IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Protection In The Digital Era:

A Comparative Study of India's Legislative Framework with EU and US, Data Protection

Raynold Nongdhar
LL.M 4th Semester
Department of Law
North Eastern Hill University, Shillong, India

Abstract: The world is witnessing rapid technological growth, with the internet becoming a ubiquitous presence that transcends geographical boundaries, facilitating the flow of information. Data has become an integral part of our daily lives, connecting almost every aspect of modern life to some form of data. Whether it's social media, banking, or retail, our daily routines are intricately linked to data. This increased interconnectedness brings forth new and complex challenges in terms of privacy and data protection, making it crucial to ensure individuals have control over their personal data. India, as one of the fastest-growing economies, is at the forefront of this digital transformation, with various sectors being digitized and the launch of the Digital India program. In response to the growing concern over the protection of personal data and individual privacy rights, the Indian government has introduced several pieces of legislation. The bill's preamble aims to provide a legislative framework for protecting personal data and individual rights in India's rapidly evolving digital landscape. This research aims to analyze the efficiency of the law and the challenges associated with data protection in India. It will also compare the Indian data protection legislative framework with those of the European Union and the USA to identify areas for improvement. The comparison will focus on data protection principles, enforcement mechanisms, individual rights, accountability measures for data processors, cross-border data transfer provisions, and remedies available to individuals in the event of a data protection breach. The research will provide insights into the grey areas where the Indian legislative framework may face complex issues and propose improvements. In the digital age, it is imperative for countries to take significant steps to address the challenges arising from data protection and privacy concerns.

Keywords: Data, Privacy, Technology, Personal, Digital

I. INTRODUCTION

India is going through a digital transformation where people are using technology and the internet more and more in their daily lives. As a result, the necessity for cyber security and data protection measures to protect people and businesses from cyber-attacks and data breaches has increased. India is the second-largest internet market in the world, with an estimated population of 1.3 billion, and is anticipated to expand quickly. The desire for more stringent data protection rules and regulations has arisen as a result of concerns about data privacy and protection prompted by this expansion. There is no denying that the world we live in has changed and is changing quickly. In recent years, globalization and international trade have boosted the service sector, and modern industrialized societies have depended on the storage of data and information. Data is no longer only a power or source of information but has grown into a huge business from healthcare, services to education Both the public and private sectors routinely collect data using low-

tech methods for data storage. The issue of people's privacy has always been raised by the internet's never-ending nature.

The right to privacy that we formerly took for granted has been completely destroyed by the new digital environment. The development of the Internet has made it simple for the average person to conduct all of their routine online activities in a secure manner, but questions about privacy and data protection remain unanswered, which has led to security breaches. Data and information have caused individuals and organizations to pause before disclosing their information to third parties. Government bodies are quickly passing new laws emphasizing regulation on how businesses gather, store, and process client related-data in light of the concerns surrounding digital privacy issues across various sectors globally. All players in this space will greatly benefit from investing more resources into robust cybersecurity programs capable enough not only to defend against known attacks but also to detect/prevent emerging ones. Its become important to strike the right balance between privacy and innovation in the development and implementation of data protection laws and regulations.

In India, the issue of data breaches is constantly brought up. The largest data breach, according to the WEF World Economic Forum's Global Risk Report 2019, occurred in India. called the "Aadhaar leak case" In order to meet the rising demand for digital services and to secure data protection, the country's cybersecurity workforce will require an extra 1 million qualified personnel by 2025, according to a report by the Internet and Mobile Association of India (IAMAI) (IAMAI, 2020). The rise in cyberattacks and data breaches nationwide also emphasizes the importance of data protection. Over 4 lakh cyber events were reported in India in 2019, a 37% increase from the previous year (CERT-In, 2019). The world's greatest data breach, known as the Aadhaar leak case, happened in India that same year and exposed the personal information of over 1.1 billion Indian people as a result of a security hole in the country's biometric identity system, the Aadhaar system (Jan, 2018).

Data protection laws in India are now governed by the Digital Personal Data Protection Act 2023 and out-of-date Information Technology (IT) Act 2000, which is insufficient to deal with the complexity of the modern digital environment. Although the Act was updated in 2008 to add provisions for data protection and cybersecurity, academics and industry players have criticized these provisions as being insufficient (IT Act, 2000). The Digital Personal Data Protection Act 2023 is a data protection law that the Indian government has been developing in order to give Indian residents complete data protection.

The Digital Personal Data Protection Act 2023, which aims to control how businesses and governmental organizations acquire, store, process, and use individuals' personal data. Personal data is defined by the Act as any information that can be used to identify a Individual. Additionally, it lays out a number of data protection guidelines, such as purpose restriction, data minimization, and accountability. The creation of a Data Protection Authority (DPA), an independent regulatory organisation tasked with upholding Bill's provisions, is one of its fundamental components. (Digital Personal Data Protection Act, 2023) The DPA will have the authority to investigate and punish businesses and government organizations. The Indian government has also been making efforts to strengthen data security organization in the nation, the government has also started a number of initiatives and programs to support data security and privacy in India. The Digital India

programe was introduced in 2017 by the Ministry of Electronics and Information Technology (MeitY), with the goal of transforming India into a knowledge-based society and economy. The program covers a number of data privacy and security-related measures, such as the creation of safe digital infrastructure, raising public awareness of cyber-security, and encouraging cyber-security research and development. In addition, the government of India has set up a number of bodies to oversee data protection. The Data Security Council of India (DSCI), a self-regulatory organization with the mission of creating and promoting best practices in data privacy and security, is the most renowned organization. The DSCI collaborates closely with the government and other stakeholders to develop data protection policies and legislation, and it offers advice and certification to businesses on data protection.

1.2 Statement of the problems:

Data protection laws are continuously evolving worldwide, with countries like the Europe and the USA amending their legislation to address the challenges posed by evolving technologies. However, India lags behind in enacting comprehensive data protection legislation to safeguard personal data and individual rights in the digital era. Although India has made several attempts to establish separate data protection laws, these initiatives have either failed to be converted into law or have fallen short of adequately protecting individual privacy. The recently Indian legislative framework, the Digital Personal Data Protection Act (2023), introduces various changes compared to previous bills. Nevertheless, the Act has certain issues that could limit the protection of data to a particular form and complicate enforcement.

1.3 Review of Literature:

The primary literature review is the current legal legislative framework of Data protection in India, the European Union, and the United state of America

a) The Digital Personal Data Protection Act, 2023:

Union Ministry for Electronics and Technology (MeitY). The Digital Personal Data Protection Bill, 2022,. This Bill provides a roadmap of the Digital Data Protection Act 2023 by highlighting its key features and issues, as well as comparing it to the previous data protection bill. It is relevant for researchers who seek to understand the nature of the previous bill and its potential implications for data protection in the context of the 2023 Act.

b) General Data Protection Regulation, 2016/679:

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

c) United State of America Regulation on Data Protection.

California Consumer Privacy Act CCPA 2020

d) Privacy and Data Protection in India: An Analysis

The article discussed how privacy is being threatened by public servants in the name of "Procedure Established by Law" or "Public Duty". Privacy is important for a peaceful life with dignity and liberty and is essential for human rights. With the increase in digitalization and use of social media and the internet, data protection and privacy become a national issue and obligation. Data protection and privacy are interlinked and crucial in the legal world.[1]

e) Privacy and Data Protection in India: A Critical Assessment:

The paper discussed the conflict between the right to privacy and data protection in India and argues that the current Information Technology (Amendment) Act, 2008 is not sufficient in protecting data. The author suggested the need for separate legislation to protect data and privacy, and aims to initiate a debate on this topic**.** Which Is used for the reseach to analyse the IT provision and amendment act 2008.[2]

f) A Comparative Study of Data Protection Laws: Current Global Trends, Challenges and Need of Reforms in India:

The article discusses the current global trends, challenges, and the need for reforms in data protection laws in India. It highlights the importance of data security and protection in the increasing digitization of society. The article also raises questions about the ownership, access, and duration of data stored in the virtual world. It further emphasizes the need for an appropriate law to address the worries over digital security, information assurance, and data protection in India. The article also compares the General Data Protection Regulation (GDPR) in the EU and the Personal Data Protection Bill in India.

g) Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information:

The article discussed the protection of data and privacy in India. It highlights that the right to privacy is rooted in the doctrine of an individual's right to privacy, which is enshrined in the constitutions of many developed nations. The concerns for privacy and data protection gained prominence during the 1970s with the rise of computerized systems capable of storing and disseminating large amounts of information. While the Indian Constitution does not explicitly guarantee a right to privacy, the courts have interpreted other constitutional rights, such as the right to life and liberty, as encompassing a limited right to privacy. India, as a party to various international instruments, acknowledges privacy protections outlined in the Universal Declaration on Human Rights and the International Convention on Civil and Political Rights.[3]

h) A Soft Tone with a Tiger Claw a Critical Commentary on the Digital Personal Data Protection Act, 2023:

The commentary on the Digital Personal Data Protection Act, 2023, provides valuable insights into the evolution of the Act from the lengthy Personal Data Protection Bill 2019,2022 to the more concise DPDP Act 2023. The commentary examines various important aspects of the bill, including the rights and duties of

---

[1] ***Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021***

[2] ***Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011***

[3] ***Shanaz, Asifullah Samim and Mohammad Edris Abdurahim Zai, Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information, Trinity Law Review, Volume-3, Issue-2, 2023***

digital citizens, the rights to privacy of children, and the redressal mechanism for data fiduciaries. Moreover, the commentary thoughtfully analyses ambiguous clauses related to deemed consent, which has been a topic of debate. For the purpose of this research, the commentary will be utilized to thoroughly grab the understanding of the complex concept and to discuss the mentioned concept with comparison.[4]

i) Twelve Major Concerns with India's Data Protection Bill, 2022. Media:

This article discusses the 12 major concerns with the digital data protection bill 2022, which are relevant to researchers who seek to analyze these concerns in a broad manner and assess their relevance to the provisions of the bill.[5]

j) India's Digital Personal Data Protection Act, 2023: How Practical is Consent[6]:

The article provides a brief discussion of the concept of consent in relation to the Digital Personal Data Protection Bill, highlighting the key issues related to consent in the bill and emphasizing the relevance of understanding the concept of consent in different countries legislation for research purposes.

k) Shailesh Gandhi, ten instances show how the Digital Data Protection Act will undermine the RTI Act. Scroll. In (2023).[7]:

This article discussed the two important provisions of the Act and effecting the Right to information act, section 8(1) j to exempt the disclosure of personal information. For the purpose of this research, the article will be utilized to provide more comprehensive information on the Digital personal data protection bill,2022, and Section 8 (1) (j)[8] of the Right to information act 2005.

l) S. Mehrotra, The Digital Personal Data Protection Act, SSC online (2022).[9]

This article provides a comparison between the relevant provisions of the Digital Personal Data Protection Act and the European Union's General Data Protection Regulation. The research will further provide an analysis and comparison of the important provisions of the bill in a broader manner. This is important for understanding the similarities and differences between the two pieces of legislation and their potential impact on data protection.

1.4 Scope and Limitation

Scope:

1- This research focuses on privacy and the data protection laws in India and their effectiveness to secure the rights of privacy of individuals.

---

[4] ***https://www.researchgate.net/publication/368423648_A_Soft_Tone_with_a_Tiger_Claw_A_Critical_Commentary_on_the_Digital_Personal_Data_Protection_Bill_2022#fullTextFileContent***

[5] ***https://www.medianama.com/2022/11/223-twelve-major-issues-data-protection-bill-2022/***

[6] ***https://jolt.richmond.edu/2023/01/19/indias-digital-personal-data-protection-bill-2022-how-practical-is-consent/***

[7] *https://scroll.in/article/1042602/these-instances-show-how-the-digital-data-protection-bill-will-undermine-the-rti-act*

[8] (j) information that relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause an unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:

[9] *S Mehrotra , The Digital Personal Data Protection Bill, 2022, SCC online 2022 https://www.scconline.com/blog/post/2023/01/21/the-digital-personal-data-protection-bill-2022/*

2- The research compared the Indian data protection various legislative frameworks and the proposed law with the EU and US to identify the strengths and effects of statutes in data protection principles, enforcement mechanisms, rights for data subjects, accountability measures for data processors, cross-border data transfer provisions, and remedies for individuals in case of a data protection breach to a better understanding.

Limitation:

- This research is limited to the provisions and a critical analysis right to privacy and data protection law in India.
- The research is subject to the availability of relevant data and information, and any limitations in accessing such data and information could impact the findings of the research which will be based on secondary sources.
- The study is limited to only legal provisions related to data protection laws and may not consider other factors that could impact data privacy, such as social norms, cultural values, or economic policies.
- The study is limited to the scope of the comparative analysis with the EU, and US.

1.5 Research Objectives

The followings are the objectives of the Research-

- Firstly to understand the data protection and legislative framework around privacy in India,
- Secondly to understand the right to privacy, data regulation, and its relevancy in the digital era, and
- Thirdly the objective is to provide insight into the successful enforcement of data protection law by the EU and the US and to provide suggestions to India for the better Implementation of the data protection law.

1.6 Hypothesis

- Despite the efforts of comprehensive data protection legislation in the form of various Data Protection Bills India still lacks adequate set laws and regulations for data protection.
- Indian laws are not comprehensive and sufficient in terms of protection and enforcement as compared to the EU and USA

1.7 Research Question

- Whether India has any enforcement regulation in case of an invasion of the right to privacy?
- Whether the present Indian legislative framework effective in addressing the legal issue of data breaches by international entities?
- Whether data protection laws in India as effective as those in the EU and US?
- Whether there are any protection major differences in the data protection of India vis the EU, and US legislative framework?

