Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 7, December-2021, ISSN 2230-7540

A Study on Legislative Responses and Judicial Perspective of Data Protection in India

Anita Yadav[1]*, Dr. Vipin Kumar[2]

[1] Research Scholar, School of Law, Shri Venkateshwara University

[2] Professor, School of Law, Shri Venkateshwara University

Abstract - An solid data security and privacy framework is necessary for a nation's advancement. As a consequence of corporations' inclination to collect increasingly sensitive and personal information, this has occurred. Nations like the United States and the United Kingdom have recognised India as a centre for outsourcing. These countries believe that citizens have the right to their own privacy and the right to have their personal information kept private and secure. In order to stay competitive, India must thus maintain a solid legal and regulatory framework for data security and privacy. This research examines the legal and legislative responses to data protection in India from a judicial and legislative perspective.

Keywords - Legislative responses, Judicial perspective, Data protection, India

----------X----------

INTRODUCTION

A basic human right recognised across the world, privacy is the most often violated right in cyberspace. It's normal for individuals to want their own private spaces.

From this vantage point, the Indian legal system must be viewed. Cybercrime and data theft are on the increase in India, thanks to the country's burgeoning technological and e-commerce sectors. An efficient, well-structured method is needed to deal with these malpractices since India is the host and the biggest platform for data outsourcing. The term "data protection laws" refers to legislation adopted to secure and protect personal data. [1]

Data privacy and protection laws in India have been analysed as a consequence of this chapter's efforts.

India's constitution guarantees that everyone has the right to express themselves in whatever way they want regarding any subject matter. Laws can only limit a person's right to life and liberty. People's right to practise and promote their faith is further guaranteed against arbitrary detentions. There are no exceptions to this rule until such a time when the law officially indicates otherwise. The individual's right to privacy and dignity are protected under Article 21. Privacy refers to one's ability to keep one's private information secret. [2]

Because we live in an information-driven world, the Supreme Court has found that the state is not the only one who poses a danger to our privacy [3]

OBJECTIVES

- To have a better understanding of the Indian judiciary's approach to key issues of data protection.
- To evaluate India's current data protection mechanisms in comparison to other countries.

RESEARCH METHODOLOGY

Research design

The Researcher used the doctrinal technique for this study, which involves doing research using facts and data from the library and archives. It includes case law analysis, the arrangement, ordering, and systematization of legal concepts, as well as the study of legal institutions. The stated idea is methodically examined, and numerous facets of it are considered.

Sample design

It was impossible and infeasible to reach out to a large number of individuals since the topic of data security has become so commonplace. For this study, the universe is made up of people and organizations involved in data security. There are a great number of people and things in this cosmos as well. As a result, the Investigator limited the size of its population to a sample that was typical of the aforementioned enormous cosmos. The following individuals comprised the sample used for this study:

(a) Lawyers (70);

(b) Representatives of companies engaged in data exchange and information technology (30);

(c) Police officers (20);

(d) Academicians (25); and

(e) Bankers (15).

It may be claimed that the sample chosen by the Researcher provides a wide range of viewpoints on the same topic because of its diversified character. As a result, the sample size is large enough to for valid conclusions and interpretations to be drawn from the data.

Data collection strategy

Doctrinal information may be gleaned from both primary and secondary sources. Consequently, primary sources such as legal and regulatory frameworks in India and other countries were used to collect data for the research along with an assessment of legislation and its application. For the purposes of this investigation, several documents and notifications issued by authorities addressing issues related to data protection and privacy were examined.

To complete current doctrinal study, secondary sources include books and research papers released by diverse writers in journals, media releases, and websites. Secondary sources, such as reports from the Indian government and criticisms of India's data protection and privacy rules, have been examined.

Descriptive Model

Research cannot be considered complete unless the data are correctly evaluated to discover relationships and connections between them. To put it another way, this strategy is used to understand the data.

Analytical Model

Models like this one are used to evaluate the current legal framework in India and other nations that govern data protection and privacy regulations, and their influence on the legal landscape.

