IP BULLETIN

Vol. IV Issue 2, JULY-DEC., 2023, Pg. 12-20

EVOLUTION OF DATA PROTECTION

Akshita Gupta[1] *and Amaan Siddiqui*[2]

ABSTRACT

Privacy, arguably the most crucial factor for humanity's survival on Earth, appears to be under threat in contemporary times under the guises of "Procedure Established by Law" or "Public Duty," particularly when it comes to actions by public officials. If we pause for a moment to contemplate what life would be like for an individual without any privacy rights, encompassing personal aspects like family, workplace, and relationships, it becomes evident that privacy is as essential to human existence as oxygen. It serves as the conduit through which one can lead a peaceful life with dignity and liberty, embodying the essence of Article 21 of the Indian Constitution. In our nation's ongoing journey towards digitalization, often referred to as the "Cyber Era," the rise in the usage of social media and the internet across various domains has underscored the critical importance of Data Security and Data Protection. These aspects are integral to safeguarding one's privacy, as they constitute a digital footprint that holds not only national significance but also carries a national responsibility. Data Protection and Privacy are intricately intertwined, forming an exceptionally sensitive domain within the legal landscape of our times. This research paper adopts an analogous research method, primarily due to the widespread impact of the COVID-19 pandemic and the resulting restrictions, which led to the utilization of secondary sources for information gathering and subsequent synthesis into a concise body of knowledge.

Keywords: Article 21 of the Indian Constitution, Data Privacy, Data Protection, Fundamental Rights, Security.

INTRODUCTION

Data protection refers to the collection of private information regulations, laws, and practices that prevent privacy invasions brought on by the gathering, storing, and sharing of private

[1] Students at DME, Noida affiliated with GGSIPU
[2] Students at DME, Noida affiliated with GGSIPU

information. Any data or information that may be utilized to identify a specific individual, regardless of whether it was gathered by a government agency, a business organization, or another entity, is known as private data has become one of the most valuable and pervasive assets in our society. From personal information such as names and addresses to sensitive financial records and health data, the digital landscape is awash with a vast ocean of information. While this data holds immense potential for improving our lives, it also raises significant privacy concerns. Data privacy, often used interchangeably with the term "information privacy," is a fundamental concept that revolves around an individual's right to control their personal information and determine how it is collected, processed, stored, and shared.

In an era where data is collected on a massive scale by governments, corporations, and various online platforms, the need to safeguard individuals' privacy has never been more critical. Data breaches, identity theft, and the misuse of personal information have all underscored the importance of data privacy in our interconnected world. This introduction aims to delve into the multifaceted realm of data privacy, exploring its significance, underlying principles, and the evolving landscape of data protection laws and regulations. It will also discuss the various challenges and ethical considerations surrounding data privacy in an age where technology continuously reshapes our understanding of what is possible in the realm of data collection and utilization. Ultimately, data privacy is not merely a legal concept but a cornerstone of individual autonomy and freedom in the digital era. Understanding its nuances and implications is crucial for both individuals and organizations navigating this complex terrain. There are very famous and landmark judgments in the Indian judiciary such as the Puttuswamy case[3] and the Auto Shankar case. Under which the apex court has regarded the right to privacy as the fundamental right enshrined under the constitution. A study claims that the future legal system will unquestionably be built solely on Artificial Intelligence (AI), which will provide greater difficulties and barriers to the right to privacy and data protection in India and around the globe. We can observe how technologies can violate your data and lead to mistakes in your daily life. India marked the beginning of a new era in safeguarding information. From the time being, the only statutes that have been used to interpret anything information-related are the Information Technology Act of 2000 (the "IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 (the "SPDI Regulations"). These regulations had several restrictions, though, and the introduction of the Digital Personal Data Protection Act in 2023 offers much-needed respite in the digital age where worries over private information are on the rise.

