"Need for Sensitive Information and Data Protection Regulations in India," *International Journal of Law Management &Humanitiesavailable at*: https://www.ijlmh.com/paper/need-for-sensitive-information-and-data-protection-regulations-in-india/ (last visited June 10, 2022).
[24]SumaiyahFathima, "Right to Privacy and Data Protection: Indian Perspective," 6 *Supremo Amicus* 480–90 (2018).

being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes), or stored internally in the memory of a computer system or computer network".[25]

The IT Act includes definitions for the phrases "breach of confidentiality" and "invasion of privacy".[26] The phrase *"whoever, intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person"* is a very eloquent explanation of what constitutes a violation of privacy, and it is found in Section 66-E of the code.

The permission of the individuals who are the subject of the investigation is required under Sections 66E, 72, and 72A, but only within certain parameters[27]. This is because it is questionable whether or not the provisions could provide an adequate degree of protection for the individuals' personal information. In point of fact, the scope of these parts is limited to the activities and inactions of those individuals who have been given authority in accordance with the Act[28]. Monitoring of privacy violations, confidentiality violations, and information disclosures in violation of valid contracts are all included in these areas. The Act gives public and private bodies the authority to conduct their business in a manner that violates the confidentiality and privacy of individuals.

III. CONTEXT & CONCERNS

SC in 2017 ruled that the effective need of a data protection legislation in its decision in 2017 in *Puttaswamy*. The European Union passed a regulation known as the "General Data Protection Regulation (GDPR)" in 2018, which imposed various restrictions on companies regarding the use and management of individuals' personal data. On the heels of multiple high-profile data breaches by Indian commercial organizations, a committee was formed in 2018 to address this loophole in the country's legislation. The report and proposal for the PDP Bill, 2018 were sent to the Meityby the committee. "The Personal Data Protection Bill, 2019", which is a spin-off version of this bill, was just approved by the Lok Sabha.

PDP Bill was introduced in Lok Sabha in 2019. The "General Data Protection Regulation (GDPR)" served as inspiration for the proposed "Personal Data Protection Bill (PDP Bill)", which was intended to bring about a thorough reform of the present data protection framework in India, which is currently controlled by the Information Technology Act, 2000 and the laws thereunder.[29]

The bill provides a mandate for how information pertaining to persons must be handled and stored, and it also outlines the rights of individuals in relation to the information they provide about themselves. In order

[25]Section 2(1)(o), IT Act, 2000
[26]*Ibid.*
[27]Dhiraj R. Duraiswami, "Privacy and Data Protection in India," 6 *Journal of Law & Cyber Warfare* 166–86 (2017).
[28]*Ibid.*
[29]Devika Sharma, "Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study" *SCC Blog*, 2020*available at*:
https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/ (last visited June 11, 2022).

for this legislation to be enforced, it is intended that an autonomous organization, the Data Protection Authority (DPA), would be established in India.[30]

"Personal Data Protection Bill, 2019" is the latest in a long series of privacy laws in India[31]. This line of privacy law has been influenced by both global events and the personal constitutional law of the country. Although the right to privacy is not explicitly stated in the Indian constitution, Indian courts have held that the right to life guaranteed by Article 21 includes the right to privacy. A preventative framework for regulating how corporations collect and utilize personal data is the goal of the law, rather than safeguarding informational privacy as a consequence of the damage caused by the breach of such privacy[32].This is in contrast to existing legislation, which protects informational privacy with a purpose to the resultant harm. In doing so, it places a primary emphasis on generally regulating behaviours that are associated with the use of data[33].

In the event that specific nexus conditions are satisfied, the "Personal Data Protection Bill" would apply extraterritorially to enterprises that are not based in India. Additionally, the bill will impose significant financial penalties on firms that do not comply with its mandates.

This will not be restricted to simply businesses involved in e-commerce, social media, or information technology but will also encompass traditional stores, firms involved in real estate, medical facilities, and pharmaceutical enterprises.[34] However, there will be certain exceptions, such as for tiny organisations, which includes small merchants' firms who gather information manually and fulfil other standards that will be stipulated by the Data Protection Authority. These small entities will be considered an exemption.[35]

As a result of the fact that many worldwide commercial and telecommunications businesses are already subject to privacy and confidentiality criteria imposed by their sectoral authorities, many corporations already adhere to some of the policies and processes that are required by the law.[36] On the other hand, these regulations would be brand new for every other kind of company, and they would be required to comply with them.

