IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CHALLENGES TO PRIVACY AND DATA PROTECTION IN INDIA

Maithreyi BS

Student, LLM (Constitution and Administrative Law)

School of Law

Christ University, Bangalore, India

Abstract: This research explores the subject of privacy from an Indian viewpoint, focusing on challenges in three areas: legal, technical, and political. To address these issues, we have suggested a framework. Advances in technology, such as mobility (geographic knowledge discovery), data mining, cloud computing, and so on, carry with them unanticipated concerns, one of which is the threat to "privacy." We can now access any information on anyone and from any location, but this creates a new threat to private and protected data. Due to the greater worldwide adoption of technology, many nations have implemented diverse legal frameworks, but India lacks a comprehensive legislative framework that addresses privacy concerns. To address serious cyber threats, we turn to the Information Technology Act of 2000, which was enacted to facilitate e-commerce and hence did not prioritize privacy. This proposed framework offers a comprehensive solution addressing current and future privacy needs in the Indian context. "The true power of any legislation resides in its ability and ease of enforcement," as it is accurately noted.

Indexed Terms **– Data Protection, Privacy, Challenges.**

I. INTRODUCTION:

The term "privacy" might imply different things to different people in different situations. Perhaps it was our culture and way of life, or maybe the lawmakers' lack of foresight into impending and rapidly evolving technologies, that compelled them to leave the privacy problem out of the country's legislative framework. We need to define privacy before we can talk about e-privacy and data protection in India. The term "privacy" is derived from the Latin word "privatus," which means "to be apart from the rest." It's described as a person's or a group's capacity to keep themselves or information about themselves hidden and then selectively reveal it.

When it comes to privacy, it may be defined as an individual's right to determine who has access to their information, when they have access to it, and what information that people have access to. As per Article 21, of our Indian constitution, privacy is a form of personal liberty. "Protection of Life and Personal Liberty" means that no one's life or personal liberty may be taken away unless and until legal procedures have been followed. One of the essential rights protected by the constitution is the right to privacy, which is included in the list I.

At the international level, privacy is recognized as a Human Right[1] in various dimensions, including the privacy of the individual, privacy of personal activity, the privacy of personal communication, and privacy of personal data.

Contrary to popular belief, the phrases privacy and confidentiality are not interchangeable. The terms privacy, confidentiality, and information security are sometimes used interchangeably, yet each term has its own particular meaning and use in the information security field. In its most basic definition, "confidentiality" refers to the exercise of judgement in the safeguarding of confidential information.

II. LEGAL CHALLENGES:

As there is no proper privacy legislation model in India, it is incredibly difficult to ensure that privacy rights are protected. However, in the absence of formal legislation, the government employs a few proxy laws or incident safeguards for privacy purposes.[2]

Article 21[3] of the Indian Constitution, the IT Act 2000[4], the Indian Contract Act 1872[5], the Indian Penal Code 1860[6], the Indian Copyright Act 1957[7], the Consumer Protection Act 1986[8], the Specific Relief Act 1963[9], and the Indian Telegraph Act 1885[10], all provide indirect support to privacy concerns in India.

In the current Indian legislative framework for privacy, there are the following deficiencies.

- There is no comprehensive law, and the question of privacy is still handled by a proxy, therefore there is no consensus on the subject of privacy.
- Information is not classified as public information, private information, or sensitive information.
- There is no legal structure that covers private and sensitive data and information ownership.
- There is no standard protocol for creating, processing, transferring, or storing data.
- There is no standard that determines data quality, proportionality, or transparency.
- There is no structure that addresses the issue of cross-border information transmission.

Such a shortcoming in the legal structure cannot be disregarded in this age of information technology, as it can have major ramifications for both the person and the nation.

III. TECHNOLOGICAL CHALLENGES:

Indian information has been substantially modified as a result of globalisation and the Information and Communications Technology (ICT) revolution[11]. It improved the portability and accessibility of information. Not just the corporate sector, but also the government sector and even individuals desire to be adaptable and clever in today's world. Despite the fact that it has made our lives easier, faster, and more advanced, it has also brought about some unexpected mayhem and made our personal lives more visible.

