e-ISSN 2320 –7876 www.ijfans.org
Vol.11, S Iss.2, 2022

Data Privacy – A Part of Human Rights

Dr. Narayan Chandra Sarangi[1], Dr. Biranchi Narayan P Panda[2]
[1] Dean Academics, Xavier Law School, XIM University Bhubaneswar, India
[2] Assistant Professor, Xavier Law School, XIM University Bhubaneswar, India
Email: [1]narayan@xim.edu.in, [2]biranchi@xim.edu.in

Abstract:

Data protection primarily addresses the handling of personal data, which involves unique and distinctive hazards. Personal information may expose a person's identity, relationships, health history, financial information, sexual preferences, and religious convictions. Therefore, processing it might seriously jeopardize someone's right to privacy. The main focus of the current study is to throw light on the need for data privacy, study the threats regarding data privacy and to study the different regulations made for data privacy. The present study is based on the secondary sources of information. Required information has been gathered from different journals, books and internet sources.

Keywords: Relationships, Right To Privacy, Data Protection, Indian Judiciary

INTRODUCTION

Any information that has been recorded in some way is referred to as data. It may exist offline or online, in formats that humans can understand or formats that only computers can read. Not all information is private. A factory sensor counting the cans of beans produced each hour is not handling any personal information. Even though the loss or damage of this information could have a significant negative impact on society or the economy, personal data only qualifies when it relates to an identified or identifiable living individual (the data subject). A data controller is a person or organization that collects and manages personal data.

Although there has always been information about people or information that can be used to identify a person, the term "personal data" was first used formally in the 1970s with the development of the first digital technologies. And up until the present, the fundamental components of this definition have largely remained the same: personal data is simply any information that relates to an identified or identifiable individual.

It is possible for the processing of data, both personal and non-personal, to make people's lives better. It can improve services, encourage medical and public health breakthroughs, and produce

better goods and services. However, the same characteristics that make data processing useful can also pose risks. Data loss or exposure poses a risk of harm to people, systems, businesses, and even states. Data protection specifically addresses the handling of personal data, which involves unique and particular risks. Personal information can reveal a person's identity, relationships, health history, financial information, sexual preferences, and religious beliefs. Therefore, processing it could seriously jeopardise someone's right to privacy.

Providing people with control over their personal data is one of the goals of data privacy regulations. Therefore, in order to preserve the privacy of people' personal information, the majority of data privacy laws establish what are known as "data subject rights." It's crucial to keep in mind that not all of these rights are "absolute," meaning that some only apply under certain conditions.

STATEMENT OF THE PROBLEM

Already at an all-time high, worries over the protection of personal data and information—basically, one's right to privacy—is prevalent. The term "right to privacy" refers to the particular ability of an individual to control the collection, use, and dissemination of personal information. In addition to information about your family, your education, your communications (including phone and mail records), your health, and your money, personal information may also contain specifics about your interests, daily routines, and activities. New worries about data protection and privacy rights have also emerged as a result of the convergence of technologies. Access to personal data and communication are made easier by innovative technology.

SIGNIFICANCE OF THE STUDY

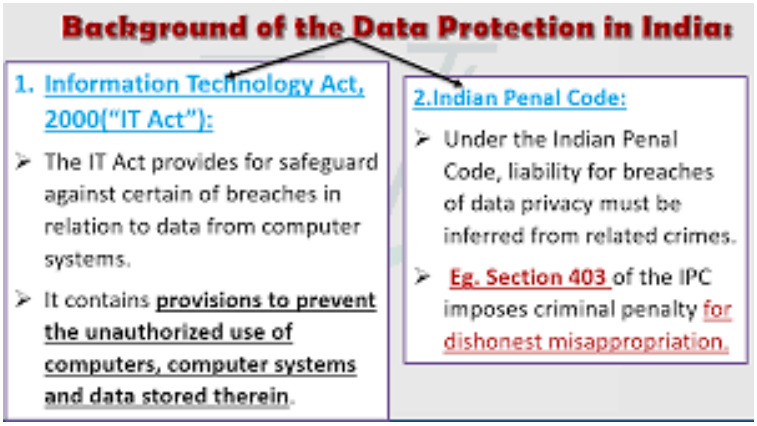
The right to privacy has been seen as an unspoken fundamental right under the Indian Constitution ("Constitution"). The increased frequency of instances when the State infringed this right for valid reasons motivated the Indian Judiciary to take a proactive role in protecting it (that was not always legitimate). A crucial decision on this issue is Kharak Singh v. State of U.P. The Supreme Court ruled that it is against a person's personal liberty to enter their home without their consent and disturb them since their right to privacy is guaranteed by Article 21 of the Constitution. In Gobind v. State of Madhya Pradesh6, the Supreme Court, however, circumscribed the right to privacy and determined that a violation of privacy might be justified by the law.

