ISSN: 2278-4632
Vol-10 Issue-6 No. 4 June 2020

RIGHT TO PRIVACY AND DATA PROTECTION IN INDIA

Pooja Kiyawat

Ph.D. Research Scholar,
School of Law, Jagran Lakecity University, Bhopal (M.P.)

INTRODUCTION

It has often been opined by the commentators and the experts in the field that the big data comes with bigger challenges to the goal of securing privacy of the individuals[1]. With the advent of enormous technological developments all across the world, the use of data in the day to day lives has witnessed an unprecedented fillip[2]. Apart from the private sector, which has consistently honed the potential of data for crafting the change in the goods and services sector, the approach of the government towards adopting the digital mediums has been exemplary[3]. The economic survey of India, 2019 dedicated an entire chapter focusing on the virtue of digitalization and the need for implementing measures to bring data under the ambit of public goods[4]. The government and the private businesses have aggressively adopted the digital measures to ease up providing services[5]. In a span of past few years, the advent if digital platforms cutting all across sectors such as finance[6], health[7], food delivery[8], academics[9],

---

[1]The Indian Express. 2020. *India'S Challenge Is How To Use Big Data For Better Governance: Electronics And IT Secretary*. [online] Available at: <https://indianexpress.com/article/technology/tech-news-technology/indias-challenge-is-how-to-use-big-data-for-better-governance-electronics-and-it-secretary-4877508/> [Accessed 5 June 2020].
[2]*Id.*
[3]BW SC. 2020. *PM Modi Prioritizes Digital India, Start-Up For $5 Trillion Economy*. [online] Available at: <http://bwsmartcities.businessworld.in/article/PM-Modi-prioritizes-Digital-India-Start-Up-for-5-trillion-economy/01-10-2019-176968/> [Accessed 5 June 2020].
[4]Businesstoday.in. 2020. *Why A Strong Digital Ecosystem Is Key To India's $5 Trillion Economy Vision*. [online] Available at: <https://www.businesstoday.in/opinion/columns/strong-digital-ecosystem-key-to-india-5-trillion-dollar-economy-vision-digitalisation-indian-economy-modi-government/story/383932.html> [Accessed 5 June 2020].
[5]FinanSys Solutions Ltd. 2020. *What Is The Role Of Digitalisation Within The Financial Services Sector?*. [online] Available at: <https://www.finansys.com/blog/what-is-the-role-of-digitalisation-within-the-financial-services-sector/> [Accessed 5 June 2020].
[6]*Id.*
[7]*Id.*
[8]Republic World. 2020. *Are Swiggy&Zomato Delivering Food In Mumbai, Delhi, Bengaluru & Other Metros? Answered - Republic World*. [online] Available at: <https://www.republicworld.com/technology-news/apps/swiggy-zomato-resume-services-in-mumbai-delhi-bengaluru-and-other-m.html> [Accessed 5 June 2020].
[9]The Week. 2020. *Unacademy Hacked, Data Of 20 Million Users Up For Sale*. [online] Available at: <https://www.theweek.in/news/sci-tech/2020/05/07/unacademy-hacked-data-of-20-mn-users-up-for-sale.html> [Accessed 5 June 2020].

services[10], e-commerce[11], business[12]etc have almost replaced the traditional ways of service industry. No doubt that a digitalized economy is in the interest of the country, the risks posed by exponential rise in the use of data in every day to day lives is equally enormous. There have been numerous instances in the recent past where the personal data of the individuals have come under cyber attacks.

The threat to informational privacy of the individuals stems from the fact that the voluminous data in the public domain can act as a great asset for the companies which can use to for purposes that are beneficial to them. The recent leaks from Cambridge analytica, the Aadhar data base leak[13], the UnAcademy data base leaks[14] and the recent debit card leaks[15] are some of the most notable examples of the threat that the breach of informational privacy poses to the personal and sensitive data of the individuals.