Biometrics (fingerprints, hand geometry, face, voice, iris, and keystroke recognition), RFID, Smart cards, Voice over Internet Protocol (VoIP), Wireless technologies, Location detection technologies (such as Global Positioning Systems), Data-matching and data mining technologies, and Surveillance Technologies are some of the technologies that have the potential to impact privacy.

Technology has developed to the point that computers can now not only store large volumes of data but can also automatically filter through, extract, and compare data from large amounts of data. Data matching is a type of data mining that requires looking at specific bits of data or patterns within data to see whether they indicate a particular trait, propensity, or behaviour that may be predicted. Data-matching poses a unique threat to personal privacy because it includes evaluating information about huge groups of persons without a suspicion of committing a crime. When data warehouses are handled by third parties, such as business process outsourcing (BPO) companies, this sector becomes even more important.

"Privacy shields us from abuses by those in authority, even if we're doing nothing wrong at the time of surveillance," explains security expert Bruce Schneier[12]. A number of Internet security and privacy professionals say that "security doesn't exist" and that "privacy is dead-get over it." Cookies and site loggers have made private information more susceptible on the internet.

IV. POLITICAL AND SOCIAL CHALLENGES:

Any technology must be supported by a robust human resource infrastructure in order to be successful. When it comes to political issues, those active in a certain technology are discussed. People are the weakest link in the chain of information protection, according to the Information Technology principle.

People play a critical part in the Indian scene; they are the policymakers who will decide and lead the way for any technology. Though the privacy issue is not at its pinnacle in our culture since individuals are indifferent about their privacy and there is yet to be a privacy-related scam, it is frequently stated that prevention is better than cure. The majority of BPO offshore business comes from nations that have formalized their statutory framework.

They do business in India since the cost of capital is so low. They take proper care of their data by following the guidelines set forth by non-governmental international organizations such as ISO[13], ITIL[14], and others. The majority of cases are in family court because of a breach of privacy based on a breach of trust between two parties. The media is critical in informing individuals about government policies and public grievances in a democracy, however today's media has encroached on public life, and no one's personal information is kept secure for their own advantage.

India has embraced new technology, and there is a new trend of connecting people through social networking sites like Instagram and Facebook, where we may meet others who have similar interests and build communities. Many people share information on current events, express their opinions, and critique certain issues in such networks. All of these activities have the potential to raise sensitive issues, resulting in a contagious and unbalanced society. In today's environment, blogs are becoming increasingly popular. People can

publish their views and opinions on blogs, but private information may be created in the public and government sectors, and the original goal may be lost.

V. CURRENT SYSTEM:

Though India does not have codified legislation to deal with privacy, as noted above, the IPC[15], Information Technology Act 2008, Copyright Act, Special Relief Act, Telegraph Act, Contract Act[16], Article 21, and a variety of other laws are used to deal with key privacy issues. The Indian government has approved a special law on privacy, the Information Technology Act, 2008, which provides a basic definition of privacy.

As privacy is the most crucial personal characteristic, every case that is now pending in court will cause mental harassment for the user. For speedy decisions in India, a swift judicial system is essential.

The judgment of the Delhi State Consumer Disputes Redressal Commission (the "Commission"), which fined Airtel, the Cellular Operators Association of India ("COAI"), ICICI Bank, and American Express Bank a total of Rs.75 lakhs on a complaint of consumer harassment by unsolicited telemarketing calls and text messages, assumes enormous significance in this context. In 1997, the Supreme Court of India instructed the Reserve Bank of India ("RBI") to create and execute methods to avoid unwanted calls, citing the right to privacy as a fundamental right.

A tort is classified as a discretionary action. Maneka Gandhi sued Khushwant Singh's book Truth, love, and a little malice in the Delhi High Court, claiming that it infringed on her privacy. Khushwant Singh won his case in court. The two-judge bench pointed out that Article 21's right to privacy could only be utilized to challenge government activities, not private companies. Article 21's main objective, as demonstrated in the preceding example, is to protect an individual's privacy from the state.

