

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 5

2021

© 2021 International Journal of Legal Science and Innovation

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at International Journal of Legal Science and Innovation, kindly email your Manuscript at submission@ijlsi.com.

Data Surveillance: A Protection to Privacy or a Tool for Government

SHARMISHTHA TRIVEDI¹

ABSTRACT

Data protection as we all know is the most sensitive issue not only in India but across the world. India, is one of the largest country with world's largest democracies, but there still is no single legislation in the country which specifically speaks about the data protection and its privacy. In the year of 2018, a new draft of Personal Data protection was introduced in the Indian parliament. The surveillance activity across the country has increased vividly because of cross border terrorisation and terrorist threats which has impacted the entire world. The surveillance activities are also a threat to privacy of the citizens and there has been certain cases where data is leaked.

As the Indian government with the help of private sector set up their digital infrastructure and has extended a large number of internet services, issues of digital rights, data ownership and privacy protection. One of the landmark cases of data protection and privacy

The Right to Privacy is a concept which is multidimensional in nature and is most recognized in the modern society in both the eye of the law as well as in common parlance. Talking with regard to Indian Constitution, Article 21 , which protects the right to privacy and promotes the dignity of the individual in the recent years has grown at a very significant level. With the advent increase and development of digitization, it has become very much important to protect and safeguard the right and data of the citizens and their privacy and this research paper tries to shed some light on the same topic with the chapterisation process which is further divided into two parts.

Keywords: Data Surveillance, Private sector, Data protection, Right to Privacy.

I. INTRODUCTION

The supreme court of India in the year 2018 declared Right to privacy as a fundamental right and that no one can work in violation of that right. The right to privacy works as a specific

right of an individual, to control the collection, use and disclosure of personal information. Personal information are of several types and most of it are available on the government websites which sometimes can be accessed by people who have enough knowledge of hacking

¹ Author is a student at Christ Academy Institute of Law, Bengaluru, India.

the data and working in respect to it. The legal codification and protection of data is a very complex topic which should be carefully handled by the government. There are end number of social websites which takes our data or surveillances them and hence, to protect them from different social contexts demanding different forms needs a different degree of protection.

The recent debate of privacy mainly revolves around two major topics that are: surveillance and data protection. Surveillance as a topic can be understood as a form of capturing the data where phone calls, messages and all such related communication forms are tapped and a person under authority has full knowledge regarding it. The interception of communications – phone calls, emails, and letters, – which is a type of surveillance, is statutorily regulated in India in an uneven way. A colonial law permits and regulates wiretaps in India.²

The researcher in this paper will analyze the topics under two main chapter that are, Limitation of Data Surveillance and Data surveillance benefits for protection of privacy of citizen. The researcher will also analyze all the questions related with the current topic and shall provide with a legal status of current system of data protection in India with respect to right to privacy of citizens and data surveillance activity carried out by India and the authorities who have

power to tap the data for official purposes. Social media is one of the major and giant parties which effect the right to privacy of citizens as they usually collect the data and stores them into their information portal. Social media applications like Facebook, WhatsApp, Instagram and the largest search engine of the world, Google, have in built phone algorithm where they have techniques of listening to your voice and storing data with themselves. If people have had noticed, during recent times, they can see how various web pages and social media accounts start suggesting you pages and websites of similar products and pop ups which you have earlier talked about. These are the various ways by which data theft happens across the world and the buyer has to beware of such thefts.

II. RIGHT TO PRIVACY

In India, Right to Privacy is a fundamental right guaranteed under Article 21³ of the Indian Constitution, which also lays down fundamental rights of the citizens. The term privacy and right to privacy cannot be easily conceptualized. These both terms are taken into consideration in different ways, when needed according to time. In modern society privacy has been recognized both in the eye of the law and in common parlance. But it varies in different legal systems as they emphasize different aspects.⁴

The Right to Privacy was affirmed by a 9-judge bench of the Supreme Court in the case of KS

² Bhairav Acharya, 'Understanding Surveillance and Privacy in India' The center for internet and Society, (India, August 28 2014), <https://cis-india.org/internet-governance/news/understanding-privacy-and-surveillance-in-india>, Accessed on 3rd Feb, 2020.

³ Supra3.

⁴ Dr. Shiv Shankar Singh, 'Privacy and Data Protection in India' The Practical Lawyer, (India, 2012 February) S-2 Introduction, http://www.supremecourtcases.com/index2.php?option=com_content&itemid=5&do_pdf=1&id=23269, Accessed on 4th Feb.