EXISTING LEGAL REGIME IN INDIA

Indians, in general don't care at all about their right to privacy. This is one of the most notable reasons behind the failure of the legislature to put in place a comprehensive data protection law that would cater to the need of having an effective data protection regime in place[16]. While, the member states of European Union and United States, had an effective data protection regime as back as over four decades ago[17], India has still struggled to put in place, a data protection legislation that would ensure informational privacy for the citizens of the country. One of the other probable reasons for the non-existence of a comprehensive data protection regime in India could be the absence of the threat to the right to privacy few decades ago[18]. The growth of Information technology industry in India and the subsequent threats to the offshoring business

[10]Id.
[11]Pbr.co.in. 2020. [online] Available at: <http://www.pbr.co.in/2018/2018_month/Feb/24.pdf> [Accessed 5 June 2020].
[12]Id.
[13]BBC News. 2020. *Identity Database 'Leak' Worries Indians*. [online] Available at: <https://www.bbc.com/news/world-asia-india-42575443> [Accessed 5 June 2020].
[14]Id.
[15]Id.
[16]OrlaLynskey, *Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order*, 63 Int'l & Comp. L.Q. 569 (2014).
[17]LiliiaOprysk, *The Forthcoming General Data Protection Regulation in the EU*, 24 Juridica Int'l 23 (2016).
[18]Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data*, 21 Temp. Int'l & Comp. L.J. 103 (2007).

propelled the enactment of the Information Technology Act, 2000[19]. However, the absence of the key data protection principles in the legislation leaves the current data protection framework prone to breaches.

THE INFORMATION TECHNOLOGY ACT, 2000

The provisions of the Information Technology Act along with the Reasonable Security Rules, 2011 are the only laws that India has in the name of data protection legislation. The section 43 A of the Act provides for the compensation for the data owners in case the body corporate that is handling their data fails to implement reasonable security measures and thereby cause some sort of wrongful loss to him. Notably, the provision applies only to the body corporates and places numerous conditions for obtaining the remedies under the Act. It provides that in case the body corporate has taken reasonable security measures to prevent the breach of the data and at the same time there must be some wrongful loss to the data owner[20].

However, in last two decades the digital world has undergone a sea of changes and the measures envisaged by the IT Act, 2000 have proven to be insufficient to prove as an effective control mechanism against the potential breaches of right to privacy[21].

UNDERSTANDING THE RIGHT TO PRIVACY

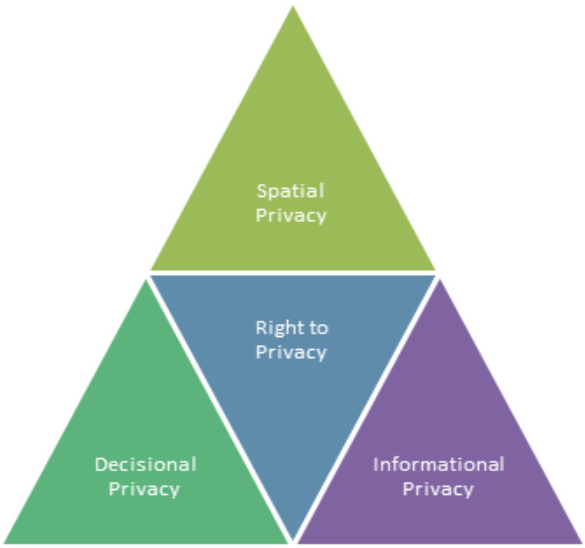
The landmark judgment of the Supreme Court of India in Justice K S Puttaswamy v. Union of India[22] was the watershed movement in the realm of the privacy jurisprudence of India wherein the Supreme Court of India recognized the right to Privacy as a fundamental right. However, striking a direct correlation between the right to privacy and data protection can be established only after one has deeply analyzed the underpinnings of the right to privacy. The author would

[19]Dhiraj R. Duraiswami, *Privacy and Data Protection in India*, 6 J.L. & Cyber Warfare 166 (2017).
[20]Section 43A Information Technology Act, 2000.