1.8 Research Methodology:

"For the purpose of this research, the author utilized the Doctrinal Research framework method. This framework involves a critical analysis of legal documents and literature, including statutes, case law, and scholarly articles. the author draws on both primary and secondary sources. Primary sources include relevant Indian, European Union, United States, and Canadian regulations, such as the Information Technology Act, of 2000, the Digita Personal Data Protection Act, of 2023, the General data protection Regulation of 2016, etc as well as case law and judicial decisions. Secondary sources include scholarly articles, books, and reports from relevant organizations and experts in the field of data protection. A Comparative Study method is also employed for analysis of the different topics in the research and to make a comparison between India, European Union and United States, laws. This method involves a comparison of the laws and regulations of India with the European Union, and United States, in terms of data protection, privacy, and enforcement. This allows for a comprehensive analysis of the strengths and weaknesses of India's legal framework and the potential implications of the data protection law, in comparison to other jurisdiction.

CHAPTER II

ORIGIN AND DEVELOPMENT OF DATA PRIVACY AND PROTECTION

II. ORIGIN AND DEVELOPMENT OF PRIVACY AND DATA PROTECTION

- **Background of Privacy**
- **Privacy in India**
- **Data protection**
- **Need for Data Protection**

2.1 Background of Privacy

Throughout history, the notion of privacy has been a fundamental aspect of human life[10]. The preservation of a certain level of privacy has been a consistent feature of human societies, and its significance has been reflected in various religious texts and legal systems, the biblical story of Adam and Eve illustrates the importance of privacy in human life, as they covered their bodies with leaves to maintain their privacy after eating the forbidden fruit This demonstrates that even in the earliest times[11], humans had a basic understanding of the need for privacy. Similarly, in ancient Greece and Rome, the concept of privacy was equally crucial, and laws were in place to protect it. For instance, in Athens, it was illegal to read other people's mail or break into someone's house[12]. Similarly, in Rome, the law ensured that a person's home was their sanctuary, and no one could enter it without permission[13]. Furthermore, the Romans constructed private chambers within their homes, known as "cubicula," for various purposes such as sleeping, bathing, or relaxation[14]. These ancient practices demonstrate that privacy was a significant concern for people even in the

[10] *Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006, 154 (3), 477-560*

[11] *Konvitz, M. R.: Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272*

[12] *Lefkowitz, M. R. Women's Life in Greece and Rome: A Source Book in Translation; JHU Press: Baltimore, 20*

[13] *J. P Balsdon,. V. D. Roman Private Life and Its Survivals. In Roman Civilization: Selected Readings; Kagan, D.; Viggiano, G., Eds.; Columbia University Press: New York, 1960; pp 231-248.03*

[14] *Maffei, G. L. Roman Art; Harry N. Abrams: New York, 2002*

earliest civilizations. Although the concept of privacy has evolved over time, its importance has remained constant throughout history[15].

In the 19th and 20th centuries, technology began to play a significant role in shaping the concept of privacy. the Kodak camera emerged as a revolutionary invention by George Eastman in 1888 that transformed the world of photography and raised questions on privacy. This technology was affordable, portable, and user-friendly[16], empowering the masses to capture life's precious moments on the go. However, this breakthrough also ushered in a new era where privacy became a scarce commodity. With cameras becoming ubiquitous, people could be snapped in their most intimate moments without their knowledge or consent, raising concerns about the misuse of their images.

The Kodak camera's impact on privacy was profound, leading to legal challenges that tested the limits of privacy law. In the landmark case of ***Pavesich v. New England Life Insurance Co*[17]*.,*** the plaintiff argued that the unauthorized use of his photograph in an advertisement had violated his right to privacy and caused him emotional distress. This case set the stage for the development of privacy law, establishing the legal concept of the right to privacy.

Academically the privacy theorist made a valuable contribution to established privacy, in the second half of the 20th century The Legendary article of 1890 written by Samuel D. Warren and Louis D. Brandeis [18]was published in the Harvard law review and is recognized as the birth of legal recognition of privacy in its own right. The foundational law review essay "The Right to Privacy," written by Samuel D. Warren and Louis D. Brandeis, was published in the Harvard Law Review in 1890. Warren and Brandeis argued in this piece that individuals have a basic right to privacy that is protected by law. According to them "The right to privacy does not preclude the publication of information of public or general interest." The protection granted by privacy law is limited to the individual's private life. It does not include the debate of public affairs or subjects of general interest in which the public has a legitimate interest." Warren and Brandeis both claimed that developments in technology and the expansion of the press had made it easier for the public to intrude on people's private lives. They demanded that legal safeguards be placed in place to preserve people's privacy rights.

Their article influenced the development of privacy law in the United States and has been cited in numerous court cases and legal opinions. It is regarded as one of the most important books on the subject of privacy.

Later, **Warren**, a member of the Boston commercial elite, was outraged when he discovered that intimate details of his family were publicly shared without his consent.[19] The authors argued for the protection of "the sacred precincts of private and domestic life" and the right to be left alone, rejecting any form of personal infiltration without clear consent and a legal basis. They recognized that privacy, especially the right

---

[15] *H Nissenbaum,. A Contextual Approach to Privacy Online. Daedalus 2011, 140 (4), 32-48*

[16]*Naomi Rosenblum, A History of Women Photographers, Abbeville Press, 2010).*

[17] *Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905).*

[18] *Samuel D. Warren & Louis D Brandeis., The Right to Privacy, 4 Harv. L. Rev. 193 (1890*).

[19]*, Samuel D. Warren, and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193-220. https://harvardlawreview.org/wp-content/uploads/2012/12/1939-1940_4_1930-1939.pdf#page=136.*

to be let alone, was not a universal right, but necessary in a modern era of mass media, and therefore required legal protection. The article's influence on privacy law is further discussed in the chapter on privacy and law.

In 1960 Dean William Prosser Surveyed Over 300 privacy cases that occurred subsequent to the publication of the Warren and Brandeis article were examined. As a result, Prosser formulated the principles of privacy law in his article 24, which were also incorporated into the Second Restatement of Torts on pages 652A-652I (1977). Prosser has identified four categories of privacy rights that qualify for a tortious remedy.

- **The First category** pertains to instances of unreasonable intrusion upon the seclusion or solitude of another, including physical intrusion in a person's home, such as undesirable entry, peeping into the house through windows with binoculars or cameras, telephone tapping, obtrusive telephone calls, scanning and collating financial and personal data without the person's consent and information.
- **The Second category** involves the appropriation of a person's name or likeness for the advantage of others, such as unlawful use of a person's name or likeness for advertising and soliciting clients/consumers on a product label that injures the personal feelings of the person.
- **The Third category** addresses public disclosure of embarrassing private facts like financial position, sexual orientation, personal correspondences, family feuds, medical history, and personal photographs taken at their home.
- **Finally, the Fourth category** concerns publicity placing one in a false light in the public eye by putting information in the public domain to create a false impression about the person.[20]

However, the supreme court ruling of the United States has also played an important role to establish the right to privacy. In 1965, the Supreme Court issued a ground-breaking ruling in the case of ***Griswold v. Connecticut,***[21] which invalidated a Connecticut law that prohibited the use of contraceptives. In the decision, the Court recognized a "right to marital privacy" that was not explicitly stated in the Constitution but was nevertheless protected by the Bill of Rights and the Fourteenth Amendment's Due Process Clause. This decision was a significant step in the development of privacy law in the US. The Court further expanded privacy protections in the 1973 case of ***Roe v. Wade***[22], which established a woman's right to choose to have an abortion without undue interference from the government. The Court found that a woman's decision to have an abortion was protected by the "right to privacy" recognized in Griswold and other cases, including ***Eisenstadt v. Baird***[23], which extended the right to use contraceptives to unmarried couples.

In 1986, the Supreme Court issued another landmark ruling in the case of ***Bowers v. Hardwick***[24], which upheld a Georgia law criminalizing sodomy between consenting adults in private. However, in 2003, the Court reversed its position in the case of ***Lawrence v. Texas,*** [25]which struck down the Texas law that criminalized same-sex sodomy. The Court found that the right to engage in private, consensual sexual activity was protected by the Due Process Clause of the Fourteenth Amendment. These cases illustrated the ever-

[20] ***Prosser, William L. "Privacy." California Law Review 48, no. 3 (1960): 383-423. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2973&context=californialawreview.***
[21] ***381 U.S. 479 (1965).***
[22] ***U.S. 113 (1973).***
[23] ***405 U.S. 438***
[24] ***478 U.S. 1986***
[25] ***539 U.S. 558 (2003).***

evolving nature of privacy law where the Court has expanded privacy protections to include the right to marital privacy, the right to make personal medical decisions, and the right to engage in consensual sexual activity in private.

2.2 Right to Privacy in India:

The Constitution of India stands as the paramount law of the land, serving as the supreme authority. It is an irrefutable fact that our Constitution is a dynamic and adaptive document, capable of shaping itself in accordance with the changing social and environmental landscape. Among the plethora of fundamental rights, it enshrines, the right to privacy holds a significant position, falling under the protective umbrella of Article 21. Article 21 explicitly states that "no person shall be deprived of their life or personal liberty." It is universally acknowledged that the right to privacy is intricately linked with an individual's life and liberty, making it an inherent part of the fundamental rights guaranteed by Article 21.[26] The discourse on the existence of a fundamental right to privacy in the Indian context can be traced back to a series of judgments by the Supreme Court of India, starting from ***M.P. Sharma vs Satish Chandra*** [27]***to K.S. Puttaswamy v. Union of India***. [28]

In the series of Landmark cases on the right to Privacy in India ***M.P. Sharma vs Satish Chandra***,[29] is remarked as the first case in which the right to privacy has been discussed the issue of whether privacy is a fundamental right was first raised before the esteemed Supreme Court of India. The case involved a search and seizure carried out by the authorities in pursuit of disputed documents of the Dalmia Group of Delhi, based on a First Information Report (FIR) and warrants issued under the statutory provisions of the Code of Criminal Procedure, 1973. The Group challenged the validity of the search and seizure through a writ petition, contending that it was arbitrary and violated their Right to Privacy and Fundamental Rights as guaranteed under Article 19(1)(f)[30] and Article 20(3) [31]of the Constitution, pertaining to protection against self-incrimination. The matter was referred to an Eight-Judge Constitutional Bench of the Supreme Court, which thoroughly examined and deliberated on the issue. In the end, the Supreme Court ruled that the Constitution does not regard searches and seizures carried out in accordance with established legal procedure, such as a FIR and subsequent decisions of the District Magistrate, as a violation of personal privacy or fundamental rights. The Indian Constitution does not recognize the right to privacy as a fundamental right in India, according to the court, because the language of the Indian Constitution does not conform to the Fourth Amendment of the US Constitution. The court found that the current case's search and seizure weren't illegal or unconstitutional.

---

[26] ***Nivedita Baraily, An Analysis of Data Protection and Privacy Law in India***

[27] ***(1954) S.C.R. 1077***

[28] ***Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others, (2017) 1 SCC 10***

[29] ***(1954) 1 SCC 385***

[30] ***Article 19, of the Constitution of India***
"Right to freedom"

[31] ***Article 20.***
(1) No person shall be convicted of any offence except for violation of a law in force at the time of the commission of the act charged as an offence, nor be subjected to a penalty greater than that which might have been inflicted under the law in force at the time of the commission of the offence. (2) No person shall be prosecuted and punished for the same offence more than once. (3) No person accused of any offence shall be compelled to be a witness against himself.

In ***Kharak Singh v. State of U.P***[32]**,** The petition before the Supreme Court challenges the constitutionality of Chapter 22 (Regulations 236 and 237) of the Uttar Pradesh Police Regulations and the powers conferred on police officials by its various provisions, claiming that they violate citizens' rights guaranteed by Articles 19(1)(d) and 21 of the Constitution. The Court referred the ***J Frankfurter's remark in Wolf v. Colorado***[33]**.** "The protection of one's privacy against arbitrary police intrusion... is fundamental to a free society." As a result, it is implicit in "the concept of ordered liberty" and, as such, enforceable against the states under the Due Process Clause. The knock on the door, whether day or night, as a prelude to a search, without legal authority but solely on the authority of the police, did not require the commentary of recent history to be condemned as inconsistent with the conception of human rights enshrined in the history and basic constitutional documents of English-speaking peoples... We have no trouble in stating that if a state knowingly sanctioned such police intrusion into privacy, it would violate the Fourteenth Amendment guarantee." The Court took notice. "It is clear that the knock at the door, or the man being roused from his sleep, does not impede or prejudice his locomotion in any way," and so does not violate Article 19 (1)(d).37 Clause (b) of Regulation 236, in our opinion, is clearly in violation of Article 21, and because there is no "Law" to justify it, it must be declared unconstitutional."38 However, the majority of the Judges who participated in the ruling stated that the right to privacy is not a constitutionally guaranteed right.

In his opinion, ***Justice Subba Rao favored*** inferring the right to privacy from the phrase "personal liberty" in Art. 21. "Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also a right to be free from encroachments on his private life," writes **Subba Rao, J.** Although our constitution does not directly declare the right to privacy as a Fundamental Right, it is a fundamental component of personal liberty. Every democratic country values family life.

In the series of landmark cases ***R. Rajagopal v. State of Tamil Nadu***[34], also known as the "Auto Shanker Case," the Supreme Court of India has unequivocally established that the right to privacy, or the right to be left alone, is protected under Article 21 of the Constitution. This fundamental right extends to safeguarding an individual's privacy in various aspects, such as their personal life, family, education, marriage, procreation, and motherhood. Furthermore, in the case of State of ***Maharashtra v. Madhulkar Narain***[35]**,** it has been conclusively held that the right to privacy is applicable to all individuals, including those who may be considered of "easy virtue," and that no one can infringe upon their privacy.

In the case of ***People's Union for Civil Liberties v. Union of India***[36], The practice of administering the tapping of telephone, which is intricately tied to the Right to Privacy and Data Protection, is commonly referred to as the "Telephone Tapping Case" in legal circles. A Public Interest Litigation (PIL) was initiated by a voluntary organization in response to reported incidents of Telephone Tapping of Politicians by the Central Bureau of Investigation (CBI), purportedly in the interest of public security and safety. The Petitioners alleged that

[32] *(1964) 1 SCR 332*
[33] *338 U.S. 25 (1949)*
[34] *(1994) 6 SCC 632*
[35] *(1991) AIR 207*
[36] *(1997) AIR 568*

telephone tapping constitutes a grave violation of the Right to Privacy, as well as a brazen infringement of Article 21, which guarantees the Right to Life and Personal Liberty.