LEGISLATIONS GOVERNING CYBER SECURITY AND DATA PROTECTION IN INDIA

Indians have been clamouring for an information technology-friendly legal framework for a long time now. A fascinating study of India's development in the information technology and data security fields would be interesting even if big adjustments were required to the country's existing legislation. [4]

a. The Constitution of India

Even though the Constitution of India is not a form of law, it acts as the foundation for every legislation made by the Indian parliament. As a result, the

remainder of the country's laws is based on the Constitution. [5]

Article 21 and Right to Privacy

India's Supreme Court has interpreted Articles 21100 and 101 of the Constitution as implicitly granting privacy in several cases, notwithstanding the lack of express privacy provisions in the Constitution. [6]

This right to privacy, or the right to be alone, was reviewed by the Supreme Court in R. Rajagopal v. State of T.N.102. In this instance, the privacy of a condemned prisoner was at risk. Precedents from Britain and the United States argued that the right to privacy could inferred from Article 21 of the Constitution, even if it wasn't clearly mentioned. By giving citizens the right to know, the public sector has been made more accountable and transparent. 2005's Right to Information Act paved the way for a more transparent government and less cronyism. [7]

RELATIONSHIPS BETWEEN THE GOVERNING BODY AND THE INTERNET

It is protected in India under the Information Technology (IT Act) and the Information Technology (Sensitive Personal Data or Information) Rules, 2011114, which govern the protection of personal data ("Privacy Rules"). In terms of data protection, these are India's most important legislation. [8]

Rules for the management of personal information pertaining to "sensitive personal data or information" (SPDI) are within the purview of Indian law. These include passwords, bank account and health information, as well as sexual orientation and biometric information. People in India may still access non-sensitive personal information about themselves without fear of repercussion. Because of the wording's ambiguity, under Indian law, consent is often interpreted as agreement because of this. Extraterritorial jurisdiction of Indian courts is unclear in light of current Indian law. Whether an Indian citizen's personal information is protected by the IT Act or Privacy Rules when shared with a US company while in the United States is not clear, according to this article. [9]

This provision protects the privacy of individuals and organisations to the fullest degree practicable. Policymakers have taken action on a variety of fronts in response to looming data privacy breaches. Procedural flaws and technical skill shortages in courts and law enforcement are some of the problems in India. Because of these obstacles, a legal framework must be constructed to address the underlying issues of technology. [10]

Definition of Sensitive Personal Data

Transgender and intersex individuals' biometric and genetic data, as well as caste and tribal information are now considered to be "sensitive personal data," in addition to passwords and financial information. Data that is deemed "sensitive" under international data protection laws like the GDPR is defined in a far more restrictive manner. [11]

Localization of Data

An Indian-based server or data centre must operate as a data fiduciary for a person or organisation that controls how and why personal information is gathered and processed. Data fiduciaries may see this requirement as arbitrary due to the financial repercussions it may have. International data transaction organisations may have a tough time complying with this rule when interacting with Indian citizens' personal information. [12, 13]

Critical Personal Data

Only Indian servers and data centres are permitted to handle sensitive personal information, according to the proposed law. There is no specified term for "sensitive personal data" in the Bill, and the Indian government is responsible for notifying the public of this fact. Many multinational corporations may find it challenging to store client data only on servers or

data centres in India. As a result, international data may be hindered.

Vicarious Liability in Case of Breach

Those who were in charge of a company's activities at the time of the crime will be held accountable under the bill's provisions. The harshness of this paragraph may be based on the fact that even the most comprehensive data protection standards do not hold CEOs personally liable. We all know that companies make data processing decisions based on what will bring them the most profit. Making the officials personally accountable for their actions is a bad idea. [14]

Since the statute is ambiguous, the directors and executives in control of the company may also be held responsible for the same penalty as the company. In addition, it's not obvious if a data breach holds a single data processor or a group of processors liable for the consequences of the breach. [15]

Repeal of Section 43A of IT Act, 2000

Under the proposed law, the Information Technology Act of 2000's Section 43A would be abolished. Certain aspects of the Bill, such as a privacy policy's exclusion, have been dropped from the legislation. There has to be more clarity on whether data fiduciaries need their own privacy policies or whether the Bill's need for a comprehensive notice is sufficient. [16]

Employment

The Bill exempts concerns with employment from the need to get consent from the data subject before processing their information. Because of the nature of the relationship between the employer and the employee, it is clear that the ground for exempting the employer from obtaining consent for data processing is provided. Because this data was obtained while they were working, firms may encounter issues if they wish to maintain the data of former employees after their employment ends. [17]

Review of Stored Personal Data

Regular evaluations of personal data are mandated by law for the data fiduciaries. Perpetual review and its frequency are not specified in this regulation, which is necessary to guarantee that data is only kept for as long as is necessary for processing. In order to avoid data fiduciaries using data in an undesired way, it would be helpful if the nature and frequency of the review were made apparent. [18]

