

Detailed Study and Analysis on Indian Data Protection Laws

Tushar Tiwari¹, Dheeraj kumar²

^{1,2} School of Legal Studies and Governance, Career Point University, Kota

Abstract-

In the current digital era, data protection is one of the most important and pertinent issues. With a population of more than 1.4 billion, India is one of the fastest growing economies in the world. The nation is more dependent on data processing, storage, and transmission as the digital economy grows. Through the introduction of numerous legislation and policies to protect its residents' personal data, India has acknowledged the significance of data protection laws. The right to privacy is recognized as a fundamental right by the Indian Constitution, and the Indian Parliament has implemented numerous legislations to safeguard people's right to privacy. This study seeks to give a summary of Indian data protection regulations and examine their development.

Keywords: Data Protection, Data Privacy, Constitution of India, Indian Penal Code, 1860, Information Technology Act, 2000

I. INTRODUCTION

Given that database maintenance is comparatively less complex than upholding their authenticity, identifying the optimal data safeguarding strategy is presently a matter of paramount significance. The evolution of technology has brought about a shift in the landscape of criminal activities. A substantial portion of contemporary crimes is executed by adept professionals employing computers and allied electronic devices, which constitute the most convenient avenue. These offenders can swiftly breach protective barriers to access sensitive material. The surge in incidents of cybercrime is propelled by the thirst for acquiring information.

In recent times, the matter of data security has emerged as a significant global apprehension. The widespread adoption of digital technology has simplified the accumulation, retention, manipulation, and distribution of copious volumes of personal data by both individuals and entities. This has engendered apprehensions concerning the confidentiality and integrity

of personal data, prompting numerous nations to formulate regulations pertaining to data protection. India is no anomaly and has recently enacted a fresh legislation pertaining to data security, namely the Digital Personal Data Protection Bill, 2022 (DPDP Bill). This research paper will furnish a comprehensive outline of the data protection statutes applicable in India.

Notwithstanding the manifold conveniences that the modern world has bestowed upon us, it has also inadvertently led to several instances of procurement improprieties resulting in unintended data breaches. To delve into this phenomenon, consider the following illustrations:

After each instance of accessing the email account at cybercafés, an electronic trace of the password was inadvertently exposed.

Post every credit card transaction, a trail disclosing the brand, retailer, and related particulars is invariably left behind.

Whenever an individual connects to the internet, a digital imprint is left in its wake, enabling website proprietors and advertising agencies to track individuals, thereby unveiling their interests.

Employees face potential vulnerabilities as employers routinely utilize software to gain access to employees' email communications and whereabouts.

Among the most recurrent offenses committed by malefactors is the pilferage of proprietary source codes.

Another prevalent method employed by malevolent entities to acquire users' personal information is through dispatching unsolicited emails.

Via hacking activities, unauthorized agents can substantially manipulate a user's account, effecting alterations at their discretion.

II. LITERATURE REVIEW

Although the Act was legislated prior to India's attainment of independence, it presently serves as a robust guardian of creators' intellectual property rights due to its integration into our legal framework. Throughout an author's lifetime and for a span of 60 years following their demise, the Act offers substantial protection to their literary, theatrical, musical, and artistic works. In cases where an individual reproduces, duplicates, or employs the author's work without explicit permission for personal gain or any other intention, such as publication, distribution, or

transmission, the Act furnishes remedies on both civil and criminal fronts.

Research Objectives

1. To comprehend the idea of data protection and the effects that data protection laws have on society.
2. To examine various Indian data protection laws.
3. To know how the government regulates data protection.

III. METHODOLOGY

The research is doctrinal in nature. Secondary sources, including books and articles from different websites. The issues were divided into components and elements in the study report, and the issues' structure was classified using analytical and descriptive techniques. "The research methodology employed in this work is based on secondary data, which implies it is based on some previously collected information, also known as primary data. In secondary research, the main data is joined and integrated with other data in order to produce what is known as secondary data. Since secondary research is convenient and time-saving, many individuals today opt to go with it.