The constitutionality of Section 5 of the Indian Telegraph Act[37], of 1885, which confers the power to record phone calls upon the Central and State Governments subject to certain conditions, was challenged in the PIL. The Hon'ble Supreme Court of India pronounced that phone tapping indeed amounts to a serious encroachment upon Article 21 and the Right to Privacy, and should only be invoked in exceptional circumstances of public safety, such as situations involving grave danger to the general public or public emergency. The Court further emphasized that, except in these limited circumstances, the Central Government is not authorized to resort to phone tapping, even if it believes that the Sovereignty or Integrity of India is under threat. The Court also issued guidelines to be followed in the exercise of Section 5(2) of the Indian Telegraph Act, of 1885. These guidelines include the appointment of a review committee and periodic review of the Order of Phone Tapping every two months, among others, to ensure that the power of phone tapping is exercised judiciously and in compliance with the constitutional principles of the Right to Privacy and personal liberty. the Supreme Court has ruled that telephone tapping constitutes a serious intrusion upon an individual's right to privacy, which is an integral part of the right to life and personal liberty as enshrined in Article 21 [38]of the Constitution. The Court further stated that such surveillance should only be conducted by the State in cases of public interest, emergency, or safety. It is important to note that while the Indian Telegraph Act of 1885 and the Information Technology Act of 2000 grant the government authority to conduct surveillance based on certain criteria, such as protecting the sovereignty and integrity of India, state security, friendly relations with foreign states, public order, or prevention of incitement of offenses, these grounds are subject to reasonable restrictions on free speech as outlined in the Constitution of India.

The Apex Court held that the right to privacy was not a guaranteed right under **Part III of the Constitution of India**, based on the understanding of Part III as per the law laid down in **A.K. Gopalan v. State of Madras**[39]. However, ***A.K. Gopalan***[40] was overruled in **Rustom Cavasjee Cooper v. Union of India[41]** and subsequently clarified in **Maneka Gandhi v. Union of India[42].** Since then, smaller Benches of the Apex Court have consistently held that the observations in **M.P. Sharma** and the majority judgment in **Kharak Singh** on the right to privacy were not good law.

Gobind v. State of M.P. [43] recognized the right to privacy as implicit in the concept of individual autonomy and liberty, but not an absolute right and subject to restrictions based on compelling public interest. The Court noted that the contours of the right to privacy would have to develop through a case-by-case process. The Court also acknowledged that the right to privacy contained multiple aspects, such as spatial privacy, informational privacy, decisional autonomy, and full development of personality.

---

[37] ***Power for Government to take possession of licensed telegraphs and to order interception of messages***

[38] ***Article 21, the Constitution of India***

"No person shall be deprived of his life or personal liberty except according to procedures established by law."

[39] ***(1950) S.C.R. 88.***

[40] ***Ibid***

[41] ***(1970) 1 SCC 248***

[42] ***(1978) 1 SCC 248***

[43] ***(1975) 2 SCC 148***

Subsequently, many judgments of the Apex Court have relied on Gobind case and recognized the right to privacy as a fundamental right under the Indian Constitution.

Finally, in the case of ***K.S. Puttaswamy v. Union of India***[44], (AADHAAR CASE) a nine-judge constitutional bench of the Supreme Court of India in 2017 invoked the concept of "Liberty" as enshrined in the Preamble and Article 21 of the Constitution to establish that the Right to Privacy is a fundamental right. This right encompasses the protection of data, including unauthorized access or use of an individual's data without their explicit consent, which constitutes a grave violation of the Right to Privacy. Individuals have the option to approach the Supreme Court of India directly under Article 32 [45]or the High Court of their respective state under Article 226 [46]to seek redressal for such infringements. overruled the *M.P Sharma and Kharak Singh case* and declared the Right to privacy as the fundamental right under Article 21 of the Constitution of India.

2.3 DATA PROTECTION AND RIGHT TO PRIVACY:

Data protection and the Right to privacy have become crucial issues in today's digital world. With the increasing use of technology, forms of data have diversified, making it more challenging to ensure adequate protection for personal information. It also underscores the need for robust data protection measures that can effectively safeguard sensitive information against misuse, theft, or unauthorized access by malicious actors online. From our personal information, financial records, and even medical history, a vast amount of sensitive data is being generated and processed every single day. However, with this abundance of data comes the need for effective protection measures to ensure privacy and prevent unauthorized access or misuse. In recent years, there has been an increasing concern regarding the security of sensitive data due to high-profile breaches that have exposed millions of people's personal information. This has led to a growing awareness of the importance of protecting sensitive data from cyber threats such as hacking, identity theft, and phishing attacks. Data protection and data privacy is also been misunderstood in the term of privacy. However, Data protection and data privacy are totally different in nature.

---

[44] ***(2017) 10 SCC 1***

[45] ***Article 32. Of the Constitution of India***

(1) The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed. (2) The Supreme Court shall have the power to issue directions or orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto, and certiorari, whichever may be appropriate, for the enforcement of any of the rights conferred by this Part. (3) Without prejudice to the powers conferred on the Supreme Court by clauses (1) and (2), Parliament may by law empower any other court to exercise within the local limits of its jurisdiction all or any of the powers exercisable by the Supreme Court under clause (2). (4) The right guaranteed by this article shall not be suspended except as otherwise provided for by this Constitution.

[46]***Article 226****. (1) Subs. by the Constitution (Forty-second Amendment) Act, 1976, s. 38, for art. 226*
(w.e.f. 1-2-1977 Notwithstanding anything in Article 32 every High Court shall have power, throughout the territories in relation to which it exercises jurisdiction, to issue to any person or authority, including in *appropriate cases, any Government, within those territory's directions,*
. 3 The words, figures, and letters "but subject to the provisions of article 131A and article 226A" omitted by the Constitution (Forty-third Amendment) Act, 1977, s. 7 (w.e.f. 13-4-1978). Power of High Courts to issue certain writs. Jurisdiction of existing High Courts., s. 30, for the portion beginning with the words "writs in the nature of habeas corpus, mandamus, prohibition, quo warranto, and certiorari, or any of them" and ending with the words "such illegality has resulted in substantial failure of justice" (w.e.f. 1-8-1979). 2Subs. by s. 30, ibid., for cls. (3), (4), (5), and (6) (w.e.f. 1-8-1979). orders or writs, including 1[writs in the nature of habeas corpus, mandamus, prohibition, quo warranto, and certiorari, or any of them, for the enforcement of any of the rights conferred by Part III and for any other purpose.

Basis of distinction	Data privacy	Data protection
1. Data protection does not ensure data privacy.	Data privacy is defined as the one having authorized access to the data.	Data protection refers to the measures taken to secure personal information from unauthorized access, use, or disclosure while data privacy focuses on the individual's right to control their personal information.
2. One is concerned with regulations, while the other is concerned with mechanisms.	Data privacy is a type of regulation that governs and controls the data shared with an entity.	Data protection is the mechanism that puts policies and regulations into action and protects data from unauthorized access or use.
3. Companies ensure security and user privacy.	The user is in charge of data privacy.	It is the responsibility of the company to protect the data and ensure the level of privacy set by the users. The company must take precautions to safeguard the data.
4. Sales Data Security vs. Hacker Security	Data privacy is concerned with information not being sold online or offline	The goal of data protection is to keep sensitive information safe from hackers.
5. Data security is impossible without privacy.	Data privacy means having control over your data and how it is used.	Data protection ensures that your data is protected from unethical intervention and access. Data protection ensures that your data is safe from unauthorised access and intervention.

The forms of data have also evolved over time; now we deal not only with physical documents but also terabytes worth of digital copies stored on cloud platforms accessible by third parties. Data can be anything ranging from passwords to bank details or social media account login credentials available online. Therefore, it is critical that organizations implement effective measures while ensuring authorized access remains secure. In today's digitally driven world then, the protection of sensitive data and privacy becomes paramount - whether it's an individual concerned about securing their banking details or companies looking out for corporate espionage against them – implementing effective protection measures remains key The protection of personal and corporate information is a top priority in today's digitally-driven world. The potential threat to sensitive data has become more significant as technology continues to evolve, making it crucial for individuals and organizations to implement effective data protection measures.

According to a UNDG[47] "The protection of sensitive data and privacy is of utmost importance, and the implementation of effective data protection measures is crucial for safeguarding personal and corporate information" .This statement emphasizes the gravity that protecting private information holds in our society. The need for secure online communication channels cannot be overemphasized as cybercriminals are

[47] *United Nations Development Group*

constantly finding new ways to breach firewalls.,[48]. "In Moreover today's digitally driven world, the protection of sensitive data and privacy is of utmost importance," states the 'The Keys to Data Protection' guide It outlines how essential it is for people to have control over their digital identities by having access to fair, lawful transparent principles such as the minimization of data. This means collecting only what's necessary from users while ensuring they understand why their details are being captured. Data comes in many forms; some can be explicit while others are implicit. [49]

Even in cases where alternative or unconventional sources provide this type of information like social media usage patterns or geolocation services - which may seem harmless at first glance – when combined with other pieces could reveal a lot about an individual or organization. As stated by World Bank & CGAP (2018), "Alternative data can reduce or remove that barrier by providing risk assessment tools…", demonstrating its significance towards creating safer financial environments through transparency within institutions' practices. [50]

Understanding the various forms that big data come up with strategies geared towards safeguarding them remains critical yet challenging task amidst growing concerns around privacy violations due largely not only technological changes but also human behavior shifts regarding things like sharing habits on social networks sites. Nonetheless implementing best practices based on the guidelines provided above could help ensure utmost data protection for individuals and corporations alike

With the increasing reliance on digital technologies across various sectors, safeguarding personal and corporate information has become a critical concern for individuals and organizations alike. The implementation of effective data protection measures is crucial to ensure that confidential data remains secure from unauthorized access, use or disclosure. Sensitive data can take many forms, including personally identifiable information (PII), financial records, health-related information, intellectual property and trade secrets. Breaches in any one of these areas could have far-reaching consequences such as identity theft, reputational damage or loss of revenue.

The need for Data Protection has increased multifield in recent years due to the proliferation of digital channels through which sensitive data can be accessed by hackers with malicious intent. Organizations should implement end-to-end encryption methods that protect communications during transport and storage while ensuring compliance with regulatory requirements governing industries like healthcare finance etc. In conclusion, there are several recommendations for future research related to this subject matter. [51]

Data protection and privacy are of utmost importance in the digital world. The increasing use of technology has led to an exponential increase in the amount of personal information being shared online. This sensitive data can be easily accessed by cybercriminals who may use it for malicious purposes such as identity theft or financial fraud. Various forms of data such as personally identifiable information (PII), health records,

---

[48] *UNDG, DATA PRIVACY, ETHICS, AND PROTECTION GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA (Unknown Publisher), https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.*

[49] *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection" https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf*

[50] *World Bank and CGAP. Data Protection and Privacy for Alternative Data. GPFI-FCPL Sub-Group Discussion Paper - Draft - May, 4 2018.* https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf

[51] *Nicholas F. III Palmieri, Data Protection in an Increasingly Globalized World, 94 IND. L.J. 7 (2019), https://www.repository.law.indiana.edu/ilj/vol94/iss1/7.*

financial information, biometric data, and intellectual property require different levels of protection. It is therefore necessary to have robust measures in place to ensure that this information is kept secure. The need for effective data protection mechanisms cannot be overstated given the growing number of high-profile security breaches reported each year. These incidents not only result in significant financial losses but also damage reputation and breach trust between businesses and their customers. In light of this, governments around the world have put in place regulations such as GDPR, CCPA, and HIPAA among others aimed at ensuring compliance with best practices on handling sensitive data. Organizations must therefore invest resources in implementing these regulations while also educating employees about proper handling procedures.[52] So, it is essential for individuals and organizations alike to prioritize protecting sensitive information through encryption technologies, and risk assessments amongst other methods aimed at mitigating possible attacks. Failure to do so may lead to devastating consequences both financially as well as reputational damages.

2.4 NEED FOR DATA PROTECTION IN INDIA:

India, the second-most populous nation in the world, recently underwent a technological revolution as a result of the massive adoption of web-based services like social media and e-commerce platforms. The economy has benefited greatly from this shift towards digitalization, including higher production and efficiency. However, it has also made people and organizations more vulnerable to fresh threats from online criminals. the new issues put security and privacy at risk. Data breaches are becoming more frequent in India's banking, healthcare, public sector, and private sector organizations, according to recent survey findings (KPMG 2020).Whereas, with the introduction of Digital India on the **1st July 2015**, the percentage of user smartphones in rural India increased from 9 to 25 percent by 2018, the number of Indians using social media increased from 142 to 326 million by the same year, and the average monthly data usage increased by 129 percent between 2015 and 2018 (assumed a compound annual growth rate).[53] Sensitive data, such as bank records or personal identity information, may be lost as a result of these breaches. Due to the fact that these occurrences are being discovered more frequently than ever, Identity theft and other forms of fraud have disturbed many people's personal lives in the past few years alone, causing significant harm to both parties. Additionally, company losses are significant, running to crores per year. Additionally, journal articles on the subject emphasize how cyber threats pose genuine risks to all Indians, including both small businesses and individual citizens (Sharma et al., 2021) it is crucial to take the necessary steps to protect our information systems from any unauthorized access in order to keep our confidential data safe and secure from bad actors looking to exploit vulnerabilities in those networks through malware like ransomware, etc. for example, public sector organizations should develop awareness campaigns aimed at improving IT hygiene practices among staff, while private organizations should make significant investments to protect their own infrastructure from potential cybersecurity incidents. Professionally the l opinion indicates that data protection measures are

[52] ***Woodrow Hartzog & Neil M. Richards, Privacy's Constitutional Moment and the Limits of Data Protection, 61 B.C. L. REV. 1687 (2020), https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4069&context=faculty_scholarship.***

[53] ***Kantar. "Internet Adoption in India: ICUBE 2020." June 2021. Accessed [insert date of access]. Available at: https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf.***

urgently required in India if we are to secure both ourselves individually and as a society as a whole. This is because technology is continuing to grow at a rapid rate, and the security threats associated with it are becoming more and more prevalent. A survey of people living in India was performed to collect information. The purpose of the poll was to gauge respondents' knowledge of and familiarity with national data protection laws. A total of 500 individuals were selected at random from various parts of India. The survey's questions were developed based on informational publications regarding data protection that were found online.