[21]Dhiraj R. Duraiswami, *Privacy and Data Protection in India*, 6 J.L. & Cyber Warfare 166 (2017).
[22]Justice K S Puttaswamy v. Union of India, (2017) 10 SCC 1

ISSN: 2278-4632
Vol-10 Issue-6 No. 4 June 2020

argue that the right to privacy has to be understood as a combination of several sub-categories of the right to privacy. These subcategories are the Spatial Privacy, the right to Decisional Privacy and the right to informational privacy.



The conception of privacy being the superset of these three prongs shows that the right to privacy has its outreach way beyond the traditional notion of the right to be left alone.

The initial jurisprudence relating to the right to privacy can be traced back to the 4th Amendment of the US Constitution which recognizes the right of the individuals to be left alone. The spatial notion of the right to privacy associates the right to specific places and not persons. However, this stage was short lived and the Supreme Court in the case of Kharak Singh v. State of U P[23] held that the right to privacy is inherently attached to the noble value of protection of right to privacy.

> *"If the reason for protecting privacy is the dignity of the individual, the rationale for its existence does not cease merely because the individual has to interact with others in the public arena. The extent to which an individual expects privacy in a public street may be different from that which she expects in the sanctity of the home. Yet if dignity is the underlying feature, the basis of recognising the right to privacy is not denuded in public spaces… Privacy attaches to the person and not to the place where it is associated."*

[23]Kharak Singh v. State of U P , 1963 AIR 1295

ISSN: 2278-4632
Vol-10 Issue-6 No. 4 June 2020

Further, the notion of the right to privacy was expanded to include the concept of decisional privacy by the Supreme Court in the case of K S Puttaswamy wherein it was held that

> *"The inviolable nature of the human personality is manifested in the ability to make decisions on matters intimate to human life. The integrity of the body and the sanctity of the mind can exist on the foundation that each individual possesses an inalienable ability and right to preserve a private space in which the human personality can develop*[24]*."*

The Supreme Court of India in K S Puttaswmay[25] highlighted the importance of the right to informational privacy in order to secure the decisional privacy of the citizens. Justice Chandrachud opined that the concept of the Data protection is an inherent aspect of the right to informational privacy.

The rationale of Data Protection is based on the concept of Informational privacy. This aspect of privacy embeds within its fold, the principle of Informational self-determination, the SC in Puttaswamy observed that the "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well". It must be acknowledged that the data to decisional privacy will be meaningless without the right to informational privacy.

After recognition of the right to privacy as a facet of the fundamental right to life and liberty, it becomes the constitutional obligation of the legislature to enact a comprehensive data protection law. This will be instrumental in setting up a robust data protection regime that incorporates the key principles of data protection laws. Additionally, a strong framework to protect the personal and the sensitive data of the citizens will make the country less prone to the threat of cyber attack.

CONCLUSION

[24]Justice K S Puttaswamy v. Union of India , (2017) 10 SCC 1
[25]Id.

ISSN: 2278-4632
Vol-10 Issue-6 No. 4 June 2020

In the light of the aforementioned discussion, we may arrive at an undeniable conclusion that the existing law regulating the data protection framework in India is very limited in its scope and ambit and thus there exists a pressing need for the legislature to enact a comprehensive data protection code. The author would like to recommend the following aspects that should be incorporated in the upcoming code in order to ensure that the informational privacy is protected to its fullest extent.

1. Adoption of all the Data Protection Principles
2. Emphasis on the element of consent before processing of personal data
3. Greater protection to the sensitive personal data
4. Formation of an independent data protection authority
5. Adequate framework to implement the mandates of the code.

It is only through these elements, that India will be able to get a robust data protection framework. The emphasis on informational self determination should form the key aspect of the data protection law in India.

