
LAWS REGARDING RIGHT TO PRIVACY OF PERSONAL DATA IN INDIA

Kishori Goswami, Amity University

ABSTRACT

Globalization and industrialization have sparked a wide range of worldwide changes. One of the things that transformed the world's perception completely was the development of the internet. The internet, which analyses, evaluates, saves, and transfers information in the form of data, is essential to every aspect of our life. Additionally, the COVID-19 and the Digital India project push individuals to switch from paper to data. This change can be characterized as efficient, modern, and environmentally friendly. But at the same time, it intrudes or encroaches upon a person's privacy in a needless and undesired manner. Every human person is born with the inherent right to life, which is a crucial and integral aspect of the right to privacy. The idea that the right to privacy is a fundamental right that is protected by article 21 of the constitution has emerged according to the Supreme Court's numerous rulings. The Information and Technology Act, 2000, which separates data into two categories—personal data and personal sensitive data—was put into place by the Indian government to protect data. Additionally, the I.P.C., 1860 does not directly contain any specific section for data protection; rather, the judge's decision to accept an argument made in court depends entirely on his or her discretion. Under the 2012 Copyright (amendment act), copyright data is protected in India. Although there are other laws governing data privacy, they are insufficient to solve the current complaints of people. Hence, India needs more exhaustive and comprehensible legislation.

Keywords: Privacy, data, Supreme court, government, Article 21, Rights

Introduction

Rapid technological and digital transformation has altered how the world perceives us. The Internet, which the United States of America first created as a weapon during the Cold War, is today a tool in everyone's hands. Virtually every aspect of our life now depends on the Internet. We utilise the Internet for a variety of purposes, including communication, data processing, storing, and learning.

The 1960s saw the beginning of the Internet as a means for states to exchange information. However, the internet was stationary at the time, thus visiting another website was required to transmit information. Later, the US Defense Department encourages the development of ARPANET when the Soviet Union launched a Sputnik satellite from US soil¹. A new communication protocol called TCP/IP was introduced on January 1st, 1983. The Internet was established on January 1, 1983. The ARPANET was discontinued in 1990. HTML (Hyper Text Markup Language), which Berner Lee and his colleagues created, and URL (Uniform Resource Limited). This resulted in the World Wide Web's initial incarnation. When Microsoft released Windows 95, it was a turning point. That year also saw the introduction of Amazon, Yahoo, e-ball, and Internet Explorer. Google ruled the online world starting in the year 2000. However, India was considerably behind the curve in terms of internet usage. In India, educational uses of the Internet were initially observed. The United Nations Development Programme and the Department of Electronics together organised the Educational Research Network, which saw the introduction of the Internet and online systems in 1986. At the time, VSNL was the only telecom operator to build a cybercafé and offer internet access. However, before the www was introduced in India, the common public could not access the Internet on a large scale. In the beginning, VSNL offered Internet Access Service gateways in Bombay, Delhi, Calcutta, and Madras. In 2004, the emphasis was placed on making the Internet accessible to a large number of people at a download speed of 256 kbit/s or greater. The latter data speeds keep improving, going from 1G to 2G to 3G and now 4G. In the coming months or years, businesses are attempting to introduce 5G. In terms of the total number of Internet users, India is now ranked 132 out of 192 nations²

Everything is now processed, saved, and transferred as data thanks to the growth of the internet. The Indian government has also launched the Digital India programme, which aims to convert

¹ Advanced Research Projects Agency Network

² Report of UN Human Development Index in 2021-22

the entire economy to digital and cashless transactions. Although this is a good strategy, it also introduces some undesired and unwelcome intrusions into the privacy of data. Security company FireEye revealed that hackers had obtained the personal data of over 68 lakh patients and doctors in August 2019. Big Basket paid USD 40,000 in 2020 to sell the personal information of its 20 million subscribers on the Darkweb. In January 2000, information on roughly 15 million people was stolen from a government database. It is obvious from looking at all these incidents that our nation has to enact strict data privacy regulations for its citizens.

Objectives:

- To know about data and right to privacy.
- To know about inter-relationship about Right to Privacy and data.
- To know about why protection of data is important.
- Different-different legislations and policies dealing in protection of data.

Research Methodology

A doctrinal research methodology was used to guide the investigation. In order to complete this inquiry and theory composing, a variety of laws cases, panel reports, and preparations made under a variety of laws related to living seeing someone in India and the modern world are combined. Because of this, the study activity has included a clarifying and experimental approach in the development and construction of the proposal.