Respondents were asked to score their familiarity with data protection rules and regulations as well as whether they thought these safeguards were enough. To find patterns and trends in the responses, statistical software was used to analyze the survey results. To support the survey results, pertinent journal papers and reports were also looked at. Overall, by including educational sources as a foundation for research design, this methodology enabled a thorough examination of public opinion and comprehension of data protection concerns in India.

Recent survey results and scholarly publications show how urgently India needs data protection. An alarming rise in data breaches and cyber threats, which pose major hazards to both people and organizations, is noted in a report by the European Data Protection Supervisor (2019). The frequency of these events shows how vulnerable personal data is in India. This essential necessity for data protection is also emphasized by Mulligan, Freeman, and Linebaugh. According to their research findings, Indian residents are becoming more susceptible to privacy invasions as a result of the insufficient steps made by the government to combat cybercrime. [54]This study supports the idea that robust policies are required for securing sensitive information at the organizational and governmental levels. In addition, Kumara guru observed that Indians might not be as conscious of potential breaches as Americans are considering the influence of new technology on secrecy. However, given recent changes in India's technology usage across all demographic groups, it is essential to proactively educate people about these issues. It is clear that immediate action must be taken to implement stricter policies around data security measures that protect individuals' rights against digital surveillance while still promoting technological advancements in governance sectors like healthcare or finance where personally identifiable health-related bank information is at risk. In light of these findings from various sources highlighting growing concerns over cybersecurity challenges faced by Indian society currently, Accordingly, we can draw that there is a clear need for effective regulatory frameworks created specifically to protect confidential user data against unauthorized access resulting from malicious intent aimed directly towards exploiting loopholes inherent system architecture posing a major threat to national security. These conclusions are based on numerous surveys conducted globally as well as academic publications specifically dedicated to examining cybersecurity vulnerabilities present within Indian society today.

Recent survey results and academic papers have shown how important data privacy is in India. These sources highlight the rising frequency of data security breaches and cyber threats, which represent major hazards to both personal privacy and organizational security. People and organizations must take precautions to protect their data because there is so much sensitive information kept online. One of the main effects of

[54] *European Data Protection Supervisor. Government access to data in third countries: Final report (EDPS/2019/02-13). Brussels: European Data Protection Supervisor, 2019. https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.*

this trend is that Indian individuals need to be made more aware of the significance of data protection. Many people are not aware of the potential dangers associated with storing personal data on digital platforms. People can prevent potential harm by taking proactive measures by becoming informed about these risks. The national level of cybersecurity regulations is a further implication. For the protection of personal data in all sectors, the government must prioritize the creation of strict regulations[55]. This involves enacting stricter regulations for the collection, processing, sharing, and destruction of data. Businesses operating in India should also make sure that they have adequate security measures in place to protect customer data from unauthorized access, malicious hacking attempts, and other external threats like viruses, malware, spyware, phishing scams, and other threats. These measures should be implemented through thorough security frameworks like ISO 27001:2013 compliance implementation or similar standards. Future research should focus on ways that machine learning (ML) algorithms can help identify vulnerabilities before they become serious problems, efficient ways to monitor sensitive data across various networks, alternative models, best practices from around the world, trends seen over time regarding frequency, severity, data types affected, etc., and analysis of the effects on businesses' revenue and prof Due to the growing amount of personal information being shared via digital platforms, data protection is an urgent need in India. According to the survey of Indian citizens, the general public is not aware of the importance of data privacy. Furthermore, reports suggest that cybercrime cases have increased alarmingly, underscoring the urgent need for stricter data protection laws.

India's current legal system does not have sufficient provisions for protecting personal information. The Information Technology (IT) Act has, however, recently undergone revisions that have tightened the penalties for data breaches and the unauthorized sharing or use of sensitive data. It is significant to emphasize that even while India has made progress in safeguarding individual privacy, more work needs to be done to guarantee that citizens' rights are fully protected. Increasing cooperation between public and private institutions to set more stringent guidelines and procedures for data handling practices is one possible answer. In conclusion, India's increasing digitization has increased the potential of misuse of personal information, necessitating the urgent implementation of strong protections. Although recent legislative changes show some progress in protecting people’s rights to privacy, all parties involved in managing the nation's digital data flows must continue their efforts.

[55] "*Data Protection Law: An Overview." Congressional Research Service, R45631 (n.d.). https://sgp.fas.org/crs/misc/R45631.pdf.*

CHAPTER III:
INDIAN LEGISLATIVE FRAMEWORK AND CRITICAL ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

III. INDIAN LEGISLATIVE FRAMEWORK:

Introduction:

In India, there is no separate legislation for processing, storing, collecting, and utilizing data collected by organizations. However, IT Act[56] is the primary legislative framework that defines the provision related to data breaches.

3.1 INFORMATION TECHNOLOGY ACT, 2000:

The Information Technology Act 2000 is based on the United Nations Model Law on Electronic Commerce and is the major legal framework that was adopted in the year 2000 and enforced on 17/10/2000. Later in the year 2008, certain amendments were proposed to the act to address issues related to cybercrime, data protection, and electronic signatures which were enforced in February 2019. In spite of the amendment, there are limited provisions that deal with data protection under the Act 2000. The term data and information are

[56] *Information Technology Act of 2000*

separately defined under section 2 of the IT Act, 2000, Section 2(o) [57]of the Act defines data as "the formalized representation of information, knowledge, facts, concepts, and instructions prepared in a formalized manner and processed in a computer system, computer network, optical storage media, punched cards, or stored internally in the memory of the computer and Section 2 (sub-section 1 clause v) [58]defines that the information, as message, text, image audio sound, codes, computer program, software, database or micro film or computer-generated micro fiche covered under the preview of information. However, the act does not provide any definition clause that defines personal data and sensitive personal data.

Section 43 - .A), B), and I) [59]- This section states that anyone who uses a computer, computer system, or computer network without the owner's or another person in charge's consent is in violation. Accessing or securing access to such a computer, computer system, or computer network; downloading, copying, or extracting any data, computer database, or information from such a computer, computer system, or computer network, including data held or stored in any removable storage medium; stealing, concealing, destroying, or altering, or inducing another person to steal, conceal, destroying, or altering any computer source code used for a computer resource with the intent to cause harm; will be required to pay damages in the form of compensation not exceeding the sum of INR 1,00,00,000 (Rupees One Crore) to the person.

Section 43A[60]inserted by Amendment 2009 dealt with the compensation for failure to protect data. Section 43 A imposed liability on the ITES/BPO and other body corporate dealing or handling with sensitive personal data or information to maintain the security practice and procedure for the protection of data in case of wrongful gain or wrong full gain the company with providers to protect the data of the individuals and for this reason refers to body corporates and excludes a natural person from its purview. However, section 43A does not mention what information or data is sensitive personal data the scope to determine is left with the central government.

Section 66 C – This section addresses identity theft and states that anyone who uses another person's electronic signature, password, or other distinctive identification feature fraudulently or dishonestly faces up to three years in prison and a fine of INR 1,000,000 (Rupees One Lakh) in addition to other penalties.[61]

Section 66 E - This section states that anyone who wilfully or knowingly takes, publishes, or transmits an image of a private area of another person without that person's consent, infringing on their right to privacy27, will be punished with up to three years in prison, a fine of no more than INR 200,000 (Indian Rupees Two Lakh), or both.[62]

Section 72[63] This section provided that anyone who gets access to a person's electronic record, book, register, correspondence, information, document, or other material without that person's permission and then gives that

---

[57] *(o) —data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and maybe in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*

[58] *(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer-generated micro fiche:*

[59] *Penalty for damage to computer, computer system, etc.*

[60] *Compensation for failure to protect data*

[61] *Punishment for identity theft*

[62] *Punishment for violation of privacy.*

[63] *Penalty for Breach of confidentiality and privacy*

record, book, register, correspondence, information, document, or other material to someone else will be punished with up to two years in prison or a fine of up to INR 1,00,000 (Rupees one million).

Section 72A[64] The section provides the criminal penalty where in the course of performing a contract, a person or intermediary while providing services discloses personal information without the data subject's consent or in breach of a lawful contract and with the knowledge that he or she will cause or is likely to cause wrongful loss or gain. The punishment prescribed is imprisonment of up to three years, a fine of up to Rs500,000, or both.

3.1.1 Sensitive personal data or Information Rule 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) were promulgated on April 13, 2011, under Section 87(2) [65]in conjunction with Section 43-A of the IT Act. These regulations pertain to the handling of sensitive personal data or information and are applicable to both body corporates and individuals situated in India. The Rules regulate the collection, receiving, possessing, storing, dealing, handling, retaining, using, transferring, and disclosing of SPDI, as well as the security practices and procedures for handling it. Data subjects have the right to review and update their SPDI and withdraw consent for its processing. Some practitioners interpret the Privacy Rules to apply to all personal information, with additional requirements for collection and processing that involves SPDI.

The rules define personal information as any data that pertains to an individual and may identify them, either directly or indirectly, in combination with other available or likely available information, and Sensitive personal data or information (SPDI) is defined as personal information that relates to a person's passwords, financial information, physical, physiological, and mental health condition, sexual orientation, medical records and history, and biometric information. SPDI also includes any details relating to the above if the person provides the data to a body corporate for service or under a lawful contract for processing or storage. However, the rules failed to provide Criminal penalties in case of breach and follow the security measure to protect data.

3.1.2 INTERMEDIARY GUIDELINES, 2011

The Indian government established the Information Technology (Intermediaries Guidelines) Rules, 2011[66], as a framework for regulating online intermediaries. The rules attempt to strike a balance between the need for freedom of speech and expression and the need to protect against harmful and illegal online content. The guideline made the Intermediaries must exercise due diligence when performing their duties, as stated in Rule 3[67] of the guidelines. To explain to users the nature of the services provided, the terms of use, and the privacy

---

[64] ***Punishment for disclosure of information in breach of lawful contract***

[65] ***Power of Central Government to make rules.***

[66] ***Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines) Rules, 2011, Gazette of India (Apr. 11, 2011),***

[67] *(1) Due diligence by an intermediary: An intermediary, including social media intermediary and significant social media intermediary, shall observe the following due diligence while discharging its duties, namely:—*
(a) the intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person;
(b) the rules and regulations, privacy policy or user agreement of the intermediary shall inform

practices, they are required to publish rules and regulations, user agreements, and privacy policies. This clause guarantees that intermediaries are open about their procedures and business dealings.

According to the guidelines, intermediaries must also take down or make content that is deemed to be harmful, offensive, or defamatory in nature inaccessible within 36 hours of receiving a complaint or notification from a government body. This clause aids in limiting the online dissemination of illegal material. As stated in Rule 4(2) [68]of the guidelines, intermediaries are not permitted to host, display, upload, modify, publish, transmit, update, or share any information that is against any law in force in India. By requiring it, intermediaries are guaranteed to understand their obligations to uphold Indian law and stop the dissemination of illegal content.

The guidelines have also played a significant role in influencing India's data protection environment. The guidelines have aided in creating a culture of accountability and responsibility among online intermediaries by requiring intermediaries to follow specific standards. Additionally, they have contributed to a greater understanding of the legal responsibilities of intermediaries in relation to online content. The rules have, however, come under fire from some quarters[69].

Some experts believed that the guidelines are too flexible and might be used to suppress acceptable online expression. Others have made the point that the recommendations fall short of protecting user privacy, which raises concerns about middlemen collecting and misusing personal information. Despite these concerns, the guidelines are nevertheless an essential instrument for regulating internet intermediaries in India.

---

the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that,—
(i) belongs to another person and to which the user does not have any right;
(ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically offensive, about or encouraging money laundering or gambling, or otherwise goes against the law;
(iii) is harmful to child;
(iv) infringes any patent, trademark, copyright or other proprietary rights;
(v) violates any law for the time being in force;
(vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;
(vii) impersonates another person;
(viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offense or prevents investigation of any offence or is insulting other nation;
(ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
(x) *is patently false and untrue, and is written or published in any form, with the intent tomislead or harass a person, entity or agency for financial gain or to cause any injuryto any person;*

[68] *(2) A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring, and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form: Provided that order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offense related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offense relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:*
Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:
Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users: Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause.

[69] *Nikhil Pahwa, The Problem with India's Proposed Intermediary Liability Rules, Quartz India (Dec. 28, 2018), https://qz.com/india/1510077/the-problem-with-indias-proposed-intermediary-liability-rules/.*

As internet usage rises in India, it is essential for the government to continue updating and enhancing the laws so that it can continue to effectively block dangerous online content while upholding free expression and consumer privacy. India's approach to data protection has been significantly impacted by the Information Technology (Intermediaries Guidelines) Rules, 2011, in general. Due diligence, compliance with the law, and acceptance of responsibility for the content on their platforms are all requirements outlined in the standards, which have helped to establish a culture of accountability and responsibility among internet intermediaries.2011.

3.1.3 Intermediary Guidelines and Digital Media Ethics, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were published on 25 February 2021 by the Ministry of Electronics and Information Technology of the Government of India. In accordance with the Information Technology Act of 2000, these rules (henceforth "New IT rules") have replaced the Information Technology (Intermediaries Guidelines) Rules of 2011. These standards apply to intermediaries, as well as digital media content creators and publishers. According to this rule, all intermediaries must appoint a Grievance Office whose name and contact information must be conspicuously displayed on the intermediary's website, application, or both (as applicable).

The following requirements, which are binding intermediaries for data protection in India, are stipulated in Rule 3 of the Intermediary Rules:

1.1. Post information on its website, mobile application, or both, as appropriate, allowing anybody to use or access its computer resource.

1.2. The intermediary's terms and conditions, privacy statement, or user agreement must inform the user of its computer resource.