Puttaswamy v Union of India in its historic judgement passed on 24th of August, 2017 and here it was declared that 'Right to Privacy' is a fundamental right of the citizens and everyone should be guaranteed that without any violation. Also, Right to Privacy is fundamental right which is guaranteed under Part III of the constitution of Constitution of India.

This question of 'Right to Privacy' was brought in front of the bench under a case of Aadhar Card and protection of data. The bench wanted to decide if privacy is a fundamental right or not before deciding the Aadhaar case. The Attorney General in the present case argued that although several judgements in the past has recognized right to privacy but they however, have refused to accept the contention that right to privacy is a fundamental right⁵ and should be envisaged under part III of the constitution of constitution of India. The case of Kharak Singh was a six-judge bench case where Right to Privacy was recognized but there was no mention of fundamental right attached to it. Later, in the KS puttaswamy case, a need for higher bench of judges was felt and therefore, a nine-judge bench was constituted to decide whether 'Right to Privacy' is a 'Fundamental Right' or not.

Through this broad interpretation by the court under Article 21 as well as under Article 19 helped the Indian government to constitute and draft more legislations with respect to data protection and Personal Laws.⁶ Hence, before 2017 the Right to Privacy was not considered as

a Fundamental Right which should be guaranteed by the Indian Constitution but after 2017, it is a fundamental right of citizens to protect their data and have a right to privacy.

III. EXISTING FRAMEWORK FOR DATA PROTECTION INDIA

Article 21 of the Indian Constitution is a fundamental right that guarantees protection of life and liberty to its citizens. As discussed above in the case of KS Puttaswamy, the court decided the case where Right to Privacy was considered as a Fundamental Right and it is a constitutionally protected right. The protection under Article 21 is not absolute and it is subject to certain restrictions. The law is created and certain restrictions are imposed by the legislature so that the interest of the nation and its integrity is maintained and is not hampered by anyone.

Personal Data Protection Bill

The Personal Data Protection Bill (PDP) helps in monitoring the data privacy in India. This bill was introduced in parliament in the year 2018 post the hearing of Aadhaar case and ruling by the supreme court that Right to Privacy is a fundamental right and should not be abrogated by anyone. After the Aadhar case ruling the Government of India(GOI) took a step in the direction of saving and protecting the data of citizens from getting leaked and sold to other people. A stricter law was needed for protection of data of the citizens and therefore, this bill was introduced. Though the bill was introduced in the

⁵ Kharak Singh v. The State Of Uttar Pradesh (1964) SCR (1) 332.

⁶ Priya Rao, 'Personal Data Protection Law in India' K&S Partners Legal 500, (India, October 2 2020),

<https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/>, Accessed on 4th Feb, 2020.

year 2018 but it was not passed by the parliament. After several sitting in the parliament and suggesting changes in the bill, the bill was finally passed by the cabinet in the year December 2019 after which it was referred to a joint committee (comprising of members of the Lok Sabha and Rajya Sabha), which is to present a final report before the next budget session for final deliberation before it becomes a law.⁷

The Personal Data Protection Bill primarily focuses on protecting the data of citizens and provide more stringent laws towards it. The bill seeks to provide more control to the citizens of India over their personal data and protection of it from getting leaked. The new bill not only protects the data privacy of the citizens but also balances the importance of personal privacy and new technological innovation which helps in gaining the ethical and fair advantages from the data they are willing to share. The bill also aims to protect the data from getting leaked through various social media applications and stops it from getting sold to other countries data. The bill ultimately aims to provide with an environment of trust towards processing of personal data information.

The main objectives of Personal Data Protection Bill are:

1. To protect and empower the vulnerable class- under the vulnerable class there has been division of classes which needs extra protection and control so that their data is more protected

and does not get leaked from anywhere. Vulnerable class includes-

- Children- the PDP Bill talks about parental control or consent which further empowers the citizens from protecting their personal data information of a child.
- Employer employee relationship
- LGBT Community
- Patients Data- The data of a patient is one of the most confidential data which by default should be protected by the government. There are several obligations in protecting a patients' data with regard to design, data privacy impact assessment and individual rights. These are the privacy concerns of a patient which should be protected. There are different kinds of requirements while protecting data of a patient like cross border data transfer, consent and technical safeguards.

2. Enhanced control to consumers- the new PDP bill will provide more enhanced and transparent control to the consumers and will make them owners of their personal data. There always have to be consent of a consumer before any personal information is taken from the consumers.