OBJECTIVES

The main objectives of the study are –
To study the need for data privacy
To discuss the threats regarding the data privacy
To study the different regulation for data privacy

Data Protection & Right to privacy

The terms "data protection" and "right to privacy" are becoming more similar. Only if the invasion of privacy is curbed would "data protection" be conceivable. Informational privacy law in particular, as well as general privacy law, has always been intimately correlated with technological advancement. 33 Warren and Brandeis lament the "instantaneous photographs and newspaper enterprise that have invaded the sacred precincts of private and domestic life," and a number of mechanical devices threaten to fulfill the prophecy that "what is whispered in the closet shall be proclaimed from the house-tops" in their seminal 1890 article "The Right to Privacy." 34 This is when the issue of privacy began. This is currently being developed under "data protection." Data protection is a concept with several facets. The new right to privacy is made up of today's various data protection rights, such as the right of access to data banks, the right to verify their accuracy, the right to keep them current and to make corrections, the right to the confidentiality of sensitive data, and the right to give permission for their dissemination. 35 As a result, the relationship between "Data Protection" and "Privacy" status in this case is quite acceptable.



THREATS TO PRIVACY

The potential of information technology to gather, analyze, and distribute information about persons has increased in complexity, creating a feeling of urgency in the need for privacy laws. Additionally, advances in telecommunications, improved transportation systems, medical research, and financial transactions significantly boosted the amount of information created by each person. Without the need for a single central computer system, computers connected by high-speed networks and equipped with sophisticated processing tools may build full dossiers on any individual. New technologies created by the military sector are being used by commercial businesses, government organizations, and law enforcement. Polls indicate that there is more public awareness about privacy issues today than at any other time in recent memory. People all across the globe voice the same concerns about invasions of privacy, which has prompted an unprecedented number of countries to establish laws particularly safeguarding their residents'

privacy. Human rights organizations are worried that a significant amount of this technology is being transferred to underdeveloped nations with inadequate safeguards. The commerce in surveillance technology now faces minimal obstacles. It is now widely accepted that information technology ("IT") is advancing quickly in terms of power, capacity, and speed. The degree of privacy invasion, or at least the potential for privacy invasion, grows in direct proportion. Beyond these apparent cost and capacity factors, there are many significant trends that support invasions of privacy:

The Information Technology Act, 2000 ("ITA")

The ITA was enacted to provide a thorough regulatory framework for e-commerce. Regarding the right to privacy on the Internet, it is crucial to look at Sections 69 and 75 of the Act. The provision of Section 69 is analogous to Section 5(2) of the Indian Telegraph Act of 1885 which gives the ontroller10 the power to direct any government agency. It is necessary to intercept any information sent via any computer resource in order to ensure Users risk up to 7 years in prison if they fail to surrender their encryption keys. Section 72, however the act's only explicit clause relating to invasion of privacy and confidentiality. It states that anybody who divulges any electronic record's contents without the individual's permission, etc., will result in a year in jail. Sentence that might last for two years, a fine that may cost one lakh rupees or both using both.

However, both of the Information Technology Act of 2000's clauses relate with the government's authority over people's personal information. It is clear from knowledge of the Indian legal situations that there is no Indian law that addresses the preservation of private rights, which is interpretable in the sphere of business dealings between people and companies, or between two people, over a website.

Need for Data Privacy: Urgent Need for Privacy Regulations

India must work with the international community to adopt rules that firmly address the protection of privacy and personal data, particularly in light of the expansion and ramifications of global commerce and the impact of the Internet. Due to India's lax privacy laws, several nations (such as those in the EU) are now reluctant to deal with that country. This is especially important as India develops into a hub for the outsourcing of many back-office tasks including credit processing, medical transcription, etc. Threats to privacy also stand in the way of creating a safe online environment for communication. India cannot fully profit from the enormous prospects and advantages those e-commerce offers to emerging countries like ours until these problems are resolved.

The techniques and objectives of assimilation of personal data offline and online must be outlined in a legal framework that is formed. No data should be gathered without the explicit agreement of the consumer, who must be made aware of the voluntary exchange of information.

The ability to effectively strike a balance between individual freedoms and safe methods of business will determine the future of India's trade.

Current Issues Surrounding Data Privacy:

i. Before interfering with fundamental rights, the State must first satisfy three requirements set down by the Honorable Supreme Court. The State may intervene to protect legitimate state interests, but in order to do so, the following requirements must be satisfied: (a) there must be a law in place to justify an invasion of privacy, as required by Article 21 of the Constitution; (b) the nature and content of the law imposing the restriction must fall within the zone of reasonableness mandated by Article 14; and (c) the means which are adopted by the legislature must be proportional to the object and n As a result, going ahead, any law that seeks to violate someone's right to privacy would have to satisfy the proportionality and reasonableness test. A few years will pass before the legal precedent for what constitutes appropriate and proportionate State engagement is established. In light of this decision, the validity of the Adhar Scheme will now be evaluated.

ii. It is often stated that India need to switch from the current "consent based" approach of data protection to one that is "rights based." Once the user's permission has been gained, the data controller is free to use, handle, and share the data with any third parties. However, few people at the time of giving permission are aware of the true repercussions of the improper data sharing. The "rights based" approach, on the other hand, gives users more control over their data while requiring the data controller to make sure those users' rights are upheld. As a result, consumers have more control over their personal data.

iii. The Hon'ble Supreme Court's ruling gives Indian people the right to file a lawsuit if their rights to data privacy are violated. The privacy and protection practices followed by IT businesses in India may be impacted by this. Users may assert their basic right to privacy in addition to claims based on torts

General Data Protection Regulation (GDPR)

A series of laws known as the General Data Protection Regulation (GDPR) governs the gathering and use of personal information about natural people in the European Union (EU). The new framework intends to make data protection and privacy regulations more uniform across EU member states. Three categories make up the GDPR.