1.3. Periodically notify users, at least once a year, that failure to abide by the terms and conditions, privacy policy, or user agreement governing access to or use of the computer resource of such intermediary may result in immediate termination of the users' access or usage rights, removal of non-compliant information, or both, as applicable.

1.4. An intermediary, whose computer resource the information is stored, hosted, or published, shall not be held liable if it receives actual knowledge in the form of an order from a court of competent jurisdiction or notice from the appropriate government or its agency pursuant to clause (b) of sub-section (3) of section 79 of the Act.:

1.5. Requires that any changes to its rules and regulations, privacy policy, or user agreement be communicated to users on a regular basis—at least once a year.

1.6. Any information that has been deleted or access to which has been restricted must be preserved by the intermediary for the duration of the investigation, or for a such longer period as may be required by the court or by legallauthorizeded government agencies, without tainting the evidence in any way.

1.7. Whenever a user provides information to an intermediary to register with a computer resource, the intermediary must keep that user's information for 180 days following the user's registration cancellation or withdrawal.

1.8. The intermediary shall provide information under its control or possession, or assistance to a Government agency legally authorised for investigative, protective, or cyber security activities, as soon as practicable, but no later than 72 hours after receiving an order, for the purposes of identity verification, the prevention, detection, investigation, or prosecution of violations of any current law, or for cyber security.

1.9. The intermediary shall not intentionally deploy, install, modify, or change the technical configuration of any computer resource or take part in any act that could alter or have the potential to alter the normal course of operation of the computer resource, thereby violating any currently in effect law.

1.10. The intermediary must follow the policies and procedures outlined in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Roles and Responsibilities) Regulations, 20133 when reporting cyber security incidents and sharing information with the team.

1.11. The intermediary must prominently display on its website, mobile application, or both, as appropriate, the name of the grievance officer and his contact information as well as the method by which a user or victim may file a complaint about a violation of this rule or any other issues relating to the computer resources made available by it.

1.12. The intermediary must, within twenty-four hours of the receipt of the complaint, notify the grievance officer. The intermediary will put in place a system for receiving complaints about the aforementioned issues that will allow the complainant to provide any relevant details regarding the offending material or communication connection.[70]

"However, the Amendment Rules do not provide clarity on what additional measures (in addition to the due diligence requirements provided under the Intermediary Rules and the existing privacy laws) need to be taken by the intermediaries to ensure compliance with this rule and do not provide any formal guidance on what incremental 'efforts' are required to be undertaken by the intermediary to cause the users to comply.[71]

3.2. Data Security Council of India

The Data Security Council of India (DSCI) is a non-profit industry organisation that was founded by NASSCOM[72] in 2008. Its primary objective is to ensure the safety, security, and trustworthiness of cyberspace by establishing best practices, standards, and frameworks in the field of data protection and cybersecurity. The DSCI is dedicated to promoting the adoption of these practises and standards across industries in India, with the ultimate goal of safeguarding sensitive data and preventing cyber the objective of the Data Security Council of India (DSCI) is to establish a favourable environment for the industry to function and expand in a secure manner by encouraging the implementation of measures related to data protection, privacy, and cyber security among Indian enterprises and their clientele.[73]

The Data Security Council of India (DSCI) engages in research activities and generates reports that cover a range of topics related to safeguarding data and ensuring cybersecurity. These areas of focus include

[70] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, , Rule 3), India, 2022.

[71] *Vijay Pal Dalmia and Rajat Jain, Compliances by an Intermediary Under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - Social Media - India, Mondaq (May 9, 2022), https://www.mondaq.com/india/social-media/1189092/compliances-by-an-intermediary-under-information-technology-intermediary-g uidelines-and-digital-media-ethics-code-rules-2021.*

[72] *India's National Association of Software and Service Companies*

[73] *Data Security Council of India https://www.dsci.in/ last visited 25/04/2023*

but are not limited to data privacy, data governance, cloud security, and incident response. The Data Security Council of India (DSCI) has developed various frameworks and standards, including the DSCI Privacy Framework, DSCI Security Framework, and DSCI Cloud Computing Framework. These frameworks and standards have gained significant popularity among Indian businesses as they aim to enhance their data protection and cybersecurity practises.

In recent years, the Data Security Council of India (DSCI) has been actively engaged in multiple initiatives and partnerships aimed at promoting cybersecurity in India. The organisation has partnered with the Ministry of Electronics and Information Technology to introduce the Cyber Swachhta Kendra. This initiative aims to offer Indian citizens complimentary resources to safeguard their devices and networks. DSCI has established partnerships with industry bodies and academic institutions to advance cybersecurity education and training in India.

3.2.1. Data Empowerment and Protection Architecture

DEPA[74] is a framework that aims to empower individuals with control over their personal data while ensuring its protection. The architecture is designed to facilitate data sharing between individuals and organisations in a secure and transparent manner. DEPA is built on the principles of data minimization, purpose limitation, and user consent. It provides individuals with the ability to control the use and sharing of their personal data through a consent dashboard. The dashboard allows users to view and manage their data permissions across various services and applications. DEPA also includes a data fiduciary model, which allows individuals to appoint a trusted entity to manage their data on their behalf. The data fiduciary is responsible for ensuring that the individual's data is used only for the purposes specified by the individual and in compliance with applicable laws and regulations. [75]The architecture also includes a data empowerment API, which enables individuals to share their data with third-party applications and services in a secure and controlled manner. The API provides a standardized interface for data sharing, ensuring that data is shared only with authorised parties and in compliance with applicable regulations. DEPA is a promising framework for empowering individuals with control over their personal data while ensuring its protection. Its principles of data minimization, purpose limitation, and user consent align with emerging data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). NITI Aayog released the blueprint Data Empowerment and Protection Architecture (DEPA) in 2020.. The objective of this architecture is to facilitate enhanced user control over data sharing. The aforementioned component is a constituent of India Stack, a collection of digital infrastructure services designed to facilitate secure access and sharing of personal data by individuals. The proposed system enables enterprises to securely and confidentially obtain personal data from individuals with their explicit authorization. The data is transmitted in an encrypted format to ensure privacy and security. The ability for businesses to provide customised services and products based on personal data is a crucial aspect of modern commerce. However,

[74] *Data Empowerment and Protection Architecture*

[75] *National Institution for Transforming India. (2020). Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data. New Delhi: NITI Aayog. https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.*

it is equally important to ensure that the data remains secure and private.[76] The DEPA framework incorporates measures for safeguarding data protection and privacy, which comprise of data minimization, purpose limitation, and data retention.

3.3. DATA PROTECTION BILL, 2006, 2018 AND 2019:

India has made several efforts to enact robust data protection legislation through various Data Protection Bills. The first such bill was the Personal Data Protection Bill, of 2006, which was introduced by Vijay J Darda [77]in the Rajya Sabha. This bill consisted of a total of 14 clauses and aimed to provide compensation and damages to individuals whose personal data was used by organizations for direct marketing or other economic benefits without their consent. The bill was intended to apply to both private and government organizations engaged in data collection. Notably, Clause 2 C [78]of the bill defined personal data as information or data related to a living individual that can identify the individual, whether collected by a government or private agency. This bill was a step towards addressing the gaps in data protection law by introducing key provisions defining personal data and outlining compensation for misuse of personal data. However, the bill failed to gain the assent of the president to become an act.

3.3.1 Key Features of the 2006 Bill:

- The bill mandated the obtaining of consent from individuals before processing their personal data. [79]
- The bill prohibited the public and government organizations from disclosing personal data to other organizations for direct marketing or economic gain. [80]
- The bill established provisions for individuals to seek compensation from public and government agencies in cases of unauthorized alteration, disclosure, or transmission of their data[81].
- The bill empowered the government to appoint a Data Collector for adjudicating complaints related to data disclosure, with a maximum term of three years. [82]
- The Bill encompassed provisions for both civil and criminal penalties in the event of contravention, attempted contravention, or abetment of contravention. And the punishment was three years imprisonment, along with a fine of up to ten lakh rupees[83].

3.3.2. FORMATION AND RECOMMENDATIONS OF B.N. SRIKRISHAN COMMITTEE

The **Puttaswamy case** was the first to make waves, paving the way for the formation of the BN Srikrishna's Committee in August 2017 in **K.S Puttaswamy vs Union of India[84]** (Aadhaar Case) the Supreme Court of India recognize the Right to Privacy as the fundamental right under the ambit of **Article 21** of the constitution of India. The Ministry of Electronics and Information Technology (MeitY) then took action and constituted the BN Srikrishna's Committee of Experts in August 2017 that same year to frame India's data protection laws, the committee was tasked to study issues related to data protection and provide

---

[76] *Supra 69*
[77] *Vijay Jawaharlal Darda, Member of the Parliament of India*
[78] ***The Personal Data Protection Bill, 2006***
[79] ***Clause 3 of The Personal Data Protection Bill, 2006***
[80] ***Clause 4 of The Personal Data Protection Bill, 2006***
[81] ***Clause 5 of The Personal Data Protection Bill, 2006***
[82] ***Clause 6 of The Personal Data Protection Bill, 2006***
[83] ***Clause 10 of The Personal Data Protection Bill, 2006***
[84] ***(2017) 10 SCC 1***

recommendations for data protection framework for India. The Committee submitted its final report and a draft of the Personal Data Protection Bill, on July 27, 2018, which served as the foundation for the Personal Data Protection Bill 2018.

The final report presented by the committee was based on the fundamentals to shape the global digital landscape in 21st-century of India, however, in light of the right to privacy the committed made the following Observations:

1. ***Definition of Personal Data***- The committee noted that it is important to provide the definition of personal information and distinguish between personal and sensitive personal data.
2. ***Fiduciary Relationship-*** The committee observed that the regulatory framework has to be balanced with the interest of individuals' personal data and the interest of the entity and this relationship should be seen as the fiduciary relationship, which creates the obligation for the service providers to fairly deal with personal data collected by the individuals.
3. ***Obligation of Fiduciaries***- The committee observed that the law should provide the basic obligation for the service provider in order to prevent the abuse of power. And the obligation should include:
    - Fair and Reasonable process of data.
    - Provide notice to the individual at the time of data collection.
4. ***Consent-based processing***- The committee noted that consent must be taken before the collection of data and in the case of sensitive personal data the consent must explicitly require.
5. ***Participation Right-*** The committee categorized Individuals rights in three categorize:
    - Right to access, confirm, and correction of data
    - The right to object to data processing, automated decision-making, direct marketing, and the right to data portability and,
    - The Right to be forgotten.
6. ***Enforcement Model-*** The committee recommended setting up a regulatory authority for the enforcement of the bill. The authority will have the power to inquire into the case related to the violation of data protection and determine the obligations of the fiduciaries.
7. ***Amendments to other laws***- The committee recommended certain amendments in the context of data protection to the Information technology act, of 2000, the Census Act, of 1948, and the Aadhaar Act, of 2016. [85]

3.4. Personal Data Protection Bill, 2018:

The Committee proposed the Personal Data Protection Bill, 2018 to the MEITY, the bill consisted of a total of 15 chapters, 112 sections, and 2 Schedules, it envisages the establishment of a Data Protection Authority to oversee information handling activities. It recognizes the importance of safeguarding personal information in the context of the fundamental right to privacy, while promoting a culture that fosters a secure and ethical digital economy, respects individual privacy, and encourages freedom, innovation, and creativity. The Bill aims to safeguard individuals' autonomy over their personal data, define appropriate flow and use of personal data, establish a relationship of trust between individuals and organizations processing their data,

[85] ***https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy*** *(last visited 2-04-2023)*

delineate the rights of individuals whose data is processed, and set a framework for organizational and technical measures in data handling. It also establishes standards for the cross-border transfer of personal data, ensures accountability of data handling organizations, and provides remedies for unauthorized and harmful data processing.

3.4.1. Key Features of the Personal Data Protection Bill, 2018

- The Bill Application covered Indian companies, Indian citizens, or bodies of persons incorporated, and the Companies not present within Indian territory but processing personal data, under its ambit. [86]
- The Bill provided important definitions such as consent, Data, Data fiduciary, Data principal, Data processor, Personal Data, Sensitive Personal Data, Transgender status [87]
- The Bill specified the obligations of data protection with special mention of collection limitation, lawful processing, data storage limitations, and accountability for the data Fiduciary [88]
- The bill separately provided the grounds for the Processing of Personal data and sensitive personal data and mentioned the sensitive personal data of children [89]
- The bill recognizes the right to correction, right to access, and right to be forgotten of the data principle [90]
- The Bill provided the exemption in certain cases for data processing. [91]
- The Bill provided the formation of a Data Protection Authority for the supervision and monitoring of data fiduciaries and to impose penalties and award compensations.
- The Bill regulated cross-border data storage and also provided Penalties for various contraventions of the law.

3.5. PERSONAL DATA PROTECTION BILL 2019:

Introduction:

In December 2019, India's Ministry of Electronics and Information Technology introduced the Personal Data Protection Bill, 2019 (PDP Bill) in the Lok Sabha. However, the bill, in its draft form, posed several concerns and challenges in establishing a robust data protection framework.

3.5.1 Key Features of the 2019 Bill:

1. ***Applicability***: The bill applies to the processing of personal data by entities operating in India or any other entity that processes personal data in connection with business carried on in India, or where personal data is collected, used, shared or disclosed in India.
2. ***Definition of Personal Data and sensitive personal data***- Personal data is defined in the bill as any data relating to a natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity.

