INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: ISSN Print

Data Protection Policy Regulations in India

Dr. A. Vijayalakshmi M.L., Assistant Professor, School of Excellence in Law, TNDALU, Chennai

Article information
Received: 8th April 2024
Received in revised form: 15th May 2024
Accepted: 18th June 2024
Available online: 21st August 2024

Volume: 1
Issue: 1
DOI: XXXX

Abstract

Indian Constitution under Article 21 ensures that "no one shall be denied his life or freedom of movement except under a process established using law." The goal of this basic right is to defend against infractions on individual freedom or taking one's life provided it is important to carry out a process imposed by law. The Supreme Court in India has interpreted and included the "protection of the right to privacy, properties & data" under "personal liberty," even though it is not specifically mentioned in the article. The Indian government has formulated many policy guidelines, laws, and regulations in the recent years for data protection and privacy. This paper aims to investigate the topics of data analysis and the right to privacy in the digital era. This study examines privacy concerns by examining circumstances in which user-provided data may be abused or, in certain cases, utilized against the individual who submitted it. The usefulness of the IT Act and other current privacy-related laws, and the extent to which they include data protection rules, are also examined in this research. The implementation of regulations in one of these sectors is going to be examined and contrasted since both private and public sectors collect data in an equal manner. Recently, experts led by former Supreme Court of India Judge B.N. Srikrishna were appointed by the Ministry of Information Technology and Electronics to write a law protecting data protection and privacy of Individuals.

Keywords: - Indian Constitution States, Supreme Court of India, Article 21, Right to Privacy, Property and Data', Public and Private Sector, Ministry of Electronics and Information Technology, Data Protection Laws, Personal Liberty.

"The Rajya Sabha made a landmark decision on August 9th, 2023, bypassing the Digital Personal Data Protection Bill"
—Indian Govt.

I. INTRODUCTION

India, home to approximately 1.2 billion people, is the world's most populous democracy. It has a multiparty bicameral legislative system. A thriving private sector has emerged in the once mainly state-dominated Indian economy throughout the last 20 years. It is currently the main economy growing at the quickest rate in the globe, with its economy ranking tenth in the world. It is also among the most well-liked destinations in the world for outsourcing of company processes, or the global outsourcing of the handling of personal information. Call center operations for telecommunications, medical transcription of conversational notes, and numerous more businesses are examples of this.

Awareness of a country's data protection scenario requires an awareness of its monitoring mechanisms. In some specific conditions are met, Indian governments can intercept electronic communications "in cases of any public emergencies or the most efficient interests for public safety. However, the 1996 Supreme Court's determinations
restricting who and when might tap phones curbed this
judicial power.

Because of recent "anti-terrorism" legislation "gave law enforcement agencies a great deal of power to bring down suspected terrorists, track interpersonal interaction, and decrease free expression," they are currently under protest, even though audit processes involve judicial examination and parliamentary control. Indian courts are aggressively working to reduce searches conducted without a warrant.

By Article 21 of our Constitution, an individual's life or individual freedom cannot be taken out unless it is according to the procedure established by the law. This basic right aims to preserve human liberty and prohibit the taking of life unless in compliance with legally defined processes. Our Hon'ble Supreme Court of India interprets and integrates " safeguarding or the right to freedom of speech and expression, property, and data" under the title "personal liberty," regardless of any disparities.

Since defining the notion judicially would be difficult due to its broadness and moralistic nature, the following acts achieve enforcement of the same:

- The Indian Penal Code, 1860: Article establishes the severe consequences of offences However, that excludes fines for violations affecting data.
- The Information Technological Act of 2000, or IT Act.
- The 1957 Indian Copyright Act.
- The 1872 Indian Contract Act.