The guiding principles serve as the framework and foundation for the management or handling of private data protection. In connection to basic human rights, the principles generally give the guidelines and features of private data.

The Individual Rights describe what the data subjects should anticipate in terms of their considered privacy rights.

Accountability and governance make an effort to outline the functions and duties of corporate organisations with regard to the protection of personal information. In conclusion, the GDPR addressed a number of individual rights, such as the right to information, the right of access, the right to rectification or erasure, the right to restrict processing, the right to data portability, the right to object, and the rights relating to automated decision-making, including profiling. Included in them are permission, contract, legal duty, vital interests, public task, legitimate interests, special category data, and criminal offence data, all of which are supported by legal rules as valid bases for data processing. To accomplish the aforementioned, the GDPR required that enterprises make conscious and reasonable efforts to protect individual right to privacy. Contracts, documentation, data protection by design and default, data protection impact assessments, data protection officers, codes of conduct, and certification must all be a part of this Endeavour under the accountability and governance umbrella.

Data Protection & Indian Penal Code

The British ruled India at the time the Indian Penal Code was first written. The initial draught of the introduction was created in the 1860s under Lord Macaulay's direction. This means that the relationship between "data protection" and the "Indian Penal Code" clause is not entirely meeting all needs. Data privacy violations are not directly addressed under Indian criminal law. Liability for such violations must be derived from related offences under the Indian Penal Code. For instance, the dishonest misappropriation or conversion of "movable property"58 for one's personal use is punishable under Section 403 of the Indian Penal Code. When anything falls under someone else's responsibility, the issue of whose rights should be safeguarded arises. Anyone who misappropriates another person's property is subject to criminal breach of trust penalties, according to Sections 405 and 409. Another section of the law, Section 378, states that it is theft to dishonestly remove any moveable object from the custody of another person without that person's agreement. As of this writing, however, there is no specific law covering the protection of electronic data. There are two ways to approach the legal rights that one may exercise in this matter. Actually, only the state is the target of the crime. Therefore, it is a

fundamental worry that the state has the authority to uphold law and order. Penalties are included in the Penal Code, and in civil lawsuits, laws for damages, including the amount of damages, must be decided by a jury's verdict59. It makes perfect sense to bring up this point in order to address the appropriate problem. In addressing the right, the link between "data protection" and "Indian Penal Code" is relevant. In this context, the state is also responsible for protecting personal data of people.

FINDINGS

It has been found from the study that –

- There is a great threat to the violation of the data privacy in this ultra modern age of technology
- Supreme court has made laws and provisions for keeping the privacy of data.
- Different regulations have been made time to time for maintaining privacy.

CONCLUSION

Even though data security and governance are included in the human rights treaty, the lack of regulation is one reason why user data is still vulnerable. The development of new technology and the fact that there were 4.66 billion active internet users worldwide (as of January 2021) make regulation all the more difficult. It is time that national governments acknowledge this growing need for data security and create laws or legislations that govern an individual's right to data privacy. Proper use of technology requires careful governance and administration, as it is a challenge faced by many people today.

Reference:

- Asia-Pacific Economic Cooperation (2005) APEC Privacy Framework. December. Singapore: APEC Secretariat.
- Cavoukian, Ann (2011). Privacy by Design: The 7 Foundational Principles. January. Ontario, Canada: Information and Privacy Commissioner of Ontario.
- Economic Community of West African States (2010). Supplementary Act A/ SA.1/01/10 on Personal Data Protection within ECOWAS. 16 February.
- H.M. Seervai, Constitutional law of India, Vol.2, 2007, Universal law publishing co
- International Organization for Migration (2010). IOM Data Protection Manual. Geneva, Switzerland: IOM.
- The Commission, by a majority vote, took the opposite view: see Guerra and Others v Italy (1996) Appl 14967/89, reported at [1996] VII HRCD 878.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 17 April. A/HRC/23/40, p. 6
- United Nations (1989). Convention on the Rights of the Child. Treaty Series 1577 (1989): 3 (art. 16)
- United Nations General Assembly (2016). Quadrennial comprehensive policy review of operational activities for development of the United Nations system. 28 October. A/C.2/71/L.37.
- World Health Organization (2016). Guidance on Good Data and Record Management Practices. WHO Technical Report Series, No. 996. Annex 5.