[3] https://indiankanoon.org/doc/127517806/

PREVIOUS LEGISLATION ON DATA PRIVACY

Information Technology Act, 2000

The Information Technology Act of 2000 was enacted on the seventeenth of October 2000. The primary Indian law addressing e-commerce and cybercrime issues is this one. The legislation was passed to combat online crime, support online transactions, and advance electronic governance. The law's main objective is to diminish and completely eradicate digital crimes while facilitating legitimate, trustworthy digital, computerized, and online activities. To give legal weight to all electronic transactions, including data exchange, different kinds of digital interaction, and e-commerce, to replace the traditional printed method of communication to certify electronic signatures as reliable evidence of any information or documents that need to be verified legally. to make it possible for paperwork to be submitted electronically to governmental agencies and organizations. to facilitate the storage of digital information within India. Approving and simplifying electronic money transfers for banks and other financial institutions. Without an arrest warrant, senior police officers and other officials can access any public area to conduct detention over acts prohibited by the Act. The rules outlined in this legislation do not apply to the powers of attorney, negotiable instruments, wills, or similar documents.

In the case, **Shreya Singhal v. Union of India (2015**),[4] two women, Shreya Singhal and her friend, were arrested for posting comments on a social media platform (Facebook) criticizing the appropriateness of a bandh (strike) in Mumbai following the death of a political leader. The arrests were made under Section 66A of the Information Technology Act, 2000, which allowed the police to arrest individuals who posted offensive content online with the intent to cause annoyance, inconvenience, danger, or insult.

However, the Supreme Court of India, in its judgment on March 24, 2015, declared Section 66A of the IT Act unconstitutional. The court held that the provision was vaguely worded and allowed for arbitrary and excessive censorship of online content, violating the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution. The court ruled that the provision was not narrowly tailored and did not meet the reasonable restrictions allowed under Article 19(2) of the Constitution. The judgment in the Shreya Singhal case was a significant milestone for internet freedom and freedom of speech in India, as it set a precedent for protecting online expression from arbitrary and draconian legal measures.

[4] https://en.wikipedia.org/wiki/Shreya_Singhal_v._Union_of_India

AMENDMENTS IN THE IT ACT, 2008

According to Section 66A, this legal provision in the Information Technology Act, of 2008, makes it illegal to send content through digital means that is inflammatory, harmful, deceptive, or inappropriate. The aim is to prevent the dissemination of content that could cause discomfort, fear, or harm to others. Sections 67 and 67A provide a place to combat the spread of explicit or obscene sexual material on the internet. They serve as essential controls to regulate and prohibit such content online. As per Section 69A, the Indian government has the authority to restrict access to content that poses a threat to national security, public order, or foreign relations, or incites criminal activities related to these concerns. The enforcement of this section is governed by rules known as the "Blocking Rules" or "Information Technology Rules (Blocking of Access of Information by Public Rules), 2009."

Section 77A,[5] this section allows for the consolidation of multiple offences into a single charge, except in cases involving severe penalties, economic crimes, or crimes against women or minors. Section 79 of the IT Act[6] emphasizes the central government to create rules for intermediaries, and entities that host or transmit content created by third parties. It addresses the legal responsibilities of intermediaries, offering exemptions if they are unaware of illegal content and requiring them to remove such content once they become aware of it. Not only this, section 79 of the IT Act, 2008, 79 gives power to the central government to make rules u/s 87(1) and 87(2)(zg). Section 79 of the act provides information, data or communication made or hosted by any third person. Section 79(2) and 79(3) of the act are exemptions to section 79 which states that where an intermediary engages in the technological or any automated or sexual activities will be covered under section 79. This exception would only be considered if the intermediary was not aware of the data being sent or stored in an electronic form. In addition to this section 79(3)(b) mandates the participant to remove illegal information as soon as he has the actual knowledge of such information.

With the rapid growth of technology and the internet, India, like many other countries, has witnessed an increase in cybercrimes. These include activities such as child pornography, the online distribution of explicit content, and video voyeurism. Consequently, amendments to the Information Technology Act in 2008 were necessary to incorporate provisions that specifically address these types of crimes, which were previously not covered by the legislation.