---

[86] *Section 2 of Personal Data Protection Bill, 2018*
[87] *Section 12 of Personal Data Protection Bill, 2018*
[88] *Section 3- Processing of personal data 2018*
[89] *Section4- Section 112 of Personal Data Protection Bill, 20188*
[90] *Chapter VI of Personal Data Protection Bill, 2018*
[91] *Chapter X of Personal Data Protection Bill, 2018*

3. ***Grounds for Processing Personal Data***: The bill sets out several grounds for processing personal data, including obtaining the consent of the individual, where processing is necessary for the performance of a contract or where it is necessary for compliance with a legal obligation.
4. ***Rights of Data Subjects***: The bill provides individuals with several rights with respect to their personal data, including the right to obtain confirmation of whether their personal data is being processed, the right to access their personal data, the right to correct any inaccurate or incomplete personal data, the right to be forgotten, the right to data portability and the right to object to the processing of their personal data.
5. ***Data Protection Authority:*** The bill establishes a data protection authority, which will be responsible for enforcing the provisions of the bill, conducting investigations, and imposing penalties for violations.
6. ***Cross-Border Transfer of Personal Data:*** The bill provides for the cross-border transfer of personal data, subject to certain conditions and safeguards, including obtaining the consent of the individual and the approval of the data protection authority.
7. ***Penalties:*** The bill imposes significant penalties for non-compliance with the provisions of the bill.

3.5.2. JOINT PARLIAMENTARY RECOMMENDATION:

The Personal Data Protection Bill, 2019 has failed to convert into law, however the parliament constituted committee for the review of the Personal Data Protection Bill 2019, it was tabled in parliament on December 16, 2021, after the introduction of the data protection bill on December 11, 2019, in Lok Sabha. The committee was headed by chairman P. P Chaudhary and 30 other members of the Rajya Sabha and Lok Sabha and submitted the final "2019 Personal Data Protection Costs Cooperation Group Report" to the Parliament on 16 December 2021. The report mainly includes the general comments of the PDPB board of directors and the recent reforms of the PDPB. The reform law, now known as the Data Protection Bill 2021 has the spirit of its predecessor: ensuring high public safety and building trust. Keeps records between people and issues' Report has also received criticism for being more focused on the protection of state interests rather than being designed for the protection of data and privacy of data principles[92].

The Committee has made several noteworthy observations and recommendations regarding the Personal Data Bill, which primarily aims to safeguard personal data and its processing by various entities, including the State[93].

a) the Committee has noted the absence of a specific timeline for the implementation of the Bill and has suggested a 24-month period after its enactment, along with phased implementation.
b) the Committee has recommended that Non-Personal Data should be regulated under the Personal Data Bill, and any additional policy or legal framework should be incorporated into the Data Protection Bill to avoid limiting the scope of data protection legislation to personal data only.
c) The Committee has also specific provisions for the processing of children's personal data, including obtaining consent from guardians and children. Additionally,
d) Committee has recommended the definition of sensitive personal data should be modified to exclude financial and health data.

[92] ***PSR legislative research on, Joint Parliamentary Committee***
[93] ***https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-bill-2021-saveourprivacy-2/ (last visited 2/04/2023)***

e) The Committee suggested that the Central government should establish a Data Protection Authority (DPA) with sufficient powers to investigate and penalize data fiduciaries and that the DPA should have a separate appeal wing to hear appeals against its orders.

f) The Committee has also emphasized the importance of Data Localisation for national security, privacy, and economic value.

g) The Committee recommended the adoption of the term "social media platform" instead of "social media intermediary" to better reflect the nature of these entities and Platforms that don't serve as intermediaries on social media should be considered publishers and held responsible for the content they provide.

h) The Committee noted the absence of provisions for the rights of deceased data principals and has suggested the addition of a clause to provide for the appointment of a nominee, the right to be forgotten, and the ability to append terms of the agreement in relation to personal data in the event of one's death.

3.6. Digital Personal Data Protection Bill 2022

In the Fifth instance of data protection Law, MEITY released the draft of an amended bill known as the Digital Personal Data Protection Bill, 2022, the bill consisted of a total of 6 chapters and 30 sections which is less in number in comparison with the personal data protection bill 2021. The Bill is still pending as a draft and has not been presented before the parliament.

3.6.1 Key Features of the Bill:

1. ***Territorial application***- the Bill pertains to the handling of digital personal data within the geographical boundaries of India, encompassing data that is collected either online. It extends its applicability to the processing of personal data outside India, provided that such processing is intended for the purpose of offering goods or services or profiling individuals within India. The term "personal data" is defined as any information that pertains to an identifiable individual, while "processing" refers to the automated operations or set of operations that are performed on digital personal data, including but not limited to collection, storage, use, and sharing.
2. ***Consent-*** According to the bill, personal information can only be used for a legal reason if the person gives their permission. Before asking for permission, a notice must be given that includes details about the personal data that will be collected and why it will be used. It's important to remember that permission can be taken away at any time. But consent isn't always needed. This includes when processing is needed to carry out a legal duty, provide a service or benefit by the government, handle a medical emergency, find a job, or do other things in the public interest, like protect national security, stop fraud, or keep information safe. If a person is under 18 years old, their legal guardian must give permission.
3. ***Rights And Duties of Data Principal-*** The person whose data is being processed, called the "data principal," has certain rights when it comes to data processing. These include the right to know how their data is being used, the right to ask for corrections or deletions of their personal data, the right to choose someone else to use their rights if they die or become unable to, and the right to seek redress for a problem.

But data leaders also have responsibilities that they have to keep up with. These include not filing false or pointless complaints, giving fake information, hiding information, or pretending to be someone else in certain situations. If these responsibilities aren't met, you could be fined up to Rs 10,000.

4. ***Obligation of Data Fiduciaries***- In accordance with data protection regulations, the data fiduciary, who is responsible for determining the purpose and methods of data processing, is obligated to undertake certain measures. These measures include ensuring the accuracy and completeness of data through reasonable efforts, implementing reasonable security safeguards to prevent data breaches, and notifying the Data Protection Board of India and affected individuals in the event of a breach. Additionally, the data fiduciary must cease retaining personal data once the purpose has been fulfilled and retention is no longer necessary for legal or business purposes, as per the storage limitation requirement. It is important to note that this requirement does not apply to government entities engaged in data processing.
5. ***Transfer of personal data outside India***: - The Indian government will provide notification to countries where personal data may be transferred by a data fiduciary. Such transfers will be subject to specific terms and conditions as prescribed.
6. ***Exemptions*** – The Bill provides for certain exemptions wherein the rights of the data principal and the obligations of data fiduciaries, except for data security, will not be applicable. These exemptions are applicable in cases of prevention and investigation of offenses, as well as the enforcement of legal rights or claims. Additionally, the central government has the authority to exempt certain activities from the provisions of the Bill through notification. Such activities may include processing by government entities in the interest of the security of the state and public order, as well as research, archiving, or statistical purposes.
7. ***Data Protection Board of India*** – The Indian government has announced its intention to establish the Data Protection Board of India, which will be responsible for overseeing compliance with data protection regulations and imposing penalties for non-compliance. The Board will also have the power to tell data stewards what to do in case of a data breach and to listen to complaints from people who were affected. The government will decide who is on the Board, how they are chosen, what their terms of appointment and service are, and how they can be fired.
8. ***Penalties***- The Bill's timetable outlines the consequences for a range of offenses, including a maximum penalty of Rs 150 crore for non-compliance with child-related obligations and a maximum penalty of Rs 250 crore for failing to implement security measures to prevent data breaches and can exceed upto 500 crores. The Board will conduct an investigation before imposing penalties. This information is presented in a formal academic tone.

3.7. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

3.7.1 Introduction:

The **Digital Personal Data Protection (DPDP) Act of 2023** governs the handling of digital personal data within India's borders, whether it's gathered online or converted from offline sources. Additionally, it

extends its jurisdiction to the processing of digital personal data outside India if it pertains to offering products or services to individuals within India's jurisdiction.

3.7.2 KEY FEATURES OF ACT,2023:

i. **Applicability:** The Actl applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitised. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.

ii. **Consent:** Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. A notice must be given before seeking consent. The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Consent will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.

iii. **Rights and duties of data principal:** An individual whose data is being processed (data principal), will have the right to: (i) obtain information about processing, (ii) seek correction and erasure of personal data, (iii) nominate another person to exercise rights in the event of death or incapacity, and (iv) grievance redressal. Data principals will have certain duties. They must not: (i) register a false or frivolous complaint, and (ii) furnish any false particulars or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.

iv. **Obligations of data fiduciaries:** The entity determining the purpose and means of processing, (data fiduciary), must: (i) make reasonable efforts to ensure the accuracy and completeness of data, (ii) build reasonable security safeguards to prevent a data breach, (iii) inform the Data Protection Board of India and affected persons in the event of a breach, and (iv) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In case of government entities, storage limitation and the right of the data principal to erasure will not apply.

v. **Transfer of personal data outside India:** The Act allows transfer of personal data outside India, except to countries restricted by the central government through notification.

vi. **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of the Act. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.

vii. **Data Protection Board of India:** The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. Board members will be appointed for two years and will be eligible for re-appointment. The central government will prescribe details such as the number of members of the Board and the selection process. Appeals against the decisions of the Board will lie with TDSAT.

viii. **Penalties:** The schedule to the Bill specifies penalties for various offences such as up to: (i) Rs 200 crore for non-fulfilment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

3.7.3 CRITICAL ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Introduction:

The Digital Personal Data Protection Act of 2023 is a significant legislation designed to regulate personal data in India, marking the country's first comprehensive data protection law, after a previous attempt failed to materialize. This Act has the capacity to establish guidelines for both national and international entities engaged in data collection, its primary aim is to safeguard individuals' personal data by delineating their rights, duties, and the authorities responsible for ensuring compliance.

i. Scope And Applicability:

The Digital Data Protection Act of 2023 mandates that any entity, regardless of location, dealing with personal data of Indian citizens must comply with its regulations. "Personal data" is broadly defined to include any information identifying an individual, like name, address, contact details, biometrics, financial data, and sensitive information such as medical records, sexual orientation, and religious beliefs. This Act applies to all organizations handling personal data, including government agencies, for-profit, and non-profit entities. Its goal is to oversee the handling of personal data and ensure privacy protection. Notably, the Act extends its jurisdiction to cover organizations outside India processing data of Indian individuals, preventing evasion of its requirements. This extension strengthens the privacy rights of Indian citizens by regulating data processing activities irrespective of geographic location.

ii. Intersection of Consent Control:

The notion of consent typically aligns with the principles of autonomy and agency, whereas control tends to be linked with power dynamics and coercion. Nevertheless, there are numerous instances where consent and control overlap, leading to complex ethical quandaries.

The legislation emphasizes the critical nature of obtaining informed consent from individuals regarding the collection and management of their personal data. It requires entities to provide individuals with a clear and concise notice outlining the purpose and nature of the data being collected and processed. The legislation specifies that organizations, known as data fiduciaries, may only access such private data with the explicit or implicit consent of the individual, depending on the situation.

The legislation affirms individuals' entitlement to retract their consent at their discretion via a designated consent manager. Furthermore, organizations must promptly erase any gathered data upon

withdrawal of consent within a reasonable timeframe. The Act underscores the significance of individuals' autonomy in sharing personal data with entities, termed as "deemed consent," within the realm of data protection. This provision represents a pivotal step in fortifying individuals' privacy rights by enhancing their control over personal data.

The measures concerning consent and control as stipulated in the Act are in accordance with international standards for ensuring the privacy and security of data. The General Data Protection Regulation (GDPR), enacted by the European Union in 2018, underscores the significance of acquiring well-informed consent from individuals regarding the gathering and use of their personal information. Within the framework of the GDPR, individuals retain the right to retract their consent, necessitating companies to delete the data collected if consent is withdrawn.

iii. Data Localization:

Data localisation mandates that companies must store and handle data on servers situated within the borders of a specific country. Governments worldwide, motivated by worries regarding privacy, security, surveillance, and law enforcement, have been passing laws requiring data localisation. While a nation has the right to safeguard its interests and sovereignty, it should thoroughly assess the benefits and risks of storing data locally before making a definitive decision on an issue that could significantly impact various industries.

Data localization involves storing data within a specific geographic area, a practice gaining popularity due to concerns over data privacy and security. Previously, the Personal Data Protection (PDP) bill mandated data localization for transfers outside India, but the new draft bill lacks guidance on regulating Indian data abroad. Instead, it proposes notifying data fiduciaries of permissible data transfer destinations without details. This silence has sparked debate over whether most data should stay within India, potentially hindering the IT industry's growth. Compliance might require investing in new infrastructure, challenging for small enterprises. Supporters argue for protecting Indian citizens' privacy and preventing unauthorized data transfers abroad.

The study delves into the legal and ethical responsibilities of the data fiduciary, who is tasked with gathering, processing, and safeguarding individuals' personal data. It examines obligations such as the duty to inform, confidentiality, care, and rectification towards data subjects. Additionally, it scrutinizes the repercussions of failing to meet these obligations, including legal repercussions and damage to reputation. The research underscores the significance of data protection and the pivotal role of the data fiduciary in upholding the privacy and security of personal data. The legislation outlines specific duties for data management by the trustee, aimed at ensuring secure storage or deletion of processed data. These obligations are crafted to foster the safe and responsible handling of data.