Notice of Collection of Data

Under the rules of the Act, the data fiduciary must promptly notify the data principal of the proposed collection of personal data. Legislation dictates that the notice must be brief and simple to comprehend. The notice must also be made available in as many languages as necessary and possible. There must be clear and distinct notifications for each kind of data processing under the GDPR, therefore it's important to keep this in mind. [19]

Data Protection Authority

Data protection concerns will be handled by an independent Data Protection Jurisdiction with administrative and discretionary authority. As a result, it is imperative that the Authority's hands be empowered and that it is permitted to work as an independent body free from any influences, and that it develops its own data protection jurisprudence, addressing the nuances of this technological legal problem. [19]

EVOLUTION OF RIGHT TO PRIVACY IN INDIA

On October 16, 2012, former Delhi High Legal Chief Justice A.P. Shah presented the Indian government with an outline of the country's lengthy history of

court rulings on the right to privacy.A reference to Justice Shah's work on judicial interpretation and precedents is not only acceptable, but also essential. [20]

If a Supreme Court bench of seven justices could decide on the legality of laws that permitted police to conduct domiciliary visits and surveillance of persons with a criminal record, then so be it " He claimed that the rules violated his fundamental right to privacy, as guaranteed by Article 21's "personal liberty" provision. On the question of whether Article 21 should be construed as a protection of an individual's privacy, there was considerable dispute. The majority of people believe something to be true: [21] The Supreme Court considered Mr. X v. Hospital Z while deciding how much information about a blood donor might be kept private. An HIV-positive blood donor was unwittingly reported by the responding hospital in this case. His intended marriage was cancelled and his social position took an unexpected turn for the worst because of this. As a result of the Supreme Court's ruling, doctors and hospitals may make exceptions in cases when the non-disclosure of medical information is likely to jeopardise the lives of other persons, such as the intended wife of a blood donor. [23]

State eavesdropping on phone calls was at issue in the PUCLA vs. Union of India lawsuit, which was brought by the PUCLA. Rules of procedure were set down by the Court and must be followed in this instance. A part of the Telegraph Act of 1885 dealing with interception was not found illegal, but the Supreme Court refused to overturn it. [23]

Some sexual interactions between consenting adults may or may not be decriminalised by the Delhi High Court in Naz Foundation v. Union of India. That's why Section 377 was "read down" by the Court in Indian Penal Code, 1860, for this reason Under Article 21, only a strong justification may be shown for the State to intrude on a citizen's right to privacy in his or her sexual contacts, and the Court concurred. Since the government was unable to show an overriding interest, sexual relations between consenting adults are no longer banned. [23]

According to AFP. — A five-judge bench of the Supreme Court overturned the top court's decision in Navtej Singh Johar v. Union of India on September 6th, 2018. It is stated by the Court: In Sarda v. Dharmpal, the Supreme Court found that Article 21 reads in the right to personal liberty, but it cannot be deemed an absolute right. Even if a person's privacy is violated, medical testing may be required by the Court in order to arrive at a fair conclusion. As a result, the Supreme Court ruled that the right to privacy must be balanced with the freedoms of each person. "The public welfare and individual freedom must coexist in perfect harmony," says the philosopher David Hume. [22]

Supreme Court judgement Shreya Singhal v. Union of India had a major influence on the Indian IT law. Supreme Court judgement in this case is noteworthy for a variety of different reasons. India's people' freedom of speech has been expanded while the state's capacity to restrict it has been limited to the most severe instances. Justice Nariman made the following statement after handing down this landmark decision: [22]

Think and speak freely is more than just a lofty goal. Under our constitutional framework, it is also a fundamental principle of utmost importance. Section 19(2) had no arguments to the legality of Section 66A of the IT Act that could be considered lawful. If a legislation seeks to limit freedom of expression, it must be connected to one of the eight topics listed in Article 19(2) and satisfy two tests: an obvious and present danger, as well as the likelihood of inciting hate. [22]

The judiciary's interpretation of data privacy, i.e., Indian courts has interpreted the right to privacy in a unique way by focusing on privacy of information. [22]

DATA PROTECTION - A REFLECTION OF PRIVACY

An appeals court judgement on privacy's legality was issued by the Supreme Court of the United States on August 24th, 2017. Using an individual's Aadhaar number to authenticate his or her identity while seeking for a government subsidy, benefit, or service paid for by the Consolidated Fund of India is constitutional, according to the Supreme Court. The Supreme Court has decided on other pieces of law, circulars, and instructions necessitating the mandatory linking of Aadhaar. Temporary respite for petitioners seeking an extension of the deadline for Aadhaar-based banking and mobile services has been put on hold since January 2017 by the Supreme Court. [22]