3. Increased Accountability- there has been an increased accountability for handling and safeguarding the citizens data through the new PDP Bill. The new bill would hold both private and government organizations accountable for

⁷ Dhritimaan Shukla, Sonali Saraswat & Harbani Gill, 'Personal Data Protection Bill, 2019: What Indian citizens can expect' PWC.in, (India, April 2020),

<https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-indian-citizens-can-expect.pdf> , Accessed on 4th Feb,2020.

protecting the data of the citizens and handling it with utmost importance because it is a sensitive issue. The measure taken through new bill would also enable the government in taking consent from people (citizens) and putting up of a mandatory additional security measure to protect the data of any category they use.

4. Enhanced rights to the citizens- Through the introduction of new Personal Data Protection bill there has been enhanced right to protection which is guaranteed to the citizens of India on their personal information. The bill introduces the provision of 'sandbox'⁸ to pave a better way for responsible and more regulated methods with reduced risks and more transparency.

5. Notification on Personal and Non-Personal Data- The Ministry of Electronics and Information Technology on 13th September, 2020 announced that a new notification from (MeitY) for setting up of a new expert committee will be formed to discuss aspects of community data. The new 2019 version of PDP will also

define non-personal data which was not discussed in the old version of the bill. There has to be more analysis and probing into the usage and risks of non-personal data information.

IT Acts and its Rules

Under the existing laws related to data protection in India, the IT Act mandates protection of data through Section 43A⁹ of the said Act. Under this section a person or an organization will be liable to pay damages if there has been any misuse or no proper handling of personal data information. A body corporate means any company and includes any sole ownership as well as a firm, engaged in commercial or professional activities.

There are several reasonable security practices and procedures¹⁰ under the section 43A of IT Act which has to be observed by the body corporates.

Section 75¹¹ of the IT Act extends the privacy and protection of data outside India. According to the said provision, the IT Act will be applicable to any offence or contravention

⁸ A sandbox is a testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control.

⁹ The Information Technology Act, 2000(Act 43A of 2000).

-43A Compensation for failure to protect data. -Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

¹⁰ The Information Technology Act, 2000(Act 43A(ii) of 2000).

-(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access,

damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

¹¹ The Information Technology Act, 2000(Act 75 of 2000).

-75. Act to apply for offence or contravention committed outside India.-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

committed outside of India by any person if the network, computer or system is used by the person which is located in India.

As stated in the provision and IT Act, an intermediary will not be liable for any third-party information, data or communication link made or hosted by him.

IV. DATA PROTECTION IN FOREIGN COUNTRY

There have been different laws and policies in regard to data protection and right to privacy of citizens in different countries. One of the most famous among those policies is General Data Protection Regulation¹² of the EU Framework. It is a new legal EU Framework which governs the use of personal data across the EU. The new GDPR lays down the rules which are related to protection of data of natural persons with regard to processing and free movement of personal data. It replaces the Data Protection Directive 95/46/EC.¹³

The GDPR regulates the processing of data and protects them from getting leaked to any other foreign website or information system. The General Data Protection Regulation does not apply to personal information data processing which is done by a person for their own personal usage in the course of purely personal household or community activity.

APPLICATION- The GDPR applies globally to all the companies which are working within the

EU or outside the EU if they are using any personal data of EU data subjects in connection with offering of goods and services. The GDPR regulations of European Union will also apply to India Organization if the Indian organization has been using data which is in direct contact of EU companies or citizens and monitors their data.

Hence, the GDPR is a legal framework of European Union which is not only applicable within the EU but also outside the EU if any data is related with their citizens or companies. Currently, in India we do not have any such legislation which is directly in relation to General Data Protection Regulation but under the B.N. Srikrishna Committee formed in the year 2017 they have drafted the PDP Bill which is discussed above to protect the data and privacy of citizens.

V. DATA SURVEILLANCE

Data Surveillance is a method through which there is a close observation of a group or any particular person and the official authorities who have power can keep a track on the activities of that person or a group. The process of Data Surveillance takes place when there is any suspicion on the act of the person or the group. India, being a developing nation has brought several changes in their existing laws with regard to data surveillance and observation of people.¹⁴ There are still many changes which are required to be brought by the Ministry of Information Technology. With the growing technologies and developing nations, new types of surveillance are

¹² General Data (Protection) Act 2018.

¹³ Obhan & Associates, 'Data Protection and Privacy in India' (India, April 2019), <https://www.mondaq.com/india/privacy-protection/801302/data-protection-and-privacy-in-india>, Accessed on 5th Feb 2020.