[5] https://www.itlaw.in/section-77a-compounding-of-offences/

[6]https://www.indiacode.nic.in/show- data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=105

DEVELOPMENT OF DATA PROTECTION IN INDIA

The honourable Supreme Court of India has established the right to privacy and data protection as a fundamental right in the landmark case of **Justice K.S. Puttaswamy V. union of India 2017**,[7] outlining the information technology rules, 2011 governing the collection, receiving, processing, storing, dealing, retaining, handling, using, transferring disclosing sensitive personal data and information, security practices for handling personal information. However, this provision made in 2011 was also insufficient as it failed to address other issues involving misuse of data by children, and breach of data by companies outside India.

PERSONAL DATA PROTECTION BILL, 2018

The preamble of the bill Personal Data Protection Bill 2018[8] says that the right to privacy is a fundamental right and is necessary to protect personal data as an essential facet of informational privacy, to protect the growth of the digital economy the use of data is critical and the communication between two persons has to be kept private as well therefore to create a collective culture the fair digital economy has to be built to protect the privacy of individuals and empowering them as well.

The Personal Data Protection Bill was made to create a framework of lamenting organizational and technical measures to lay down norms for cross-border transfer of data with security ensure accountability of entities and provide remedies for unauthorized and harmful processes by the Parliament in the 69th year of the republic in India. This will also lead to some of the modifications as follows:

i. The law mandates that data fiduciaries keep "at least one serving copy" of customer information on an Indian server or data center.
ii. This bill allowed the processing of personal data for the detection, investigation and any other real legal infraction which led to adequate laws prohibiting state monitoring and access to all personal data leading to a serious threat to the right to privacy under Part-III of Article 21 of the Constitution of India.
iii. Ashley the bill made was not regulatory and independent enough.

PERSONAL DATA PROTECTION BILL, 2019

The joint Parliamentary Committee on the Personal Data Protection Bill 2019 gave its report on the 11th of December 2019 and recommended that non-personal data be regulated under the

[7] https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors
[8] https://www.meity.gov.in/writereaddata/files/model_rfp_for_selection_of_implementation_agencies-2018.pdf

personal data bill as well and legal framework should be followed instead of being separate legislation for non-personal data. To provide security to the citizens they stated that data protection legislation is to personal data not only determine privacy but also governing data protection is necessary to ensure all data is under one data protection authority.

The winter session committee held on 11th of December 2019 led to the creation of the title of the bill that changed to Data Protection Bill, 2021[9] [24]including the definition of non-personal data and non-personal data breach in clause three as "data other than personal data". Even after so many attempts made to protect personal data and other data of the citizens, this bill was also withdrawn as the cross-border transfers accountability of processing data and other data for unauthorized and our processes lead to the floor and usage of personal information of the individuals for whom personal data was processed.

DIGITAL PERSONAL DATA PROTECTION BILL, 2022

The Digital Personal Data Protection Bill[10] 2022 got its recognition in 2023 on August 11. The temporary objective of the new add is to establish a comprehensive framework for the protection and processing of personal data; The act provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect the personal data and the need to process such data for lawful purposes and matters connected there with or incidental thereto. The following act is the first ever central law in India to use her or she pronounces while referring to individuals this act also provides various digital India acts and industrial-specific laws around privacy and data protection towards the adoption of artificial intelligence and other future technologies while protecting personal data the act also aids Indian businesses to enhance their collaboration with other businesses across the globe while safeguarding personal data.

According to Section 2 of the act, the Definition and salient features of the digital personal data protection Act, of 2023 are as follows:

According to Section 2(g), *Consent Manager means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.*

According to Section 2 (h), *data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.*

According to Section 2 (i) *Data Fiduciary means any person who alone or in conjunction with*

[9] Personal_Data_Protection_Bill,2018.pdf

[10] https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019/

other persons determines the purpose and means of processing personal data.

