Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Data Privacy in Cyberspace: A Comprehensive Study on Strategies, Regulations, and Technologies

Jayshree Chaudhary[1] , Mahima Kaushik[2], Surender Kumar[3],
[1]*Assistant Professor (School of Law, JECRC University Jaipur)*

ARTICLE INFO

Received: 21 Oct 2024

Revised: 26 Nov 2024

Accepted: 21 Dec 2024

ABSTRACT

Expression "Data Protection" refers to an organized system of rules, regulations, and policies enacted by the government and regulatory bodies that safeguard people's personal information while avoiding misuse of information resulting from illegal activities such as unconsented along with illegal preservation or propagation of data. The cyber security regulations in India are relevant and mentioned in different data protection legislation in India, in addition to the right to privacy as a component of right to life, which is a basic right under Art. 19 as well as 21 of Indian Constitution. Yet, as with all other basic rights, India's Cyber Security and Data Protection regulations are restricted by appropriate constraints.

The cyber safety and protection of data regulations in India lack clear legislative underpinning, although the confidentiality of data rules in India are governed by the Information Technology Act of 2000 and the Indian Contract Act of 1872.

Furthermore, safeguarding individual information standards are included into India's cyber security and data protection laws, which control business organizations with regard to privacy.

Because of a growing amount of internet users, abuse of gadgets in cyberspace has grown, giving rise to cybercrime. This study paper discusses all of the key topics of best data protection, privacy of persons in cyberspace, and best use of electronic devices via legal initiative.

Keywords: Cybersecurity, Data Privacy, Fundamental Rights, IT Act, Cyberspace.

INTRODUCTION

Section 2(1) (o) of IT Act 2000 determines "data" to be a depiction that includes understanding, information, ideas, or directions which are being created or are currently being created in a formalized manner, as well as is designed to be analysed is being handled, or currently is being handled in an electronic system or networks of computers, while may be in any format (which incorporates computer systems copies, magnetized or visual media for storing data, card punches, pushed tapes) or maintained privately in the storage device.
According to Data Protection Rules- an individual's 'Sensitive Private Information or Data' includes-

- Passwords; monetary data; biological; along with mental wellness illnesses; gender identity; health records as well as the past; biographical data; and additional specifics.

Submitted that anything which is openly accessible or made publicly available in the public realm or made available within any legislation in effect at the time is not regarded as private information that is sensitive.

[1] jayshreechaudhary98@gmail.com.
[2] mahima.kaushik08@gmail.com.
[3] surenderkumarbishnoi16@gmail.com.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Right to Privacy as a Fundamental Right

Part III of the Indian Constitution does not include the obligation to privacy as one of its Fundamental Rights. None of each of the three listings in Schedule VII of the Indian Constitution use the term "privacy." The "Right to Life and Personal Liberty" under Article 21 of the Constitution safeguards individuals' fundamental right to privacy. Article 19(1)(a) guarantees the right to freedom of speech and expression, which means that any individual has the right to convey his opinion on specific questions under certain boundaries.
In Justice K.S.Pttaswamy (Retd) and Anr v. UOI and Ors,20 the Supreme Court proclaims 'privacy to be a basic right' and overturns the verdicts rendered in the M.P.Sharma case in 1958 and the Khark Singh case. In this case, Dr. D. Y. CHANDRACHUD, J. ruled that the right to privacy is "protected as a fundamental component of one's right to life and liberty for oneself under Article 21 and as an integral component of the freedoms provided by Part III of the Constitution."[4]

Invasion Of Confidentiality in the Cyber World:
Because of the overabundance of reliance on a machine as an instrument for sharing information as well as data preservation, and the utilization of the internet to be a means to facilitate data exchange, different hackers engage in the process of obtaining information that has been discussed via the internet through the individual, in two ways via the use of noxious malware, or via different computing glitches, or just via the information gathered from the web page, that accumulates in the gadget's cookie information file.[5] Furthermore, every bit of data that a person posts in his or her social networking description, such as LinkedIn, Twitter, Facebook, Instagram, and furthermore, can be obtained readily through any invader & can be twisted as well as exploited, generating security difficulties of those affected users of social networks.
Concerns include email attachments carrying viruses which reveal the receiver's private details to the sender of the email or any invader. person who uses the internet are particularly obvious targets for invaders since thieves can simply trace every piece of their data supplied to them.[6]

Interface between the Information Technology Act and Data Privacy

There are just a few clauses in the I T Act of 2006 that directly address data privacy issues. Section 72 of the IT Act establishes responsibility for breaches of confidentiality and privacy. Section 43A mandates accountability for data breaches, but only for Critical private data. Every business entity that handles this information is accountable for protecting its confidentiality. Section 38, 2011, Sensitive Data rules which protecting vulnerable identifiable information or data defines as personal information, which includes economic and sensitive data about individuals.