¹⁴ Prashanti Upadhaya, 'Surveillance in India and Its Legalities' (India, May 2020), ISBN No: 978-81-928510-1-3, <http://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html>, Accessed on 5th Feb 2020.

also been brought into existence like CCTV Surveillance, Internet Surveillance, Telephone surveillance and many other. The only question that arises is whether these surveillance guarantee protection to the privacy of the citizens or is the data which is surveillance is at great danger of getting misused. There are several departments which are working under the Indian Government for surveillance. Some of them are:

1. National Intelligence Grid.
2. Crime and Criminal Tracking System. (CCTNS)
3. Unique Identification Authority of India.(UID Scheme)
4. National Counter Terrorism System. (NCTC)
5. Central Monitoring System.

Limitations of Data Surveillance

Under the surveillance system of India, there are certain limitations which are imposed so as to control the data from getting leaked and that the privacy of the citizens is maintained. Some of the limitations according to Justice Shah Privacy Principles¹⁵ serve as one of the most important aspects and recommendations to control the data surveillance. The CIS (center for internet and society) participated in meetings and helped in drafting of Report with the help of experts on

privacy.¹⁶ Some of the limitations in data surveillance are;

1. Principle of consent from citizen-

According to this principle, the authorities should take consent from the citizens or the personnel whose data is been surveillance. Unless the data surveillance is for the purpose of nation's safety and integrity, the consent should always be obtained by the officials before tapping any data.

2. Principle of limitation in collection of data-

There should be a limitation set with regard to collection of data. No such data should be surveillance which is beyond the limitations of the government.

3. Principle of security-

According to this principle, security should always be guaranteed to the citizens for the data which is surveillance. The security should be given even for the information which is obtained through online websites or social media platform.

4. Principle of privacy and no data theft-

In data surveillance one of the major concerns is of data theft. There have been instances where personal data is sold to some third party for some principal amount and it is very dangerous for a citizen.

5. Principle of Disclosure and Information-

There should be full disclosure to the citizens

¹⁵ Maria Xynou, 'Policy Recommendations for Surveillance Law in India and an Analysis of Legal Provisions on Surveillance in India and the Necessary & Proportionate Principles' (India), <https://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf>, Accessed on

5th Feb 2020.

¹⁶ Justice Ajit Prakash Shah, Former Chief Justice, High Court of Delhi, "Report of the Group of Experts on Privacy", Planning Commission (CIT&I Division), Government of India, 16 October 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf, Accessed on 5th Feb 2020.

whose data is put for surveillance. The disclosure shall be based on the willingness of the government and to subject to facts.

6. Principle of Individual and Fundamental Right- Right to Privacy is a Fundamental Right and it always should be maintained and guaranteed by the government.

Benefits of Data Surveillance

There are some benefits of data surveillance and because of which it is widely used in the present world. Some of them are:

1. Reduces theft.
2. An eye on all.
3. Protect the business.
4. Protect the nation's security and safety.
5. Improves productivity.

VI. CONCLUSION

India is a growing and a developing nation and its legislative framework is also growing with the passage of time and development around the world. India's surveillance policies are growing as well. Currently, the data policies are not adequate and needs to be changed according to the time. Through the policies introduction and the PDP bill passed in the parliament, there has been a major change in the country with regard to data surveillance. In India, there is a need to pass more acts and legislatures for data protection and privacy of citizens in India. The word privacy has changed a lot from the past and therefore, it has to be changed accordingly. The case of puttaswamy has brought a huge change in the country and spoke more about the data protection of the citizens, it has gained more

traction. The Indian courts are taking initiative to ensure protection of personal data of the citizens of the country.

VII. BIBLIOGRAPHY

- <https://iclg.com/practice-areas/data-protection-laws-and-regulations/india>
- <https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949>
- <https://www.mondaq.com/india/privacy-protection/801302/data-protection-and-privacy-in-india>
- <https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-indian-citizens-can-expect.pdf>
- <https://www.epw.in/engage/article/protection-vs-privacy-debate-surveillance-and-digital-rights-india>
- <https://m.globallegalpost.com/commentary/will-indias-new-data-protection-law-serve-as-a-government-surveillance-tool-4261027/>
- <https://www.bloombergquint.com/law-and-policy/a-brief-on-data-privacy-protection-and-surveillance>
- http://www.supremecourtcases.com/index2.php?option=com_content&itemid=5&do_pdf=1&id=23269
- <https://www.dataguidance.com/notes/india-data-protection-overview>
- <https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/>
- <https://www.mondaq.com/india/data-protection/952878/judiciary-steps-in-mandates-data-protection>
- <http://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html>