According to Section 2 (j), *Data Principal means the individual to whom the personal data relates and where such individual is—*

i. a child, includes the parents or lawful guardian of such a child;

ii. a person with a disability, including her lawful guardian, acting on her behalf;

According to Section 2 (k), *Data Processor means any person who processes personal data on behalf of a Data Fiduciary.*

According to Section 2 (l), *Data Protection Officer means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10*.

According to Section 2 (m), *digital office means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode.*

According to Section 2 (n), *digital personal data means personal data in digital form; (o) "gain" means— a gain in property or supply of services, whether temporary or permanent; or*

i. an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration.

According to Section 2 (p)*, loss means—*

i. a loss in property or interruption in the supply of services, whether temporary or permanent; or

ii. a loss of opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration.

COMPARISON BETWEEN DIGITAL PERSONAL DATA PROTECTION ACT, 2023[11] TO THE PREVIOUS DATA PROTECTION ACT IN INDIA.

I. Territorial implementation of the Bill:[12] The new bill extends to Indian soil as well as outside the territory of India whereas the previous laws were limited to India and had no provisions for any offence committed outside the territory of India. The new bill also gathers personal information by the data controllers used to provide products and services across the globe

II. Consent: In 2019 PDP made a significant part and mentioned the definition of the word "consent" whereas the 2018 change in the word "consent" was also explicitly taken.

[11] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[12] https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-

III. Fine: The new Bill DPDP, 2022 increases it fine to rupees 500 crores whereas the previous poll provision had the maximum fine amount to ₹250 crores only to make sure the offenders comply with strict rules with the law.

IV. The regulation of non-personal data: The regulation of non-personal data was laid every year to which was permitted by the central government to ask for data few dictionaries to give records of non-personal data as before the Digital Personal Data Protection Bill, Personal Data Protection 2018 did not mention non-personal data at all.

WHY INDIA NEEDS A NEW CODIFIED DATA PROTECTION LAW?

1. Modernizing data protection laws: India has made significant strides in technology, but it lags in having comprehensive and stringent data protection laws that reflect the current landscape. Over the past two decades, countries like the USA and China have acted with robust data protection regulations. Therefore India needs to update legislation to keep pace with the global standard and hence the new act had to come into existence.
2. Enhancing the Information Technology Act, 2000: while the Information Technology Act of 2000 was a significant step forward it no longer fully addresses the complexity of today's digital world. There is a pressing need for rigorous enforcement and potential provisions to ensure the act effectively safeguards data and privacy.
3. Tackling the issue of spam: the proliferation of spam has become a prevalent concern. In contrast to the USA and various European nations, India lacks the specific laws to penalize spammers. It is crucial to introduce legislation that addresses this problem and protects individuals from repetitive and unsolicited messages.
4. Dedicated legislation for online transactions: while the Reserve Bank of India has issued guidelines for online transactions, having dedicated legislation in the domain would provide greater clarity and protection for both consumers and businesses participating in the digital economy.
5. Addressing emerging technology challenges: India needs to proactively address emerging technologies such as cryptocurrency, NFTs, and evolving cyber threats like cyber defamation and cyber terrorism. Legislation should establish a clear legal framework to regulate and manage these technologies and mitigate associated risks.

CONCLUSION

India's Personal Data Protection Bill, introduced to address the complexities of data privacy in a digital age, has elicited both commendations and criticisms within the legal community. On the positive side, the bill is hailed as a proactive measure that can significantly enhance data protection, aligning India with global data security standards. It establishes a comprehensive legal framework for data protection and privacy, providing individuals with essential safeguards in the digital realm. However, concerns persist regarding the extent of government powers, especially in the appointment of the Data Protection Board members, which some argue may compromise Independence. The bill's broad exceptions and the government's power to grant exemptions to data processors, without sufficient procedural safeguards, have raised apprehensions. Moreover, the exclusion of personal data publicly submitted poses risks for data protection on the internet. Striking a balance between data privacy and effective governance is vital to ensure the bill's success and India's positioning as a leader in responsible data protection.

****