1.1 India's legal scenario for data protection laws

1.1.1 International Commitments Regarding Privacy

The various treaties and conventions are not legally binding in India until they have been intentionally incorporated into our local legislation. India's only international privacy requirement is contained in Article 17 of the 1966 United Nations Conventions for the Preservation of Politics and Civil Rights (ICCPR). Article 21 has been considered to have been comprehended by international law. The following article deals with security and can be seen in the Indian Constitution. Since India is not included in the signatory list to the Optional Protocol to the Second Amendment of the Convention on Political and Civil Rights, its inhabitants are unable to protest (or make "interactions") with the U.N. (UN) about breaches of Article 17 implementation. India is not included in the membership of the OECD or APEC, and not even applied to join the Council of the European Union Convention on Private Data Privacy. Privacy and related Human Rights are not acknowledged and recognised in of the seven existing areas of engagement of the South Asian Agency for Regional Cooperation (SAARC), where India is the most active country dealing with such perspectives.

1.2 The rules for privacy protection under the Indian Constitution

According to our Constitution, *'Nobody can take away their liberty or personal freedom taken away from them unless a legally mandated procedure is followed.*

The Supreme Court of India has construed this Article to encompass protecting private information from the famous case of Mr.Kharak Singh v. A State of U.P in 2004, as stated in: *'Despite not being mentioned as a fundamental right in the United States Constitution, the aspect of right to privacy is still an essential part of private liberty.'*

Articles 19(1) (d) (the authority for free movements) and 19(1) (a) (the right to freedom of speech and opinion) have been construed to include privacy. The assurance provided in Article 14 of "a level playing field under rules or equal safeguarding provided by laws" is equally significant in Article 21. The Right to privacy must be evaluated against subsection (a) of article 19 of the US Constitution, which provides everybody the "right to freedom of speech and expression." To protect India's integrity and sovereign status, which denotes positive relationships with other included countries, public order, ethical behavior, and decency, and against defamation, contempt of our court, and incitement to offense, the State may, by Article 19(2) of the Constitution, impose appropriate restrictions on the usage of rights and privileges granted by the Article 19 (1) (a). The Supreme Court observed that the notion of free speech and expression, as expressed in Section 19 (1) (a), is the prime basis for the right of a citizen to knowledge.

1.3 The Right to Personal Information and Protections

'A person's "right to privacy" is what allows them to isolate themselves from other people and it provides for someone the option of whether to disclose or not the personal credentials to others. In essence, it refers to the freedom to express oneself to certain individuals. In actuality, it allows us to regulate the method and time of making use of the components we select to reveal and the parts that are accessible to others.

Without the individual's approval, the right forbids any person from making any public opinion and talks about them. If someone does this, they are infringing on the other person's rights and risk will be liable for damages in court. The 1948 U.N. Convention upon the Maintenance of the Rights of All Migrant Workers or Membership of Their Family Members, the 1948 International Compact on Political as well as Civil Rights, the 1948 General Declaration of Human Rights, and the 1948 UN Convention on the Protection of the Children are among the international agreements that recognize the dominant right to privacy as a fundamental freedom.

1.4 Misuse of Collected Information and Data Mining

The practice of gathering raw data and extracting usable information for later use is known as data mining. As a result, we may define it as the procedure that separates useful data from unusable data. Every action a person takes in this day of internet use has the potential to generate data. It is now feasible to gather, arrange, and use any person's data thanks to e-commerce. Data might be gathered from a variety of sources, including the following: -

(a) Marketing and retail companies that gather consumer data that can be used to identify potential stakeholders for specific marketing campaigns, forecast the success of upcoming campaigns, gauge customer reaction, implement profitable policies for the expansion of the company, and comprehend consumer behaviors or habit;
(b) Financial or banking companies gather data from their clientele, which provides financial institutions with knowledge regarding credit and loan reporting; it also assists them in identifying loans that are good or bad; it helps banks identify fraudulent credit or debit card transactions; it and it also aids in our comprehension of exchanges, purchases, banking, stocks, and other related activities;
(c) People who fill out forms for employment interviews in government departments too give information to government agencies and departments. This aids government agencies in establishing patterns and gathering data regarding money laundering as well as other facets of government employees' & officials' forgeries;
(d) Online games on PCs, tablets, and phones are yet another method by which data is gathered. Gaming websites obtain players' personal information and use it to understand their preferences. Even strangers can communicate with each other and study more about one another through internet gaming.
(e) The use of digital devices such as cameras, scanners, desktop video cameras, and video chat also contributes to the collection of user personal information;
(f) Social media platforms such as Twitter, WhatsApp, and Facebook are other sources of an individual's personal information collection. The information is posted on social media by the person.