Bill which saves information, known as Personal Data (Protection) Bill of 2019, was recently introduced in the House. The Bill does not define privacy; rather, It emphasizes protecting private and highly valuable private information of individuals. The bill suggests giving overriding effect on all current legislation directly or indirectly linked to privacy. It intends to ban anybody from collecting, sharing, processing, disclosing, or otherwise handling another person's personal data unless in conformity in respect of the provisions included in the suggested bill. The Bill indicates protecting people's private information.[7]

This is important to understand that the fact that there isn't any safeguarding of privacy for information on social networking sites.

Likewise, government agencies obtain people' information via the Aadhar identification card system without ensuring security. The Bill defines 'Personal Data' as biometric data such as sexual orientation, past medical treatment and wellness, political beliefs, religion, race, caste, monetary, and credit-related data. This term differs

[4] Justice K S Puttaswamy (Retd) and Another v. Union of India and Others (2017) 10 SCC 1
[5] Shaswati Das, 11,592 cases of cybercrime registered in India in 2019 : NCRB, 06 Apr 2024
[6] Aashit Shah and Nilesh Zacharias “Right to Privacy and Data Protection”.
[7] Report on Cyber Security & Right to Privacy submitted by the Parliamentary Standing Committee on Information Technology Act presented on Feb 12th 2014, under the chairmanship of Rao Inderjit Singh to the fifteenth of the Lok Sabha

from that defined within the Appropriate Safety Prevention and Measures and Critical Personal Information and Databases Rule 2011.
As a result, the Bill broadens the definition of personal data. The bill also provides exceptions to data privacy violations based on medical emergencies, national security, prosecution for a cognizable offense, and so on.[8] The Bill states that if an infraction is committed, the individual is subject to harsh legal consequences, possibly imprisonment and a fine. This does not need an evaluation of intention or mens rea.

Data Protection Technologies and Practices to Secure Data

When it comes to data protection, you have several managing and storing options to choose between. Solutions can assist you in controlling access, monitoring activities, and responding to threats. Here are a few of the many widely utilized practices and technology. [9]

Data Discovery**-** While you are able to protect your data, you must first identify whatever it contains and in which location it is stored. This method, also referred to as data discovery, is critical for discovering sensitive information and establishing the most effective ways to safeguard it.

Data Mapping**-** Data mapping is the next phase in data discovery, and it entails determining the locations that hold your information and how it moves across your company. This helps you understand the links between different data types and frameworks, providing you to make more educated data protection decisions.

Automated Discovery Systems- To speed up the information discovery process, many businesses are increasingly using automated systems that can scan and detect sensitive material. These applications can help you maintain track of your information inventory and stay informed of any modifications or additions.
Data Loss Prevention (DLP)- an important aspect of data security that prevents illicit use, leakage, or theft of sensitive information. DLP technologies are made up of a variety of tools and procedures that help firms keep ownership of their data.
DLP Policies– Creating and executing DLP policies is an important first step toward securing your data. These policies lay out the rules and processes for handling vulnerable information and ought to have adjusted to your organization's unique requirements.
Monitoring and Alerts- DLP technology frequently integrate monitoring and alert systems to identify possible data breaches or other security events. These systems can monitor user activity and detect any suspicious conduct or efforts to gain access to sensitive data.
Local and Offshore Backups- It is critical to have local and offshore copies of your data. Local backups allow instant access to your data, and remote backups provide further security against calamities like fires and floods.

Privacy Invading Technology

Technological developments are weakening the foundations of privacy rights. Privacy-invading technology may include the following:

1. GUID **-** Globally Unique Identifier: This is software incorporated in computer hardware that enables eavesdropping on all machines linked via LAN.

2. E-mail and document bugs**:** This technology detects and determines if the receiver has viewed the addressed e-mail or document.

[8] Privacy in cyberspace | The Indian Express
[9] Mr. Mahantesh B. Madiwalar, "Privacy Rights And Data Protection In Cyberspace With Special Reference To E-Commerce", Bharati Law Review, April – June, 2017

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Cookies**:** When someone browses the internet, he or she leaves electronic trails wherever they go. A software program known as a 'cookie' may be transferred from a website to a user's computer and remain there until the site is next viewed, at which point facts about the user and his/her past visits to the site are automatically communicated.