Protecting personal data from unauthorized access, use, disclosure, destruction, or alteration relies on implementing security measures. These encompass various methods and procedures aimed at safeguarding sensitive information. Common security practices include encryption, access restrictions, firewalls, antivirus software, and regular backups. These measures help mitigate cyber threats and ensure data confidentiality, integrity, and availability. Legislation proposes establishing a framework for safeguarding personal data by requiring data fiduciaries to implement appropriate security measures and imposing penalties for inadequate

protection. In case of a breach, both the data fiduciary and processor must notify the Board and affected data principals promptly, regardless of the breach's cause. This provision ensures transparency and allows affected individuals to take necessary remedial actions promptly to prevent further incidents. The temporal aspect of the Act, however, lacks a specific timeline for notifying data principals and the board about breaches.

iv. Right to be Forgotten:

In the digital world, with a specific focus on the Digital Data Protection Act of 2023. The aforementioned Act has a clause that mandates companies to delete personal data once it is no longer necessary for the purpose for which it was collected. the inclusion of the Right to be Forgotten clause in the Digital Data Protection Act of 2023 is a significant step towards safeguarding the privacy of individuals in the digital world. The aforementioned statement suggests that it is imperative for data fiduciaries to refrain from retaining personal data for a period longer than what is deemed necessary. The measure under consideration provides data principals with the right to revoke their consent to the collection and processing of their personal data. The importance of entities deleting personal data when it is no longer necessary is emphasized. The right to deletion is a crucial aspect of data protection and privacy, as it empowers individuals with control over their personal data. This right is considered fundamental in nature, as it allows individuals to request the removal of their personal data from various sources. By exercising this right, individuals can safeguard their privacy and prevent the misuse of their personal information. The implementation of data retention policies ensures that companies do not retain personal data for an indefinite period, thereby mitigating potential risks to individuals' privacy and security. The clause that requires the deletion of individuals' personal data represents a significant stride towards prioritising the privacy of the general public. In order to comply with data protection regulations, it is imperative for entities to establish and implement suitable processes and systems to effectively erase personal data once it is no longer necessary. This is crucial to safeguard the privacy and security of individuals' personal information. Failure to do so may result in legal and financial consequences for the entity. Therefore, it is essential for entities to prioritise the development and implementation of effective data erasure procedures. This rule highlights the importance of conducting regular reviews of personal data and its processing purposes within organisations to prevent indefinite retention of personal data.

v. The Appointment of a Data Protection Officer (Dpo):

The appointment of a Data Protection Officer (DPO) Under the Digital Data Protection Act of 2023, all businesses involved in collecting and processing personal data are required to appoint a Data Protection Officer (DPO). This individual is tasked with overseeing data protection practices and addressing concerns raised by data subjects, who are individuals whose personal data is processed. However, the legislation lacks a clear timeframe for the DPO to respond to inquiries and concerns, granting organizations flexibility in determining response times. Therefore, it is crucial for organizations to establish procedures ensuring the DPO can promptly and effectively address data subject inquiries and concerns.

vi. Right to Information Is a Fundamental Right Of The Data Principal:

The Right to Information ensures that individuals, known as "data principals," receive comprehensive information from data controllers regarding the handling of their personal data. It mandates that data

controllers provide clear and concise details about the purpose, types, and recipients of personal data processing. Additionally, individuals have the right to be informed about their data protection rights and how to assert them. This right fosters transparency and accountability in data processing, empowering individuals to monitor and regulate the usage of their personal information. It is a fundamental safeguard enabling individuals to take proactive steps to protect their privacy and data security.

vii. The Absence of a Specified Timeline:

The absence of a specified timeline for the Data Protection Officer (DPO) to respond to inquiries and apprehensions raised by data subjects is a notable limitation of the Bill. The aforementioned statement implies that entities possess a significant degree of discretion in determining the appropriate timing for their response to data.

viii. The Mechanism for Resolving Concerns Or Grievances:

The mechanism for addressing concerns or grievances regarding data privacy enables individuals to seek resolution for issues related to their personal information. If a data subject encounters problems with how their data is managed, they are advised to first contact the data fiduciary, typically the Data Protection Officer (DPO) overseeing the relevant data. If the response is unsatisfactory or if there's no response within seven days, the data subject can escalate the matter by filing a complaint with the Board. It's important to note that the data subject is responsible for initiating this process. To ensure the validity of the complaint, individuals must provide accurate information without relying on false or misleading data, and essential facts should not be omitted.

The legislation, akin to the previous Personal Data Protection Bill, provides individuals with the entitlement to demand rectification or erasure of their personal information. In the event that a correction is requested, it is the responsibility of the data fiduciary who is in charge of the data to effect the required modifications. In the event that a request for removal and deletion is submitted, it is expected that the organisation will proceed to eliminate any personal data that is deemed unnecessary unless there exists a legal obligation to retain such data.

The Legislation outlines that the data principal has the ability to file a complaint with the data fiduciary, who is designated as the Data Protection Officer if they are dissatisfied with the resolution or lack thereof within the specified timeframe. This mechanism allows for a means of recourse for data principals who feel their rights have been violated.

ix. The Establishment of a Data Protection Authority/ Board

The establishment of a Data Protection Authority/ Board is a crucial step towards ensuring the protection of personal data. This body is responsible for overseeing the implementation and enforcement of data protection laws and regulations. The formation of such an authority is necessary to ensure that individuals' privacy rights are respected and that their personal data is not misused. The Data Protection Authority/ Board plays a vital role in safeguarding sensitive information, such as medical records, financial data, and other personal information. Its establishment is a significant step towards creating a secure and trustworthy digital environment for individuals and businesses alike.

The legislation aims to create a regulatory framework for data protection by establishing a Data Protection Authority as an autonomous entity tasked with enforcing the provisions of the bill. The authority would be responsible for ensuring compliance with the regulations and safeguarding the privacy of individuals' personal data. The establishment of a Data Protection Authority is a crucial measure towards ensuring the effective implementation of the Act provisions. This authority will be empowered to investigate and penalised entities for non-compliance with the Act, which may include imposing fines and penalties, as well as suspending or revoking licences of the entities. This provision is expected to enhance compliance with the bill and promote the protection of data privacy. As per the provisions of the Act, the Board shall be equipped with an electronic filing and document management system, in addition to an electronic court system. The powers of the Board shall be derived from the Code of Civil Procedure, 1908. The Legislation lacks information regarding the composition and potency of the Data Protection Board. It is assumed that such details will be furnished in the Rules at a later stage. The board's investigative powers are limited to acting solely on customer complaints, as it does not possess any Suo moto powers to initiate investigations on its own accord. The proposed policy will confer the Board with the authority to levy sanctions across six primary categories, with the highest possible penalty amounting to ₹250 crores.

3.7.4 SHORTCOMINGS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023:

India's long-awaited Digital Personal Data Protection Act 2023 (DPDP) fails to meet expectations, despite the country's urgent need for robust data protection laws. The Act's vague language and open-ended clauses leave room for misinterpretation, while also raising significant concerns. This is particularly disappointing given the alarming rise in cyberattack, data breaches, and frauds, which had created a sense of urgency for a comprehensive data protection framework. Instead, the DPDP's shortcomings may perpetuate the limited accountability of data handlers and fail to provide adequate safeguards for individuals' personal data.

1. No Timeline to Report Breach:

The Digital Personal Data Protection Act 2023's lack of a timeline to report a breach is a significant concern, as it:

a) Delays notification to affected individuals, potentially exacerbating harm;
b) Leads to inconsistent reporting practices, making tracking and analysis challenging;
c) Undermines accountability, as data fiduciaries may not be held responsible for timely notification;
d) Deviates from global standards, such as the GDPR's 72-hour notification requirement;
e) Hinders prompt remediation, potentially leading to prolonged data exposure;
f) Erodes trust in organizations and the government's ability to protect personal data;
g) Limits public awareness of data breaches, increasing vulnerability; and
h) Undermines the Act's effectiveness in safeguarding personal data.

2. Broad Exemptions for Government:

The Act provides broad exemptions for the government regarding data collection and processing. Critics argue that this could lead to potential misuse and a lack of accountability, as government agencies might not be held to the same stringent standards as private entities.

3. **Lack of Independent Oversight:**

The Data Protection Board of India, which is responsible for enforcing the Act, is appointed by the government. This raises concerns about its independence and impartiality in overseeing data protection regulations, especially in cases involving government agencies.

4. **Ambiguity and Vague Provisions:**

Some provisions in the Act are seen as vague or ambiguous, which could lead to varying interpretations and implementation challenges. This lack of clarity might hinder effective enforcement and compliance.

5. **Limited Rights for Data Principals:**

While the Act grants certain rights to individuals (referred to as Data Principals), such as the right to access and correct their data, it is criticized for not going far enough in empowering individuals. For instance, there is limited provision for data portability or the right to be forgotten.

6. **Consent Mechanism:**

The consent mechanism outlined in the Act is criticized for being weak. There are concerns that the manner in which consent is obtained may not be robust enough to ensure that individuals are making fully informed decisions about their data.

7. **Data Localization Requirements:**

The Act includes provisions for data localization, requiring certain types of data to be stored within India. This has been criticized by some as potentially harmful to global businesses and innovation, as it could increase operational costs and complicate international data flows.

8. **Impact on Startups and Small Businesses:**

Compliance with the Act's requirements might be challenging for startups and small businesses due to the potentially high costs and resource demands involved in ensuring data protection and privacy standards.

9. **Insufficient Focus on Non-Personal Data:**

The Act primarily focuses on personal data, with limited attention given to non-personal data, which can also have significant privacy implications when aggregated or processed in certain ways.

10. **Potential for Overreach:**

There are concerns that the powers granted to the government under the Act, particularly regarding data interception and monitoring, could be used excessively or inappropriately, leading to privacy violations.

11. **Cross-Border Data Transfers:**

The rules regarding cross-border data transfers are seen as restrictive and could impact international business operations and collaborations. The need for approvals and compliance with specific conditions could slow down business processes and innovation.

While the Digital Personal Data Protection Act, 2023, is a step in the right direction for data privacy in India, addressing these shortcomings will be crucial for it to effectively protect individuals' data while fostering a conducive environment for business and innovation.

CHAPTER IV

EUROPEAN UNION (GENERAL DATA PROTECTION REGULATION) AND UNITED STATES LEGISLATIVE FRAMEWORK ON DATA PROTECTION (CALIFORNIA CONSUMER PRIVACY ACT).

IV. European Union

The roots of data protection legislation within the European Union (EU) run deep, stretching back to the 1980s. In 1995, the European Union (EU) responded by establishing regulations through its Data Protection Directive. The 1995 Data Protection Directive was replaced by the GDPR, which aims to improve individual privacy rights while harmonizing data protection laws throughout the EU . The General Data Protection Regulation (GDPR), which was adopted in 2016 and took effect in May 2018, is the main legislative framework for data protection law in the European Union. Any information pertaining to an identified or recognizable natural person is referred to as personal data under the GDPR. The evolution of GDPR can be understood through the timeline given below:

- Universal Declaration of Human Rights 1948 validating Right to Privacy OECD Guideline of
- Privacy and Trans-Border Flows of Personal Data passed in 1980
- Guidelines for Regulation of Computerized Personal Data Files adopted by the United Nations General Assembly in 1990
- Treaty of Lisbon and Charter of Fundamental Rights (Art 7 & 8) Data Protection Directive (1995/46/EC),
- Directive on E-Privacy (2002/58/EC) and
- The Directive on Data Retention (2006/24/EC) was adopted Adoption of [94]
- The General Data Protection Regulation (REGULATION (EU) 2016/679) in 2016

The processing of personal data is governed by seven fundamental principles under the GDPR. These ideas include:

[94] *"Data Protection Directive (1995/46/EC)" - European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046*

a) ***Lawfulness, fairness, and transparency***: Personal data must be handled fairly, legally, and openly.

b) ***Limitation on use***: Personal information must only be gathered for clear, explicit, and legal purposes. It may not then be used in any way that is incompatible with those purposes.

c) ***Data minimization***: Personal information must be sufficient, pertinent, and kept to a minimum necessary for the purposes for which it is processed.

d) ***Accuracy:*** Personal information must be true and, if necessary, kept current.

e) ***Limitation on storage***: Personal data may only be kept in a form that makes it possible to identify data subjects for as long as is required to fulfill the processing purposes.

f) ***Integrity and confidentiality:*** Personal data processing must be done in a way that provides the necessary security, including defense against unauthorized or unlawful processing as well as against unintentional loss, destruction, or damage.

g) ***Accountability:*** The data controller is accountable for adhering to the aforementioned guidelines and must be able to prove it.

These minimum standards included guidelines on fair processing, purpose limitations, and security measures aimed at protecting individual rights regarding data usage across all EU states. However, with rapid technological advances and increasing globalization came new issues related to cross-border transfers of personal information along with novel forms of online tracking prompting inadequacies in these laws.

Thus, arose General Data Protection Regulation (GDPR), which was introduced as a new legislative framework designed to address emerging concerns. The GDPR took effect on May 25th, 2018; it replaced the outdated Data Protection Directive while incorporating its principles. The main goal behind this regulation is to enhance transparency during data collection processes by giving users more control over their personally identifiable details. Notable characteristics outlined under GDPR include explicit user consent before harvesting or handling any sensitive information; specific rules around pseudonymization or anonymization when applicable; mandatory reporting within seventy-two hours post-discovery in case there's an unauthorized breach compromising valuable customer's confidentiality[95]. GDPR developed out of increased worries concerning privacy violations resulting from unchecked acquisition & exploitation of users' identifiable features by companies operating within Europe's domain. concerns head-on through implementing measures geared towards guaranteeing confidentiality & protection against any potential abuse thereof - thereby promoting ethical treatment towards internet users worldwide.