The Supreme Court's ruling in the *Puttaswamy* case seems to contradict key aspects of the Bill, and those sections don't appear to make sense in the context of the rest of the legislation.[37] As long as it fulfils the globally recognised standards of necessity and proportionality, the draught Bill created by the Expert

[30]Dr G. Mallikarjun and B. Md Irfan, "Right To Privacy In India: The Technical And Legal Framework," 6 *Journal of Positive School Psychology* 5785–90 (2022).
[31]"Right to Privacy and Data Protection in India," *International Journal of Law Management & Humanitiesavailable at*: https://www.ijlmh.com/paper/right-to-privacy-and-data-protection-in-india/ (last visited June 10, 2022).
[32]Sheshadri Chatterjee, "Is data privacy a fundamental right in India?: An analysis and recommendations from policy and legal perspective," 61 *International Journal of Law and Management* 170–90 (2019).
[33]Yash More and Shailendra Shukla, "Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy," 6 *Indian Journal of Law & Public Policy* 42–58 (2019).
[34]Umang Joshi, "Online Privacy and Data Protection in India: A Legal Perspective," 7 *NUALS Law Journal* 95–111 (2013).
[35]Aman Pandey and Hema Chaudhary, "The Exigency to Address the Personal Data Issues: The Personal Data Protection Bill, 2019," 2 *Jus Corpus Law Journal* 533–9 (2021).
[36]Yash More and Shailendra Shukla, "Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy," 6 *Indian Journal of Law & Public Policy* 42–58 (2019).
[37]Neelam Rai, "Right to Privacy and Data Protection in the Digital Age - Preservation, Control and Implementation of Laws in India Part III: Special Issue on Law as an Instrument of Social Transformation: Environment, Technology and Social Change," 11 *Indian Journal of Law and Justice* 115–30 (2020).

Committee enabled exemptions to be made in the name of national security provided an equivalent was authorised by a legislation adopted by Parliament. While, according to Section 35 of the PDP Bill, the Central Government may authorise any agency to handle personal data with a simple executive order, which then gives that agency the ability to undertake surveillance without any obvious protections. When such exclusions should be granted exclusively via legislation, as the Expert Committee[38] advised, the amendment as mentioned appears like an effort to diminish the private rights of people[3940].

When we take a look at the GDPR, which forms the backbone of the PDP Bill, we often notice that the GDPR provides member states of the European Union (EU) with escape provisions that are very similar to those in the PDP Bill. However, they are subject to stringent regulations as a result of other EU rules. In the absence of comparable protections, India's Bill might provide the Central Government of India with the ability to access individual data in violation of the laws that are now in effect in India.[41]

A component of the privacy right is the protection of one's personal information. In this era of information, the threats to individuals' ability to maintain their privacy might come not just from government as well as nongovernmental organisation such as businesses. The establishment of such a system calls for a delicate and nuanced balancing act between the legitimate interests of the state and the individual concerns of its citizens.[42]

Even though there are some exceptions for things like national security, defence, public security, and so on, the GDPR of the European Union is an all-encompassing mechanism of data protection that can be employed to the processing of personally attributable data in any way, shape, or form, and to processing transactions carried out from both the government as well as private organisations. In a same vein, it continues to acknowledge and put into practice the fundamental data protection principles that are outlined in the OECD Guidelines[43]. The GDPR takes a freedoms and liberties approach to the safeguarding personally attributable data and puts the individual at the center of the legal system. As a direct result of this, it imposes stringent controls towards handling of personally identifiable data both at the time of the data collection and after it has been obtained. Data on *"racial or ethnic origin, political views and religious or philosophical ideas, trade union membership and data on health and sex life"* are all illustrations that is forbidden from being collected, with a few limited exceptions. Therefore, in order for processing to be lawful[44], various principles have to be complied with.

[38]Committee of Experts, *WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA* (Government of India).
[39]Aman Pandey and Hema Chaudhary, "The Exigency to Address the Personal Data Issues: The Personal Data Protection Bill, 2019," 2 *Jus Corpus Law Journal* 533–9 (2021).
[40]Committee of Experts, *WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA* (Government of India).
[41]ShubhanshiPhogat, *The Curious Case of Right to Privacy in India* (Social Science Research Network, Rochester, NY, 28 October 2021).
[42]HaardikRathore, "An Analysis of Personal Data Protection Bill, 2019"*available at*: https://legalbots.in/blog/an-analysis-of-personal-data-protection-bill-2019 (last visited June 11, 2022).
[43]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD,*available at*: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited June 12, 2022).
[44]S. G. Abhilasha, "A Detailed Legislative Comment Exploring the Broad Contours and Nuances of the Personal Data Protection Bill 2019," 24 *Supremo Amicus* [253]-[259] (2021).