The final outcome and recommendations are also evaluated utilising fundamental and diagnostic techniques to draw attention to gaps and mistakes in the legal system. Based on the findings, websites, diaries, books, articles, and other sources, a thorough report will be created.

Literature review

According to Section 2(1)(o) of the Information Technology Act, 2000 (the "IT Act"), "data" refers to *"a representation of information, knowledge, facts, concepts or instruction is which are being has are or have been prepared in a formalised manner, and is intended to be processed, is 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 the computer."* The electronic consent framework issued by the Digital Locker Authority defines "data" to mean *"any electronic information that is held by a public or private service provider (like a*

government service department, a bank, a document repository, etc.). This may include both static documents and transactional documents. However, the concept of data is not only restricted to electronic information but also extends to information stored in physical form, e.g. on a piece of paper. “Men inherit some rights by virtue of being human or some by constitution in which liberty, freedom, and privacy are of the utmost importance³. As everything is stored in the form of data whenever we give our consent to use the internet, or worldwide web, or any software. Even the Indian government is moving toward a way to transform the whole economy in the name of digital India. This initiative has so many benefits, like helping in eliminating corruption, saving the environment by minimal use of paper, making information easily and swiftly available to people, and so on. But in the name of all development, we cannot undermine the disadvantages it carries with it. Everything we consent to on the internet or by using any software is processed, transferred, and stored in the form of data. Every message we send on social networking sites such as Gmail, Facebook, or Whatsapp, every item we buy on a shopping site, and every service we obtain from the internet is not only processed and transferred in the form of data, but it is also stored in the form of data. The most shocking fact is that it is not only stored in our devices but also in the thousands of devices that are run or managed by the giant tech company. Nothing is end-to-end encrypted. That’s why everything can be restored on devices after deleting everything. But if everything we do is stored, then what about our privacy? We are not safe because of our personal preference to wear clothes or our intimate communication with our partner and every bank detail we provide while using different software or apps is saved on the devices of those people we don't even see. To save our right to privacy, the Indian government has adopted the following measures:

The Information and Technology Act, 2000

India does not have any comprehensive and exhaustive legislation in the name of data privacy. India has only the I.T. Act, 2011 which deals with data. Under this act, there are two types of data: (a) personal data and (b) sensitive personal data. Passwords, financial information such as bank account or credit card or debit card or other payment instrument details, physical, physiological, and mental health conditions, sexual orientation, medical records and history, and biometric information are all examples of information. While this act only addresses the collection and dissemination of information, it does not address how data will be permanently

³ John Locke in 17th century

stored or deleted in each and every device in which it is processed. This act is silent on data that is available in the public domain. According to this act, personal sensitive data can only be collected by a lawful authority for a lawful purpose and only for that purpose for which it has been given in writing. The person whose data has been collected should be made aware of the fact that his personal sensitive data is being collected with the information, purpose and recipient which processes and retains that data. The information that a person provides can no longer be used for more than the purpose within a reasonable time. The body corporate receiving the information is permitted to disclose sensitive personal data to any third party with the prior consent of the information provider; or where such disclosure is permitted by the terms of the agreement between the recipient and the information provider; or when the disclosure is required to comply with legal requirements.

Judicial measures

Earlier, in *M. P. Sharma and Ors. v. Satish Chandra*⁴ District Magistrate, Delhi and Ors. and *Kharak Singh vs. State of Uttar Pradesh and ors.*⁵, the honourable supreme court refused to recognise the right to privacy was not inclusive under article 21 granted by the constitution. Later on, in the *A.K. Gopalan case*⁶, the Supreme Court recognised that Article 21 consists of the right to liberty. Privacy is an integral part of being liberal. Therefore, the right to privacy comes under the right to liberty, which is an exclusive part that is needed to live. The right to privacy against unnecessary police surveillance is inconsistent to article 21 granted by the constitution and recognised in *Gobind v. State of M.P.*⁷. In *People's Union for Civil Liberties (PUCL) v Union of India*⁸ the Supreme court clearly stated, *"We have, therefore, no hesitation in holding that the right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law"*. *K. S. Puttaswamy (Retd.) v Union of India*⁹ is regarded as a watershed case in the history of the Right to Privacy in India in which the issue regarding the Aadhar card scheme has been raised. Whether personal demographic and biometric data that

⁴ (1964) 1 SCR 334

⁵ 1954 SCR 1077

⁶ 1954 SCR 1077

⁷ (1975) 2 SCC 148

⁸ (1997) 1 SCC 301

⁹ (2015) 8 SCC 735.

has been collected by the Indian government is in breach of the right to privacy which has been granted under Article 21 of the Indian Constitution. In this case, the supreme court has recognised that the right to privacy is an intrinsic and inseparable part of the core of human life and dignity. The state intrusion on the right to life can be positive or negative. If this intrusion was not necessary or against the policy of welfare at large, It must be struck down.

