DE JURE NEXUS LAW JOURNAL

Author:

Deo Mani Tripathi

Banaras Hindu University

3rd Year, LL.B. (3 Years)

# DATA PROTECTION AND PRIVACY LAWS IN INDIA

**ABSTRACT** –

*Data protection is one of the very important and burning issue in the present scenario. Because of the transition from offline to online of almost each and everything around us, data takes a very important place and as a result its protection is also very important. In India there are various provisions regarding offences that are committed digitally in various acts like Indian Penal Code, Information and Technology Act etc. but there is no act or law which deals comprehensively and separately for the protection of data. So, there is the need of a separate act for that and that is why Personal Data Protection Bill, 2019 has been tabled in Indian Parliament and currently it is under analysis by the Joint Expert Committee of Parliament.*

**Keywords** – Data, Protection of data, Personal Data Protection Bill, 2019, Joint Expert Committee.

**INTRODUCTION** –

Data is nothing but facts or information in the form of words, pictures, animations, figures etc. which are stored in computer. This data is collected, analysed and examined to formulate plan and help in decision making. This data if used for the purpose of development can cause miraculous changes but it stolen or used or gone in wrong hand then it can also cause disaster. That is why the debate over the protection of data has emerged from the last decade or so and the intensity of debate has further increased after the covid 19 pandemic. The pandemic has

forced the population not only in India but across the world to shift to the digital mode of living of life. We are having our classes online, doctors are providing consultation online, webinars are done online, various social media platforms like WhatsApp, Facebook, Instagram, twitter etc. use internet, payments are largely done online nowadays and many more activities are done virtually today. These activities store large quantity of our data in their servers and it is important in this scenario that this data is protected and used only if permitted by us.

India is rapidly transforming into a digital society and the 21st century has witnessed such an explosive rise in the number of ways in which we use information and that is why it is referred as '**the information age**'[1]. The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction of the other. With nearly 450 million internet users and a growth rate of 7-8 %, India is well on the path to becoming a digital economy, which has a large market for global players.[2]

In 2017 a committee was constituted under the leadership of **Justice B.N. Srikrishna** for the purpose of formulating rules and laws for the protection of data and this committee submitted its report in the year 2018 as Data Protection Bill. This bill was passed in Lok Sabha and thereafter it was sent to a standing expert committee for the purpose of making amendments in some of its disputed provisions.[3] As per the provisions of Personal Data Protection Bill, 2019 the data can be broadly categorized into four types –

1. Personal data – it includes data like name, address etc. of a particular individual which is personal to him. It is the information that relates to an identified of identifiable living individual, and is also known as personally identifiable information (PII)
2. Sensitive personal data – it includes data or information like gender of an individual, health data, data related to his/her finance, data related to caste etc. This kind of data is stored and processed in India but it can also be processed outside also with the permission of the person whose data is being processed and with the permission of a nodal agency which will be set up after this data protection bill becomes an act.
3. Critical personal data – it includes data related to Indian military, armed forces and security agencies. This kind of data is stored and processed only in India and no foreign entity can access it or use it without the permission of Indian government.

[1] Available at: www.legalservicesindia.com (last visited on 15 Nov, 2021)
[2] Data protection in India – Ministry of Electronics and Information Technology
[3] Available in The Hindu on 12 April 2021

4. Non personal data – This category includes data related to traffic rules and patterns, demographic data, data related to weather and climate etc. This data can easily be accessed by Indian government through its fiduciaries.

The basic aim of data protection laws is to protect and prevent the data from the unauthorized access by the rouge element either inside a nation or outside. These laws also aim to give individuals control over the data, empowering them to know how their data is being used, by whom and why, giving them control over how their personal data is being processed and used. In 2019, 73% of customers said trust in companies matters more than it did a year ago, and we can just assume that the numbers have gone up. That is why organizations need to learn how to process personal data while protecting privacy preferences of individuals. This is what individuals expect from organizations.[4]

**ATTACKS ON THE DATA STORED** –

We have witnessed an invasion by technology in almost every sphere of human life but since there are two sides of a coin, the technology also has two sides to it. The greater availability of technology gives access to data easily which has led to cybercrimes. Cybercrimes are defined as a crime in which a computer is the object of the crimes such as hacking, phishing, spamming or is used as a tool to commit an offence.[5]Cyber criminals may use computer technology to access personal information, business trade secrets or use the internet for malicious purposes such as online monitoring of another person's activities, unauthorized users who can access their personal and sensitive information such as banking information etc. The social media is a breeding ground and platform for these attacks. The attackers create fake social media accounts and post misleading information about the concerned person. Many times, the users unknowingly grant certain permissions to the application, which allows it to access their personal information. This gives the application provider with personal information about the individual. So, the users need to be careful while installing mobile applications and be sure of the permissions granted to those applications.