India passed the Right to Information (RTI) Act, 2005 which mandates the disclosure of public information when it is requested. It has been observed that RTI infringes on personal information. It is necessary to specify privacy and information classification for the proper deployment of RTI so that it can assist in the disclosure of information without interfering with ordinary operations.

VI. PROPOSED FRAME WORK:

To be considerate of the privacy of others, we must adopt the framework stated above as part of our work culture in India, as it clearly specifies broad principles for information management at all stages. During the course of evaluating the threat to privacy and working to eliminate the system's vulnerability, we take all required safeguards. This model lowers the danger of privacy invasion to the level of one's tolerance for risk. Therefore, any subsequent threat to privacy will have a less significant impact. The process of protecting personal information is divided into four parts. They are as follows:

- Data Collection
- Data Security
- Data Process, and
- Data Access

VII. DATA PROTECTION BILL, 2019:

India lacks a comprehensive law that governs data protection and privacy. The existing legislation and approaches are primarily sectoral. The government is also working on detailed data privacy and protection legislation. A panel of experts on privacy, chaired by Justice A.P. Shah, former Chief Justice of the Hon'ble High Court of Delhi, began more serious steps in this regard on October 16, 2012, when it issued a full report. It all started in 2012 with the case of Justice K.S. Puttaswammy (Retired) against Union of India and Ors.[17]

Under the chairmanship of Justice Srikrishna, a former Supreme Court of India judge, the government established an expert committee to investigate various issues relating to data protection in India, make specific recommendations to the Central Government on principles to be considered for data protection in India, and proposed a data protection bill. The bill's first proposal was filed by the committee in July of 2018. The Personal Data Protection Bill, 2019, was tabled by Mr. Ravi Shankar Prasad, Minister of Electronics and Information Technology, on December 11, 2019.

The Joint Committee of Parliament (JCP) has been allowed a sixth extension to produce its report on India's Personal Data Protection (PDP) law. The report will now be presented by the JCP during the first week of the Winter Session, in late November 2021.

This specific data protection regulation has yet to be passed in India. The Indian Congress revised the Information Technology Act (2000) to include Sections 43A and 72A, which offer a right to compensation for the improper disclosure of personal information.

VIII. CONCLUSION:

In three dimensions, the suggested system includes all domains: legal, technical, and political. It has been attempted in the proposed system to cover many domains as per the current scenario, bearing in mind the rapid improvement in technology and developing areas. The proposed method allows for advancement without interfering with other domains, allowing for the addition of new domains. The suggested system is adjustable and expandable to satisfy not only present but also future demands. A well-structured framework for privacy is critical not only for individuals but also for society and the country's economic progress.

REFERENCES:

1. PRIVACY AND HUMAN RIGHTS http://gilc.org/privacy/survey/intro.html, last accessed 27/01/2022 at 11;40.
2. Ponnurangam Kumaraguru, Privacy in India http://www.cs.cmu.edu/~ponguru/iaap_nov_2021.pdf, last accessed 27/01/2022 at 15;40.
3. Article 21 of the Constitution of India: The Expanding Horizons (Maheshwari Vidhan) last accessed 27/01/2021 at 18;40 http://www.legalserviceindia.com/articles/art222.htm,
4. IT Act 2000, Gazette of India Part 2 –Section 1
5. Indian Contract Act 1872, ACT No. 9, 1872
6. The Indian Penal Code 1860, ACT No. 45, 1860
7. Indian Copyright Act 1957, ACT No. 14, 1957
8. Consumer Protection Act 1986, ACT No. 68, 1986
9. Specific Relief Act 1963, ACT No. 47, 1963
10. The Indian Telegraph Act, 1885
11. Philip E. Agre, Marc Rotenberg Technology and privacy: the new landscape, last accessed 26/01/2022 at 18;40. http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false
12. Bruce Schneier The Eternal Value of Privacy last accessed 10/01/2021 at 13;30 http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886
13. International Organization for Standardization
14. Information Technology Infrastructure Library
15. The Indian Penal Code 1860, ACT No. 45, 1860
16. Indian Contract Act 1872, ACT No. 9, 1872
17. (2017) 10 SCC 1