The Indian Penal Code states:

The Indian Penal Code, which was drafted by Lord Macaulay in 1860, does not talk directly so much about privacy. At that time, the internet was not invented, so the encroachment on privacy was not that much of an issue. However, our judges and advocates keenly deal with the section whenever dealing with a case. They indirectly apply the section in right to privacy cases, looking after each and every circumstance. For example, in the case of online stalking or abusing or causing any sexual offence through using the internet, it can come under section 375-77. Likewise, misappropriation of property in section 406. However, it totally depends on the discretion of the judges whether they accept it or not.

National safety:

Natural security is a very crucial issue for any country. Today, almost all countries depend on networking systems. To protect the country from cyber-attacks, countries have developed strong networking systems. The unlawful acquisition of information or data by a government and its authorities can be counted under Section 124a of the I.P.C. act. Further, illegal acquisition of data for terrorism or any other purpose can be dealt with under the Prevention of Terrorism Act and the Terrorism and Disruptive Act.

Intellectual Property Law:

It is important and crucial to recognise data privacy and intellectual property rights under the right framework. Section 63 says, "*Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be liable for infringement. The intellectual property rights of an individual are based on the 'labour, skill, and judgment' factors. If any literary, dramatic, musical, artistic, or cinematographic works are recognised by law, then the protection of the rights of the owner of that work is essential*¹⁰. "Both intellectual property

¹⁰ Copyright (Amendment) Act, 2012

rights and data privacy talks about data protection and unwarranted encroachment on data. Therefore, original work is protected under the Copyright (Amendment) Act, 2012.

Corporate affairs:

In the business world, the control of the data processor or controller has been crucial. Private companies are occasionally responsible for deciding whether or not to share. This is where private and public organisations and the enforcement agency clash. Every time someone wants to order a product or access any information online, there is a commercial asking for their information. Now that this information has been provided, the question of whether or not the authority's data complies with public policy has arisen. Accordingly, in the banking industry, the banker owes the customer a duty of secrecy and confidentiality and is required to refrain from disclosing any information that is in their knowledge. As it conflicted with the right to information and public information, the banking customer's right to privacy was limited in its application.

In another area, the Securities and Exchange Board of India Act (1992) created the SEBI to oversee and control how people's credit information is used.

The Security Exchange Board of India, which is granted broad access to data from the private sector relating to the securities market, serves as the government's intermediary for reactive access under Act 77. SEBI is only allowed to conduct an inspection if it has reasonable grounds to think that: a company has engaged in insider trading or fraud; unfair trading techniques are being employed; or transactions in securities have occurred. This restriction is in place to prevent unauthorised reactionary access.

Consumers:

Due to the age of e-commerce, the privacy of our data is under threat. When we share our data, it is saved on the devices of the companies, and they prefer or recommend our purchase based on this stored data. Sometimes, these private companies sell our personal data on the market, like Facebook, who sells the private data to third parties. In respect of it, only the IT Act 2000 deals with it.

Conclusion

Data which has become our essential part of life is need to be protected by government.

Government should neither focus on U.S. centric or European Union centric model data privacy. But itself develops a model that is based on condition of India. Government needs to protect data by building more stringent and up-dated legislation that not only protect innocent citizen from these tech companies but also punishes stringently and strictly to those who violates it.

REFERENCES:

Journal

“Data Protection and privacy issue in India”, *Economic Law Practice*, 2018

Mr. Jayanta Ghosh * Dr. Uday Shankar, ” PRIVACY AND DATA PROTECTION LAWS IN INDIA: A RIGHTBASED ANALYSIS, *Bharati Law Review*, Oct – Dec, 2016

Website

<https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>

<https://online.jefferson.edu/business/internet-history-timeline/>

<https://selectra.in/internet-speedtest/evolution-of-internet-india>

<https://www.policybazaar.com/>

<https://timesofindia.indiatimes.com/>

Statue

Constitution of India

Indian penal code, 1860

Information technology act, 2000