On September 26, 2018, the Supreme Court of India affirmed the legality of Aadhaar and said that Aadhaar is designed to help the impoverished and respects the dignity of persons from a personal and communal perspective. The Supreme Court concluded that it is desirable to be unique since Aadhaar is designed to be distinctive rather than the best. Courtroom consensus reached that: [23]

Highlights of the Aadhaar Judgment

Therefore, the judgement thoroughly reviewed the privacy of person data and information, taking into consideration all of its facets. Data protection is intrinsically tied to one's right to privacy in one's own information, according to the Supreme Court. It was noted by the Supreme Court that India needed its own specific and robust data protection legislation, showing its forward-looking mentality. [24]

CONCLUSION

On the basis of the laws and planned laws regulating data protection in India, it is safe to say that the situation is not perfect, but it is also not hopeless.The legislative structure that governs the idea of data protection could undoubtedly need some adjustment. Because of its digital revolution and its status as one of the world's most populous data consumers, India will be able to keep up with ever-increasing digital transaction needs. Almost two decades after the passage of the Information Technology Act in 2000, India has fully embraced the digital age and is making steady progress toward enacting comprehensive laws on the issue. India's new and dynamic data-protection laws were brought into existence by the creation of the Srikrishna Committee, its recommendations, and the proposed Data Protection Bill.When it comes to interpreting numerous pieces of legislation, including the Indian Constitution, the Indian judiciary is well-known for its dynamism and activity.

REFERENCES

1. Yougal Joshi and Ananda Singh, “A Study of Cyber-crime and Security Scenario”, International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18.
2. Ravikumar S. Patel and Dr. DhavalKathiriya, “Evolution of Cybercrimes in India” International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.
3. Talwant Singh, “Cyber Law and IT” pp. 1-4
4. Rohitk Gupta, “An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective”, 2013.
5. Rohit k Gupta, “An Overview of Cyber law vs. Cybercrimes”, 2013.
6. PrabhatDalei and TannyaBrahme, “Cyber-crime and Cyber law in India: An Analysis” ‘International journal of humanities and Applied science’ Vol.2 (4), 2014.
7. Aashish Kumar Purohit, “Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, Vol. 2(5) sepoct, 2011.
8. M. M. Chaturvedi, M. P. Gupta and Jaijit Bhattacharya “Cyber Security Infrastructure in India : A Study”pp.1-15

9. IDSA Task Report, "India's cyber security challenged" March, 2012
10. Angshuman Jana and Kunal Kumar Mondal, "A survey of India Cyber-crime and Law and its prevention approach" 'International journal of Advance Computer Technology'.
11. David Satola and Henry L. July, "Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework", 'The MW. Mitchell law journal'
12. AnirudhRastogi, "Cyber Law- Law of Information Technology and Internet", 2 nd ed., Published by Lexis Nexis, 2014.
13. Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues", publish on Lawoctopus, 2014
14. Talat Fatima, "Cybercrimes", 1 st ed., published by Eastern Book Company 2011
15. Vakul Sharma, "Information Technology- Law & Practice", 5 th ed., Published by Universal Law Publishing, 2016
16. Talwant Singh, Delhi, "CYBER LAW & INFORMATION TECHNOLOGY", available on accessed on April 16,2016
17. Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues", publish on Law octopus, 2014
18. Robert Roohparvar, "Elements of cyber security", Info Guard Cyber Security, 2017.
19. Shital Prakash Kharat (2016) "Cyber-crime – A Threat to Persons, Property, Government and Societies" SSRN, 2016.
20. Anita L. Allen, Coercing Privacy, 40 Wm. & Mary L. Rev. 723, 750-57 (i999);
21. Julie E. Cohen (2000). Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, pp. 1423-28.
22. Abam, B.B. (1998). Self-Concept Development and Career Aspiration: Implication for Counseling. Unpublished M.Ed. Thesis, University of Jos.
23. Adenubi, M. (2007). Self-Concept and Locus Control: Two factors determining educational achievement. Education Today 1 (1) pp. 58-60.
24. Agbe, N.N. (2007). The influence of childhood experience in the development of self-concept: Implication for psychological counseling. The Jos Journal of Education.University of Jos, Nigeria 1 (1) pp. 57- 60.

Corresponding Author

Anita Yadav*

Research Scholar, School of Law, Shri Venkateshwara University