There have been various data breaches seen in news which are limited not only to India but also worldwide. According to a report, around 3.94 lakhs cyber-attacks took place alone in India in 2019 and according to the data of **CERT-IN**, around 336 central ministries websites were hacked between 2017-2019. According to a report of **NASSCOM**, India has seen second

[4] Available at: www.dataprivacymanager.net (last visited on 18 Nov, 2021)
[5] Available in SC Gupta's book of 151 essays

highest number of cyber-attacks between 2016-2018 and IBM's report says that around 140 million rupees were spent because of breaches in various companies.[6] Some famous examples of data breaches are[7] –

1. In June 2021, data of around 700 million users was posted on a dark web forum impacting more than 90% of its users' base. The hackers by the name of "God User" attacked it and tried to sell the data of 700 million users.

2. In April 2019, 533 million users' data including phone numbers, account names, Facebook IDs was posted for free on dark web.
3. In March 2018, there was data breach of around 1.1 billion people who were related to Aadhar which allowed access to private information of Aadhar holders, exposing their names, their unique 12-digit identity numbers and their bank details.
4. The D track malware which infected Kudankulam Power Plant in India which was done by North Korea
5. The Stuxnet virus which attacked and infected Iran's nuclear programme in 2018
6. In May 2017, the issue of data theft of Zomato came in news
7. In May 2017, Wannacry Ransomware was in news because of attack on Andhra Pradesh and West Bengal Police



**ISSUE OF PRIVACY WITH THE DATA STORED** –

The privacy of individuals may be termed as the right to determine how information concerning the individual is communicated to others and how that information is controlled. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose. Some legal experts tend to define privacy as a human right enjoyed by every human being by virtue of his or her existence[8]. It depends on no instrument or charter. Privacy can also be extended to other aspects, including bodily integrity, personal autonomy, protection from state surveillance, dignity, confidentiality etc.

[6] Pratiyogita Darpan Magazine of September 2021
[7] Available at : www.upguard.com (last visited on 18 Nov, 2021)
[8] Supra 3

In fighting against terrorism, various government agencies like **R&AW, CIA, NSA** etc. have engaged in mass and global surveillance. Because of it the human right to privacy has been a subject of international debate. Now there rises a question that whether the right to privacy can co-exist with the current steps of intelligence agencies to access and analyze virtually every detail of an individual's life. A crucial question that arises here is that can the right of privacy be forfeited to strengthen defense against the rogue elements and terrorist organizations.[9] The recent issue related to the Pegasus spyware that was in news because it was alleged that this spyware has been used to target and surveillance hundreds of phones in India related to various eminent personalities including journalists, judges, cabinet ministers etc. It was said to be done for the purpose of internal security and to keep a check on them but here rises the issue of human rights violation. Concept of privacy varies from person to person and if it becomes fundamental, it would open a flood of litigations.

**CASE LAWS ON THE ISSUE OF PRIVACY** –

*Justice K.S. Puttaswamy v Union of India*[10]

The concept of Right to Privacy widely came into news from the case of *Justice K.S. Puttaswamy v Union of India.* A nine-judge bench of the Supreme Court headed by Chief Justice JS Khehar, ruled on 24th August, 2017 that the Right to Privacy is "intrinsic to life and liberty" and thus a fundamental right for Indian citizens under the Constitution of India in Article 21. Thus, no legislation passed by Indian government can violate this right. This judgment has further expanded the ambit of fundamental rights by restricting others from intrusion into one's home, the right to choice of food etc. The Supreme Court also said that it is not possible for citizens to exercise liberty and dignity without privacy. It also increased responsibility of the state in protecting the data of the citizens collected by the government under Aadhar act[11].

*M.P. Sharma and Ors. V Satish Chandra, District Magistrate, Delhi and Ors*.[12]

In the case of *M.P. Sharma and Ors. Vs Satish Chandra, District Magistrate, Delhi and Ors*., the Supreme Court for the first time considered the question whether 'right to privacy' is a fundamental right or not. It was challenged that the warrant issued for search and seizure under

[9] Supra 4
[10] 2017, 10 SCC 1
[11] Supra 1
[12] 1954 AIR 300, 1954 SCR 1077

sections 94 and 96(1) of the Crpc was violating the right to privacy of a person. The court held that these powers does not contravene any of the constitutional provisions.

*Kharak Singh v State of Uttar Pradesh and Ors.* [13]

In *Kharak Singh vs State of Uttar Pradesh and Ors*. i.e., after MP Shah case, the issue raised was whether the domiciliary visit for surveillance at night against the accused was violating Article 21 of the Constitution. It was held by the court that such a visit was in contravention of Article 21, but the majority of judges were of the view that Article 21 does not include any provision for privacy and hence the right to privacy cannot be considered as a fundamental right.