The passage of the Personal Data Protection Bill, 2019, in India would have significant repercussions for both the country's economy and its government.[45]

The bill lays forth a number of requirements that must be met by the most successful businesses as well as by the most successful multinational technology corporations who want to do business in Indian Territory. To start, it would be mandatory for digital companies to first get the users' consent before collecting any of their data[46]. Additionally, it proclaims that people who contribute data are, in effect, the proprietors of their own data. Users may manage the data they create online and request that companies erase it, much as European internet users can exercise a right to be forgotten and have proof of their online existence deleted. This has significant ramifications.

CONCLUSION & SUGGESTIONS

An extraordinary need to bring India's data protection regulations up to date with worldwide efforts that have been tried and are already in place has arisen as a result of the dynamic and ever-expanding situation in the country, which is full of problems, rising foreign investments, and economic development in the ever-expanding digital age.Recent efforts by the sector, the public, and the government have helped to make up for the absence of comprehensive law, which, although still a cause for worry, has been offset.

The Constitution does guarantee privacy rights, but how that privilege and liberty is used and expanded is completely up to the discretion of the courts. If someone is determined to get information out into the public domain in today's linked world, it is very difficult to stop them from doing so without resorting to very oppressive means. This is because of the nature of the internet. There is some discourse of data protection and privacy in the IT Amendment Act of 2008, but it is not a full treatment of the subject.[47] The Information Technology Act needs to include provisions for the establishment of a specific parameters pertaining to the techniques and end goal of assimilating personal data and rights to privacy.

The PDP Bill is a positive start toward the establishment of a data protection system; nonetheless, it is riddled with several elements that water down the fundamental right of privacy.[48]This privilege is also greatly undermined by the bill, and the capacity of the state to monitor citizens is expanded without any corresponding increase in checks and balances.[49] Academics and activists have the most significant reservations about the bill's provisions that exclude the government from certain requirements. According to Section 35 of the Bill, the any state organization can be exempted by discretion of Union Government. This power is given to the Central Government. Even while some government entities are exempt from certain requirements, certain duties, such as the adoption of security precautions and the processing of

[45]Yash More and Shailendra Shukla, "Analysing the Impact of the Personal Data Protection Bill, 2019 on the Fundamental Right to Privacy," 6 *Indian Journal of Law & Public Policy* 42–58 (2019).
[46]*Ibid.*
[47]Shiv Shankar Singh, "PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT," 53 *Journal of the Indian Law Institute* 663–77 (2011).
[48]Devika Sharma, "Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study" *SCC Blog*, 2020*available at*: https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/ (last visited June 11, 2022).
[49]S. G. Abhilasha, "A Detailed Legislative Comment Exploring the Broad Contours and Nuances of the Personal Data Protection Bill 2019," 24 *Supremo Amicus* [253]-[259] (2021).

information in a fair and reasonable manner, should continue to apply.[50] According to Section 35, the government is allowed to make exceptions to *"collection rules, reporting requirements, and other requirements"*whenever it deems it necessary or expedient to do so in the interests of India's *"sovereignty and integrity, national security, friendly relations with other states, and public order."*

It is troubling that there is not yet sufficient privacy and data protection laws in place.[51] This has been a source of worry. This worry has been voiced in particular by international businesses that are doing operations in India and are transferring sensitive data into the country. It is needed that all of the stakeholders align their policies with the standards of data protection and promote adoption of the principles of privacy by design in order for the data protection regime to be effectively implemented. This is a necessity for effective implementation. Consequently, by enacting a trustworthy data privacy legislation, India has the potential to become much more than a simple provider of services to the multi-national enterprises of the globe. In other words, it's trying to turn India into a business hub.

[50]Aman Pandey and Hema Chaudhary, "The Exigency to Address the Personal Data Issues: The Personal Data Protection Bill, 2019," 2 *Jus Corpus Law Journal* 533–9 (2021).

[51]Astha Rao and ShipraSahu, "Right to Privacy and Data Protection in India," 23 *Supremo Amicus* [161]-[166] (2021).