4. Spyware: Spyware is a term used to describe applications that track practically everything an individual does on their computer. This spyware application captures everything without the user's awareness. These apps can record keystrokes, website visits, program runs, access to the internet, instantaneous messages, messages sent and received, e-mails, chat discussions, passwords entered, windows opened, filed, and documents visited, as well as snapshots of the system's desktop.
5. Camera: Digital cameras are compact and inexpensive, there is no need to purchase film, undesired photos can be erased, and hundreds of images can be readily stored on a computer. With the use of the internet, images can be shared with people all over the world. Simultaneously, the video camera has the potential to cause significant damage. Because their cameras are so compact, people are more inclined to have them with themselves at all times. Again, you have not any requirement for film, therefore taking photo after image is free.
6. Web bugs: A website-bug, additionally referred to as an internet beacon, is a component of a file that can be embedded on an internet site or in an email message in order to track user behavior and serves as a type of spyware. [10]

Indian Laws and the Concept of Data Protection

As previously stated, there are no particular statutes controlling the security and privacy of data in India. However, the legal difficulties including punitive sanctions and remedial remedies are comprehensively addressed in the IT Act of 2000,[11] which describes the scope of India's data privacy legislation, as well as the Indian Contract Act of 1872.[12] In India, there is currently no unique legislation governing an individual's privacy rights. Only the Information Technology statute of 2000 addresses cybercrimes and offers remedies for violations of the statute. The legislation has a few measures concerning individuals' privacy, however they are not extensive in nature. [13]
According to Section 43A of the IT Act of 2000, if a body corporate possesses, deals with, or handles any responsive personally identifiable information of an individual and is careless in establishing and upholding reasonable security practices to protect the data, resulting in accidental damage or wrongful gain to any person, such body commercial may be held liable to pay that damage to the person affected. It is crucial to understand that the act does not specify a maximum amount in damages that can be requested by the aggrieved party in such situations.

- *Penalty for violating citizens' confidentiality and privacy*- Under Section 72A of the IT Act of 2000, the disclosure of information knowingly and intentionally without no the permission of the individual concerned and in violation of the lawful contract is punishable by imprisonment for three years and a fine of Rs 5,00,000.
- *Governmental Interference with Data- Section* 69 of the Act allows the government to interfere with data if it is essential for the integrity and sovereignty of India, defence, security, cooperation with foreign states, public order, or other legitimate interests.

National Cyber Security Policy, 2013

The National Cyber Security Policy 2013, released by the Department of Electronics and Information Technology (DeitY), issued as an organizational structure that helps public or commercial enterprise in defending their data from online assaults.

[10] Bob Whitehead, Invasion of privacy laws and video surveillance --what's legal, what's not? http://www.video-surveillanceguide.com/3048-invasion-of-privacy-laws.htm
[11] IT Act 2000, Gazette of India Part 2
[12] Indian Contract Act 1872, ACT No. 9, 1872
[13] Stubb, Kasiva, "data protection and privacy: cyber security laws in India", 2023

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

National Cyber Security strategy seeks for establishing and refining updated rules for enhancing safety of India's cyber atmosphere. The policy seeks to generate and train over 500,000 highly qualified information technology workers over the next five years. [14]
The NSCP aims to provide

- a secure and resilient cyberspace for individuals, corporations, and the government.
- It also monitors and safeguards digital architecture or knowledge lowering weaknesses or increasing protection from cyberattacks.

- Developing structures, abilities, or the susceptibility management methods to minimize, prevent, and respond to cyber incidents and threats.

- Encouraging groups to build digital security regulations that match via corporate objectives, company procedures, or industry standards.

- Develop organizational frameworks, staff, procedures, technology, and equipment to mitigate cybercrime harm.

National Cyber Security Strategy,2020

National Cyber Security Strategy, 2020- Indian government's long-awaited follow-up strategy to strengthen cybersecurity measures. While the strategy is currently being developed and reviewed by the National Security Council Secretariat, its primary purpose is to serve as formal advice for customers, Lawmakers and Business Executives in preventing cyber mishaps, terrorist attacks, and espionage in cyberspace.

The plan intends to increase the quality of cybersecurity audits, allowing firms to perform more thorough examinations of their protection structure with its understanding. Here expectation is that after regulation is adopted, cyber inspectors are going to enhance company's safety requirements, pushing firms to strengthen their security processes.