IV. INDIAN LAWS REGULATING PRIVACY AND DATA PROTECTION

It should be noted that although the terms "privacy" and "data protection" are not defined in any statute, law, order, or notification, their extent and breadth are sufficiently broad to include privacy and data protection under our Indian Constitution and other statutes. The following laws govern the same:

Constitution of India: The preamble constitutes a crucial element of the Constitution of India, granting specific Fundamental Rights to Indian citizens within PART III. This constitution stands as the world's most extensive, encompassing approximately 395 Articles, 12 Schedules, and 22 Parts. The Preamble of India ensures that all its citizens possess the freedom of thought, expression, belief, faith, and worship. This includes safeguarding an individual's right to privacy, allowing for governance and justice in cases of its violation.

Both Article 21, which centres on the Protection of Life and Personal Liberty, asserting that "No individual shall be deprived of their life or personal liberty except according to the established

legal procedure," and Article 21, collectively assure all citizens the liberties of thought, expression, belief, faith, and worship. The Hon'ble Supreme Court of India, in 2017, hinged on the term "Liberty" within the Preamble and Article 21. This decision led to the declaration that the right to privacy is indeed a fundamental right, especially pertinent when threats or unauthorized access compromise an individual's data without their explicit consent. Consequently, individuals hold the prerogative to directly approach the Hon'ble Supreme Court of India through Article 32 or the respective High Court of the State via Article 226.

Copyright Act, 1857: Although the Act was legislated prior to India's attainment of independence, it presently serves as a robust guardian of creators' intellectual property rights due to its integration into our legal framework. Throughout an author's lifetime and for a span of 60 years following their demise, the Act offers substantial protection to their literary, theatrical, musical, and artistic works. In cases where an individual reproduces, duplicates, or employs the author's work without explicit permission for personal gain or any other intention, such as publication, distribution, or transmission, the Act furnishes remedies on both civil and criminal fronts.

In the civil context, the aggrieved party retains the right to seek damages and injunctions, asserting that the infringing party must compensate for their actions. Conversely, under criminal circumstances, a conviction can result in a prison term of up to three years and a monetary fine of up to Rs. 2 lakhs.

Indian Contract Act, 1872: Nevertheless, the Act offers limited and indirect oversight over the realm of privacy and data protection. Its stipulations establish the lawful structure for contracts – mutual agreements involving parties to carry out actions in exchange for monetary or other advantages. Depending on the scope of the task covered comprehensively by this legislation, the contractual parties have the option to incorporate clauses that either encompass or exclude matters concerning privacy and data protection. This serves to safeguard and uphold India's rights regarding privacy and data protection, albeit to a moderate degree.

Information and Technology Act, 2000: The following provisions of the Act, which especially addresses cybercrimes, frauds, and the webs of e-commerce, are important for reducing the crimes committed in cyberspace and are closely tied to data protection and privacy:

Section 66: Hacking, colloquially known as unauthorized intrusion into computer resources or data without the owner's consent, resulting in harm to the individual's reputation or a corporate

entity's goodwill as stipulated by Section 43A, is subject to penalties. Violators can be sentenced to imprisonment for up to three years, fined up to five lakh rupees, or both.

Section 66C: Presently, fraudulent use of another person's password is considered unlawful due to the private nature of the information stored on the individual's computer resource. Unauthorized access by a third party without consent can lead to a maximum imprisonment of three years or a fine of up to Rs. 1 lakh.

Section 66E: Intentionally capturing, transmitting, or disseminating an image of an individual without their consent is a breach of privacy. This action could result in imprisonment for up to three years, a fine of up to Rs. 2 lakhs, or both.

Section 67: Distributing or transmitting explicit pornographic content through electronic means that is offensive, induces criminal activity, or neglects legal responsibilities is an offense. Conviction for this offense on the first instance can lead to imprisonment for up to three years, while subsequent convictions might result in imprisonment for up to five years and a fine of up to ten lakh rupees.

Digital Personal Data Protection Bill, 2022:

A new version of the Personal Data Protection Bill, now known as the Digital Personal Data Protection Bill, 2022, has been published by the Union Government. The main principles of this bill are highlighted below:

- Organizations are obligated to utilize personal data in a manner that adheres to legal regulations, treats individuals equitably, and remains transparent to those individuals.
- Personal data should exclusively serve the purposes for which it was initially gathered.
- The principle of data minimization holds significant importance.
- The emphasis lies on the necessity of precise data acquisition.
- A principle stipulating that personal information cannot be retained indefinitely by default and must be stored for a specific duration only.
- In order to prevent any unauthorized collection or processing of personal data, appropriate measures must be established.