*R. Rajagopal and Anr. V State of Tamil Nadu*[14]

*R. Rajagopal and Anr. vs State of Tamil Nadu* was the first case to explain the evolution and scope of the right to privacy. The Court after examining the whole jurisprudence, scope and evolution of the right to privacy held that though the right to privacy is not directly expressed under the right to life and personal liberty guaranteed by Article 21 but is a part of it and no more just a matter of public record.

*People's Union for Civil Liberties (PUCL) v Union of India*[15]

The case of *People's Union for Civil Liberties (PUCL) vs Union of India* was about telephone tapping and the issue raised was whether the telephone tapping infringes right to privacy or not. It was held by the Hon'ble Supreme Court that the telephonic conversations are private and confidential and therefore, in this case, the right to privacy was violated. It also said that including the right to privacy under Article 21 depends on the facts of the case.

Later in case of *Justice K.S. Puttaswamy*[16], the court finally laid down the law that right to privacy is a fundamental right protected under article 21 of Constitution.

In India, rapid digitisation is taking place which may result in ID theft, fraud, misrepresentation etc. Welfare benefits like pensions, subsidies etc. are also provided using computerised data collected from citizens, so this data has to be secured. Huge number of MNCs are taking data

[13] 1963 AIR 1295, 1964 SCR (1) 332
[14] 1995 AIR 264, 1994 SCC (6) 632
[15] (1997) 1 SCC 301
[16] Supra 9

of millions of Indians abroad without including protection procedures. All these issues make Right to Privacy even more important. Taking into account all these implications, Justice AP Shah panel has advocated for a privacy law in India which could protect privacy in the private and public spheres. He talked about nine principles of privacy to be followed by data collectors like notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness and accountability[17].

**EXISTING LAWS FOR DATA PROTECTION IN INDIA** –

1. The Indian Contract Act[18] provides the parties to have a clause in their contracts which protects the data like a confidentiality clause under *Section 27.*
2. Certain provision in *Information Technology Act, 2000*[19] talks about data protection like
    a) *Section 43 (a), (b) and (i)* – It penalises the person for accessing a secure computer network without the permission of the owner, or downloads, copies or extracts any data in the computer and steals, conceals, destroys, or alters any computer source or data intentionally to cause damage.
    b) *Section 43A* – It says that if any corporate body handling or possessing any sensitive personal data or information in its computer, was not careful in implementing a proper security system and had lost or shared the data. If because of the negligence of a corporate body results in any wrongful loss or wrongful gain to any person then will be held liable to pay damages as compensation not less than five crore rupees
    c) The *Sensitive Personal Data or Information* rules were notified by the government in 2011 which says that while handling sensitive information body corporates and companies are required to follow and adhere to these rules strictly.
    d) *Section 66C* punishes a person for identity theft with an imprisonment of not less than 3 years and fine up to two lakh rupees.
    e) *Section 72* states that if any person who secures access to any electronic record, book, register, correspondence, information, document or any such material

[17] Available at blog.ipleaders.in
[18] Bare act of Indian Contract Act at: www.Legislative.gov.in (last visited on 18 Nov, 2021)
[19] Bare act of Information Technology Act at: www.legislative.gov.in (last visited on 17 Nov, 2021)

without the permission or consent of the person who owns the above mentioned, also if the person disclosed such electronic record, book, register, correspondence, information, document, or any such material to another person without the permission or consent of the owner then he shall be punished with an imprisonment of not less than two years or with fine, not less than rupees one lakh, or maybe both.[20]

3. *Indian Penal Code*[21] also includes certain offences which are used to prevent data like misappropriation of property, theft or criminal breach of trust which leads to imprisonment and fine.
4. The *Copyright Act*[22], as amended, recognises computer databases under the definition of literary work, and thereby copying of computer databases amounts to copyright infringement which has criminal remedies. It protects the Intellectual Property rights of all kinds of work i.e., literary, dramatical, artistic etc.



**CONCLUSION** –

Despite various provisions related to data protection, there is the need of a comprehensive law which specifically deals with data protection. With the advancement of cyber and digital security infrastructure and with the cooperation of all stake holders involved in it, we can definitely reach at a stage where there will be less data theft and cyber-attacks and it will ultimately protect our right of privacy also.



[20] Available at: www.blog.ipleaders.in (last visited on 16 Nov, 2021)
[21] Bare act of Indian Penal Code at: www.legislative.gov.in (last visited on 18 Nov, 2021)
[22] Bare act of Copyright Act at: www.legislative.gov.in (last visited on 18 Nov, 2021)