Legal Challenges

Here is a shortage of effective privacy regulations in India, making it incredibly challenging to guarantee personal rights are protected. However, in the lack of particular legislation, the government relies on a few substitute laws or incident safeguards to protect privacy.
The current Indian legal framework for privacy has the following lacuna:

- Here is no general legislation to address privacy concerns, and there is no consensus among proxy providers.
- There is no designation of information as public, private, or sensitive information.
- There is no legal framework that addresses the management of sensitive and confidential knowledge and data.
- No standard technique for producing, processing, transferring, and storing information.
- No guidelines specify data quality, proportionality, or disclosure.
- No framework addresses cross-country information movement.

In this day and age of information technology, these gaps in the legal structure has not been ignored and can have serious consequences for both individuals and nations.
India has implemented the Right to Knowledge (RTI) Act, which addresses the sharing of accessible data when

[14] Anita A.Patil, "The era of e-consumerism and issues concerned" Indian Bar Review, Vol.XLI (2) 2014.

required. RTI has been observed to infringe on private data. For the The effective deployment of RTI, it is necessary to specify privacy and information categorization so that information may be disclosed without disrupting ordinary activity. [15]

In India, health-related privacy problems are addressed through the use of constitutional articles such as Mr. 'X' v. Hospital 'Z' was the first occasion the Supreme Court ruled on sensitive health-related data. In this instance, the appellant's blood was tested at the respondent's facility and he was discovered to be HIV positive. Several others, including his family and members of their community, became aware of his HIV (+) diagnosis and were shunned by the community. He filed a complaint with the National Commission over the defendant hospital, claiming damages for releasing health-related information that, according to him, should have been kept secret under ethical standards. The National Commission dismissed his case outright.

Meanwhile, he proceeded to the apex court by means of an appeal. The Supreme Court stated that the Right to Privacy, as a fundamental human right, is susceptible to authorized action for crime prevention, health protection, morals, and freedom for others.
However, there is currently no such framework for health companies to adopt health-related data privacy protections. Apart from the legislative framework. There are a range of privacy-enhancing technologies (PET) that play a key role in securing user information. PET are application mechanisms that are implemented with online applications to safeguard personal data as well as user identification across the network.

CONCLUSION

Despite the presence of a statutory framework and a number of national and international information security agencies and groups, privacy abuse persists on a large and chronic scale, since present legislation cannot adequately enforce it. We might cite several factors, but in recent years, buying parity has risen owing to the internet.
Many customers do not want to bear additional burdens because, nowadays, if a consumer purchases products online, the goods will be delivered to his doorstep the next day, saving consumers time and energy. On the one hand, this approach has brought additional benefits; yet, without the consumers' awareness, their information is moved and exploited by various firms or inside the companies. Individuals' information is vulnerable. In today's world, information technology is growing faster than ever, and so are cybercrimes. We are completely lopsided since our rules are unable to keep up with the pace of technology, thus we want legislation that will combat cybercrime while also protecting consumers' privacy rights. [16]
Most governments in the globe now recognize that the problem of privacy invasion is global in scope rather than exclusive to any one country. It affects whether privacy violations will be deemed acceptable internationally. This is the truth that we must confront. Many countries, including India, have failed to keep up with technological advancements, resulting in severe gaps in protection. Our task is to incorporate technological innovation in such as to ensure that it advances and supports those ideals rather than damaging them.

REFERENCES

- Mr. Mahantesh B. Madiwalar, “Privacy Rights And Data Protection In Cyberspace With Special Reference To E-Commerce”, Bharati Law Review, April – June, 2017
- Chin Kyle, top cybersecurity regulations in India, 2024
- M. Mahindra Prabhu and P. Rajadurai, “The ways to empower the e-consumer in the alarming field of online shopping,”25years of Consumer Protection Act: Challenges and the way Forward, Editor Prof. (DR.) Ashok R. Patil, Chair on Consumer Law and Practice, National Law School of India University

[15] Dr. Nehaluddin Ahmad, “The issues of personal privacy and internet-A Critical analysis of Indian position and International scenario” Senior Lecturer, Faculty of Business and Law Multimedia University
[16] Radha Raghavan and Ramya Ramachandran, “Data Protection Law in India: An Overview,” Posted on January 29, 2022 .

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Tracy Mitrano, Civil Privacy and Legislative Security Policy http://net.educause.edu/ir/library/pdf/ERM0362.pdf
- Bob Whitehead, Invasion of privacy laws and video surveillance --what's legal, what's not? http://www.video-surveillanceguide.com/3048-invasion-of-privacy-laws.htm
- Privacy and emerging technology: Are Indian laws catching up? http://www.nwmindia.org/Law/Commentary/privacy.htm