Nonetheless, there is no denying that the data gathered has facilitated national development and improved our quality of life. With the assistance of all the relevant data that is kept on our devices & any documents that are virtually connected, the information is at our fingertips. However, it is also undeniable that data extractions from various applications—such as address, phone number, workplace, information about an account via KYC, and other details—as well as self-posts on social media and WhatsApp status updates, among other similar applications, have also proven to be problematic for data mining or pose risks to the individuals whose data they pertain to. There is essentially no way to manage the amount of data streaming, including collection, distribution of wealth, usage, and misuse. Although the gathered data can be put to good use, its arbitrary & uncontrolled usage produces critical questions about how to preserve people's security and privacy.

1.5 Indian Laws Concerning Data Protection

Due to the proliferation of the internet and the data generated by it, India is experiencing issues with a range of cybercrimes. issues with identity theft, credit card/debit card theft, money laundering, privacy invasion, fraud, etc. There is no legislation so far in India that addresses an individual's most important right to privacy or data protection. We cannot, however, claim that there exists no legislation protecting citizens from it. There aren't many laws that address data privacy issues to some degree while also mitigating private and national security concerns. The 21st article of the US Constitution guarantees the "right to privacy," and Article 19(1)(a) provides appropriate limitations on the right to freedom of speech and expression. It must be acknowledged, nevertheless, that India is not having currently any particular laws addressing data protection. We rely on the Information Technology (IT) Act of 2000 and the Indian Contract Act of 1872 for data protection in the absence of any specific rules.

1.6 India's Personal Data Protection Bill's

Although data privacy laws are in place in India, the complexity, dynamism, and global reach of technological advances necessitate a far more extensive regulatory framework to allay persistent worries. To create and develop data protection rules for India, The Ministry of Information Technology & Electronics asked the country's highest court Judge B.N. Srikrishna (Retd.) to chair a committee of ten members appointed by the government in August 2017. The Committee has issued a draft bill named "The Personal Information Protection Bill, 2018" following a year of discussions and public comments."

II. LITERATURE REVIVEW

(Martin, K. D., 2017) This essay summarizes the state of privacy research in marketing along with associated fields at the moment. Grouped by the function of privacy in a society as a whole the psychological aspects of privacy, & the economics of privacy, we analyze theoretical stances and empirical discoveries about information and data privacy.

(Bhandari, V., 2018) In this essay, we attempt to conceive, in light of the Puttaswamy ruling, the fundamental right to privacy and protection, its consequences for both public and private actors. We next look at the Justice Srikrishna Committee's draft Personal Information Protection Bill, 2018, and assess how well it has worked to control State actions about the private sector, with a particular emphasis on consent, surveillance, and interactions between the two, which includes the latter's capacity to refuse the former's requests for data.

(Bhandari, V., 2021) Since at least the beginning of the 1990s, cybersecurity have been a major policy priority for the Indian government. But as of right now, its cybersecurity regulations are still patchy and inconsistent. Specifically, as the following piece will show, intelligence and our law enforcement agencies tend to lose out when their concerns that technology users conflict with their goals.

(De, S. J., 2022) Global governments are addressing the COVID-19 pandemic by leveraging their digital ecosystems. Beneficiaries must proactively communicate the data management processes for their digital projects through adequate privacy policies to raise awareness among them about privacy dangers.