- The individual responsible for determining the extent and method of personal data processing should be held responsible.

While keeping these principles in mind let's now look at key features of DPDP bill 2022:

Data Principal and Data Fiduciary:

The term "Data Principal" pertains to the individual from whom data is collected. Minors (individuals below 18 years old) will be identified as having "Data Principals," represented by their parents or legal guardians.

The entity responsible for determining the "objective and methods of processing personal data of an individual" is referred to as a "data fiduciary."

Prominent Data Fiduciary establishments are required to designate a 'Data Protection Officer' as well as an impartial Data Auditor.

Rights to Individuals:

The provision states that individuals must have the ability to access "fundamental information" in the languages specified in the eighth schedule of the Indian Constitution.

Prior to the processing of their data, individuals are required to give their explicit consent. It is mandated that each person is informed about the specific categories of personal data that a Data Fiduciary intends to gather, along with the reasons for such collection and subsequent processing. The law also ensures that individuals retain the prerogative to revoke consent from a Data Fiduciary.

Data subjects are empowered with the authority to request the deletion and rectification of data amassed by the data fiduciary.

In the case of the demise or incapacity of data subjects, they are also bestowed with the right to appoint a representative who will assume responsibility for exercising these privileges.

Data Protection Board:

The legislation suggests the establishment of a data protection board with the aim of overseeing compliance.

In cases where consumers are dissatisfied with the response from the Data Fiduciary, they have the option to file a complaint with the Data Protection Board.

Cross-border Data Transfer:

The proposed legislation allows for the cross-border storage and exchange of data with specific "notified countries and territories." This is contingent on these nations maintaining a satisfactory data security framework and granting the Indian government access to the data of its citizens in those jurisdictions.

Financial Penalties:

For Data Fiduciary: The legislation suggests substantial sanctions on enterprises that experience data breaches or neglect to inform users about such breaches. These penalties encompass a range starting from Rs. 50 crores to Rs. 500 crores.

For Data Principal: Individuals might face fines of up to Rs. 10,000 for submitting baseless complaints or presenting deceitful documentation during the process of registering for an online service.

V. CONCLUSION AND SUGGESTION

In this research paper, I have explored the profound importance of privacy for both individuals and society, contributing to a harmonious coexistence. A parallel can be drawn with the realm of data protection. Historical records indicate that in ancient civilizations, those possessing superior knowledge held dominion over regions, whether they were cities, nations, or professions. Reflecting on our ancestral heritage, it becomes evident that our predecessors emphasized the value of knowledge as a conduit to achievement and personal greatness.

In contemporary times, this paradigm has shifted to revolve around "Data," a resource of unparalleled significance, surpassing the value of personal jewelry, assets, or currency which can be replaced if lost. Data, however, wields a direct influence on one's existence and quality of life when mishandled. The potential repercussions are immeasurable and beyond comprehension. The suggestion would be:

- While India possesses a multitude of laws and constitutional provisions concerning the realm of privacy and data protection, a notable absence of a dedicated legislative body aimed at safeguarding this right serves to diminish its efficacy and certainty.
- Efforts should be made to establish dedicated expedited judicial processes within the country. These courts would be focused on handling instances of privacy violation, child abuse, and child sexual abuse, particularly when the perpetrator utilizes social media for their actions. The priority should be to ensure swift case resolution, accompanied by stringent penalties for the offender. This approach aims to promptly address the grievances of the victims and uphold the principles of justice.

VI. REFERENCES:

- [1] Constitution of India
- [2] Indian Penal Code, 1860
- [3] Indian Contract Act, 1872
- [4] Information and Technology Act, 2000
- [5] Digital Personal Data Protection Bill, 2022
- [6] Data Protection Laws in India: A Comparative Study by Dr. Ajay Kumar Garg
- [7] VidhiAagaz| Journal of Law Management and Humanities