2.1 Objectives of the study

- Evaluate the degree to which India's current laws safeguard people's rights to privacy, including the potential to access, correct, and erase their personal information with consent.
- Assess the best practices and regulatory requirements in India for handling data breaches, including the duties of notification, the associated liabilities, and the results of non-compliance.

2.2 The Scope of the study

A policy on data protection study in India, or other countries for purposes of discussion, usually covers a range of topics about the management, processing, storing, and safeguarding of personal data. These are the most essential elements that the scope might include:

- Legal Framework: examining the current legal and regulatory structure in India that governs data protection, in considering any applicable regulations or pertinent laws like the Personal Data Protection Act (PDPB).
- Industry-Specific Regulations: determining which industry-specific laws or rules, like those governing banking, healthcare, or telecommunications, may be relevant.
- Data Types: Analysing the categories of data covered by the policy, such as sensitive personal credentials, and personal data, including any other categories as specified by applicable laws or rules.
- Data Processing Activities: Recognizing the several data processing works that are performed within the company, such as gathering, storing, use, sharing, & disposal.
- Data Subject Rights: Recognizing and upholding all rights of data subjects as specified by data protection legislation, including the ability to access, correct, and erase their personal information.

III. METHODOLOGY

- Understanding Legal Framework: Start by carefully reviewing India's data protection legislation, including any modifications to current statutes or the Personal Data Protection Act (PDPB).
- Risk Assessment: Make a thorough evaluation of all the available data that your company gathers, handles, and retains. Determine any possible threats to confidentiality and information security.
- Implementation Plan: Make an implementation plan with phases that outline the organization-wide rollout of the policy. Assign roles and establish deadlines for execution.
- Monitoring and Compliance: Provide procedures for continuing to monitor processes of the different data to make sure the policy is being followed. Conduct routine evaluations and audits to pinpoint areas that require enhancement.

IV CONCLUSION

India's regulations are entirely different from those of developed countries in that they define data according to its significance and utility. It is necessary to innovate rules about data extraction & deletion. To fulfill any international standards, India does not currently offer sufficient protection for personal data about all or the majority of the most common privacy principles, within any area. Adopting laws alone won't be adequate until there is strong enforcement in place to safeguard people's rights; as a result, special courts must be established to handle issues about data protection as well as intellectual property rights in attachment to the Personal Information Protection Authority, as indicated in the Bill of 2019. Data protection is definitely connected and linked to the the right to privacy. It is guaranteed by Article 21's concept of the right to life and personal dignity, even though it is a substantial individual right with reasonable restrictions.

REFERENCES

Shri Kartikey Vyas v Employees Provident Funds Organisation Decision No. 174/ICPB/2006 [2006] INCIComm 1029 (4 December 2006).
Sharma, Vakul. Information Technology-Law & Practice (2nd Edition): Universal Law Publishing Co. Pvt. Ltd, New Delhi, 2007
C Connolly and A Vierboom, 'Do Not Call Registers backed by high-profile enforcement action', Privacy Laws & Business International Newsletter, Issue 101, at 10 (October 2009).
VK Puri, Right to Information Practical Handbook (JBA Publications 2010) at 2.3.
P. Duggal, Cyberlaw—The Indian Perspective (2nd ed Saakshar Law Publishers 2004), at 12. 61 Personal communication from Director, DSCI, January 2010.
Tewari and Nayak (23 December 2008). The industry had been asking for several amendments for some years as well by then, however. See Napinnai (2010).
Justice K.S. Puttaswamy (Retd.) and Anr. Vs Union of India and Ors., writ petition (civil) no. 494 of 2012
Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45, 135-155.
Bhandari, V., & Sane, R. (2018). Protecting citizens from the state post-Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018. Socio-Legal Rev., 14, 143.
Kovacs, A. (2021). Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork. Cyber BRICS: Cybersecurity Regulations in the BRICS Countries, 133-181.
De, S. J., & Shukla, R. (2022). An analysis of privacy policies of public COVID-19 apps: Evidence from India. Journal of Public Affairs, 22, e2801.