The European Union's legislative framework for data protection has evolved significantly with time, designed to protect individual privacy and ensure responsible handling of personal data in the digital age.[96] Numerous authors have highlighted this fact, including the European Data Protection Supervisor (2018), and an unknown author (2018). Back in the 1980s, The EU initially addressed individuals' concerns about protecting their rights to personal information. However, various updates and amendments have since been

[95] ***European Data Protection Supervisor, Handbook on European Data Protection Law (2018), https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.***

[96] ***Law Library of Congress, Global Legal Research Directorate, 6 Children's Online Privacy and Data Protection in Selected European Countries, LL File No. 2021-020137 LRA-D-PUB-002361 (2021), https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf.***

made which led to a more all-encompassing approach towards safeguarding data privacy. One crucial aspect of The EU's legislative framework is its emphasis on granting access to personal information by individuals. Granting such access confirms if one's personal data is being processed while providing information on any processing techniques employed alongside associated subject rights available (European Data Protection Supervisor, 2018). Another essential point worth noting regarding The EU legislation for data protection regards how organizations handle sensitive private information: organizations are legally mandated only-ever use user-generated content for specified purposes- a move that increases transparency in digital operations undertaken within Europe as stated by an unknown author(2018) Additionally, the General Data Protection Regulation(GDPR) of the European Union came into effect on May 25th ,2018 replacing previous regulations written before smartphones or social media existed . GDPR expanded upon existing principles entrenched within earlier directives introducing new concepts like 'accountability' meaning companies must demonstrate compliance with regulations rather than just complying[97]. In despite numerous modifications over time aimed at ensuring responsible handling of personal data and safeguarding individual privacy due largely owing mainly due large amounts legal jargon utilized throughout -the fundamental aim remains clear: protecting citizens' privacy rights in the digital age highlighted through features such as accessing one's own personal information and strict regulation guiding usage of user-generated content (European Data Protection Supervisor, 2018;

GDPR has evolved significantly to keep up with emerging challenges. Convention 108, adopted by the Council of Europe in 1981, was among the first international legal instruments to address privacy and personal data protection issues. This landmark convention established essential principles related to individual rights like transparency, purpose limitation, and proportionality. The General Data Protection Regulation (GDPR) is a key component of this legislative framework aimed at ensuring uniformity in data protection across EU member states. Since its inception in May 2018, GDPR empowers individuals with greater control over their personal information while imposing clear obligations on organizations that collect or process such data[98]. Valid consent from individuals before processing their personal information is one important aspect of achieving GDPR compliance. Furthermore, companies are mandated to appoint a Data Protection Officer responsible for overseeing compliance with these regulations. Comprehensive analysis shows that implementing GDPR may increase costs associated with regulatory compliance for businesses operating within Europe and globally; however, it could lead to safer handling practices when dealing with sensitive information. Future research should examine how emerging technologies like artificial intelligence impact compliance with GDPR guidelines or how these regulations affect small enterprises differently from larger corporations. Moreover, researchers can evaluate if strict enforcement measures have any unintended consequences or assess whether alternative approaches could yield similar results at lower costs. In conclusion, as technology advances rapidly worldwide every day bringing forth new risks and opportunities alike- The EU's legislative framework safeguards individual privacy rights while promoting responsible

[97] ***Hustinx, P., EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*** ***https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf.***

[98] ***The new EU Regulation on the protection of personal data: what does it mean for patients? A guide for patients and patients' organisations (n.d.), Unknown publisher, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf.***

handling practices concerning data protection - irrespective race color or geographic location thus benefitting policymakers everywhere seeking solutions relevant worldwide of rights to individuals, including the right to be informed about how their data is being processed, the right to access their personal data, the right to rectify any inaccuracies in their data, the right to erasure or "the right to be forgotten," the right to restrict processing, the right to data portability, and the right to object. These rights empower individuals to take control of their GDPR grants people a number of rights, such as the right to information, the right of access, the right of rectification, the right of erasure, the right to restrict processing, the right to data portability, and the right to object. The protection of personal data is a fundamental right that has been recognized by various international and national laws. Personal data refers to any information relating to an identified or identifiable natural person. The General Data Protection Regulation (GDPR) provides a range personal information and ensure that it is being handled in a responsible and transparent manner. Organizations that process personal data must adhere to these rights and take appropriate measures to protect individuals' privacy. Failure to comply with GDPR can result in significant fines and reputational damage for organizations. Therefore, it is crucial for organizations to prioritize privacy and ensure that they are compliant with GDPR regulations.

Additionally, the GDPR places a number of requirements on data controllers and processors, such as the need to obtain legal consent, put in place suitable organizational and technical safeguards to protect the security of personal data, and notify the appropriate authorities of data breaches within 72 hours. The GDPR also establishes the European Data Protection Board (EDPB), which is responsible for providing guidance and promoting the consistent application of data protection laws across the EU. Moreover, the GDPR has extraterritorial scope, meaning that it applies to any organization that processes the personal data of EU residents, regardless of where the organization is located. This has led to a significant shift in the global data protection landscape, with many countries adopting similar laws to ensure that their data protection standards are on par with the GDPR. Furthermore, the GDPR has an extraterritorial application, which means that it covers all organizations, regardless of location, that process the personal data of EU citizens. With many nations passing comparable laws to ensure that their data protection standards are on par with the GDPR, this has caused a significant shift in the landscape of global data protection. The privacy Regulation, which aims to improve the protection of privacy in electronic communications, is one of many supplemental regulations that have been introduced in the EU as a result of the GDPR. The GDPR has made some significant changes, one of which is giving data protection authorities more authority to enforce existing laws (DPAs). In accordance with the GDPR, DPAs have the authority to impose fines of up to 4% of a company's global annual revenue or €20 million, whichever is greater. Since the GDPR was implemented, there have been a number of high-profile instances of organizations receiving fines for breaking the law. For instance, the UK's Information Commissioner's Office (ICO) fined British Airways £183 million ($229 million) in 2019 for a data breach that happened in 2018, and the French DPA fined Marriott International €20 million in 2020 for a data breach that affected millions of customers.

The GDPR has already undergone evaluation and development. The Data Governance Act, which the European Commission proposed in June 2021, aims to create a uniform EU framework for the sharing, accessing, and reuse of data. This law aims to make data sharing easier while protecting personal information

and upholding privacy. The need to create a new legal framework that addresses the difficulties of the digital economy, such as the emergence of artificial intelligence (AI) and the Internet of Things, has also been discussed (IoT). A new regulatory framework that addresses the specific risks associated with AI, such as bias and discrimination, may be required, according to the European Commission's White Paper on AI, which was published in 2020.A recent study by the European Data Protection Supervisor (EDPS) found that while the GDPR has had a positive impact on data protection, there are still areas that need improvement. For instance, the study highlighted the need for more effective enforcement and the need to address the challenges posed by new technologies. The advancements in technologies have brought about new challenges in data protection, and the GDPR has only partially addressed them. The EDPS study highlights the need for stronger enforcement of the emphasized to ensure that companies comply with the rules. This can be achieved through increased monitoring and imposing harsher penalties on violators. Additionally, new technologies such as artificial intelligence and blockchain pose unique challenges to data protection, and there is a need for more research to understand their implications fully. Furthermore, there is a need for increased transparency in data processing, particularly when it comes to automated decision-making systems. In conclusion, while the GDPR has made significant strides in improving data protection, there is still work to be done to keep up with the ever-evolving technological landscape. Although the GDPR has improved data protection, there are still some areas that require improvement, according to a recent study by the European Data Protection Supervisor (EDPS). For instance, the study emphasized the necessity of stronger enforcement and the need to deal with the difficulties brought on by new technologies[99].

4.2 UNITED STATES:

The American legal system has seen major changes throughout history, particularly when it comes to data protection. Today's digital era makes privacy and security more important than ever and the United States data protection governs with the Buch of data protection law which covers a different set of subject matter from Insurance, computers, and children's privacy to the protection of sensitive personal health data every aspect of privacy is dealt with under different laws. At the federal level, the US has the following laws for the data protection

- Privacy Act, 1974
- Rights to Financial Privacy Act, 1978
- Electronic Communications Privacy Act, 1986
- Privacy Protection Act, 1980
- Computer Matching and Privacy Protection Act, 1988
- Electronic Communications Privacy Act, 1986; Cable
- Communications Policy Act of 1984
- Computer Security Act, 1987
- Video Privacy Protection Act, 1988

[99] ***General Data Protection Regulation (REGULATION (EU) 2016/679)" - European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*** ***https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679***

- Driver‘s Privacy Protection Act of 1994
- Children‘s Online Privacy Act, 1998
- Health Insurance Portability and Accountability Act of 1996.

One of the early attempts at legislation to regulate the gathering, use, and dissemination of personal information by federal agencies was the Privacy Act of 1974. As a result, before using or releasing personal data, businesses in possession of the data must confirm its accuracy, relevance, timeliness, and completeness. This law, however, only applied to governmental organizations. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) in response to concerns about the privacy rights of electronic communications as computers were more widely used than ever. One objective of this act was to expand protections from unauthorized interception and disclosure beyond the typical eavesdropping operations carried out by law enforcement personnel. General Data Protection Regulation, which regulates corporations collecting user demographics on EU individuals regardless of whether they are physically based within EU boundaries or not, was recently adopted into US law. Studies show significant gaps between what is legally required and actual practices regarding the handling of private online information, despite multiple attempts to enact regulations that protect private online information. In order to determine whether additional action in this area is necessary moving forward, this essay will examine the key provisions of each of these acts and evaluate their effectiveness in light of recent trends in consumer attitudes towards online privacy issues and rates of cybercrime.

The US legislative framework governing data protection and cybersecurity has undergone considerable modifications throughout time. Protecting people's right to privacy is a major goal of important laws including The Privacy Act of 1974, the Electronic Communications Privacy Act, and most recently, the General Data Protection Regulation (GDPR). Despite growing interest in data privacy, these legal frameworks continue to be complicated and inconsistent at the federal level.

1) **The Health Insurance Portability and Accountability Act (HIPAA) 1996**- [100]

Is applicable to all entities that fall under the category of Covered entities. These entities are responsible for collecting, maintaining, using, or disclosing personal health information[101]. The term "Covered Entity" refers to entities that fall under one of three categories: (1) health plans, (2) health care clearing houses, or (3) health care providers. These entities are considered Covered Entities if they transmit any health information in electronic form in connection with a transaction that is covered by the law.[102] The Health Insurance Portability and Accountability Act (HIPAA) mandates that Covered Entities adhere to the Privacy and Security Rules. The Privacy Rule mandates that Covered Entities are restricted from utilising or revealing Protected Health Information, except in specific situations or with the explicit consent of the patient or participant. The Security Rule mandates that Covered Entities maintain the confidentiality, integrity, and

[100] *42 U.S.C. §1301 et seq.)*

[101] *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf, accessed on 20/04/2023, , Id. at § 160.102.*

[102] *Id. at 160.104.*

availability of electronic Protected Health Information through the implementation of appropriate administrative, physical, and technical safeguards[103].

The legislation provides for the safeguarding of health-related data, including both protected health information (PHI) and electronic protected health information (e-PHI). The Health Insurance Portability and Accountability Act (HIPAA) serves to safeguard Protected Health Information (PHI). However, electronic Protected Health Information (e-PHI) is subject to supplementary requirements.

The term 'Protected health information refers to health information that can be identified individually:The definition of electronic records, with the exception outlined in paragraph (2), pertains to records that are transmitted or maintained through electronic media or any other form or medium.[104]

The Security Rule is a crucial regulation that outlines the fundamental requirements for healthcare entities and contractors. It mandates that all data processors must implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of information. Additionally, the rule requires data processors to report any security incidents that may occur. These measures are essential to safeguard sensitive healthcare information and prevent unauthorised access or disclosure.

2) Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003:

(CAN-SPAM Act) The Act in question governs the collection and utilization of email addresses. This research paper encompasses all commercial messages as defined by legislation, which refers to any electronic mail message that primarily aims to advertise or promote a commercial product or service. This includes emails that promote materials on commercial websites[105]. The use of commercial email has become a common practice in modern business communication. However, it is important to ensure that such emails are not deceptive and provide certain information to recipients. This includes the sender's identity and subject matter, as well as opt-out provisions for those who do not wish to receive further emails. Additionally, the sender's address must be included and the email must be clearly and conspicuously identified as an advertisement or solicitation. The Email Privacy Act enforces legal consequences on individuals who engage in the unauthorized collection of email addresses, whether through harvesting or dictionary attacks. Such actions are deemed criminal and subject to penalties under the Act.[106]

The CAN-SPAM Act mandates that all types of organizations, including 501(c)(3) organizations, must refrain from sending emails that contain materially false, misleading, or deceptive information in the header or subject line. This legal requirement aims to prevent the dissemination of fraudulent or misleading information through email communication. In accordance with advertising and solicitation regulations, emails must be clearly identified as such if they fall under these categories.

---

[103] ***Id. at 164.302-.318.***

[104] ***Individually identifiable health information includes demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual orfor which there is a reasonable basis to believe can be used to identify the individual. See 45 CFR 160.103.***

[105] ***15 USC §7702, http://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSCprelimtitle15section7702&f=treesort&fq=true&num=0&saved=%7CY2FuIHNwYW0gYWN0%7CdHJlZXNvcnQ%3D%7CdHJ1ZQ%3D%3D%7C0%7Ctrue%7Cprelim***

[106] ***Id. at §§ 7704(a)(1)-(2).***

3) The Fair Credit Reporting Act FCR 1976A[107]

The definition of "consumer reports" as provided by the Fair Credit Reporting Act (FCRA). According to the FCRA, consumer reports refer to any communication disseminated by a consumer reporting agency (CRA) that pertains to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation. The primary purpose of these reports is to assess a consumer's eligibility for credit or insurance. The delves into the various components of consumer reports and their significance in evaluating a consumer's creditworthiness. The Consumer Reporting Agency (CRA) is required to adhere to rational procedures to ensure the precision of the data. [108]In cases where data is deemed inaccurate, incomplete, or unverifiable, it is the responsibility of the Credit Reporting Agency (CRA) to promptly rectify the data in question. This is in accordance with the guidelines set forth by regulatory bodies governing the operations of CRAs.

4) **Electronic Communications Privacy Act, 1986**-

The act of wiretapping communications of individuals without prior consent or court approval is prohibited. The prohibition of the use or disclosure of any information obtained through illegal wiretapping or electronic eavesdropping is a crucial aspect of privacy protection. Such activities are considered unlawful and unethical, and therefore, any information obtained through these means cannot be used or disclosed in any form. This principle is fundamental in safeguarding the privacy rights of individuals and ensuring that their personal information is not misused or exploited. The prohibition of the use or disclosure of illegally obtained information is a critical element of legal frameworks that seek to protect the privacy and prevent unauthorized access to personal data.

5) **The Computer Fraud and Abuse Act of 1986-**

The legislation aimed at preventing and penalising activities related to hacking, which are defined as "unauthorised access" to computers that are protected. The Act seeks to deter individuals from engaging in such activities by imposing legal consequences.202 The Act prohibits individuals or entities from surpassing the boundaries of their "authorised access."203. The term "protected computers" encompasses a variety of computer systems, including those utilised by financial institutions, the United States government, and computers that are involved in or have an impact on interstate or foreign commerce or communication.204. The definition of "damage" as stated in the Act encompasses any form of impairment that affects the integrity or availability of data, a programme, a system, or information.

6) **Family Education Rights and Privacy Act, 1974-**

The Family Educational Rights and Privacy Act (FERPA) is a federal law that safeguards the information contained within students' educational records. It is applicable to all educational agencies and institutions that receive funding from the U.S. Department of Education, including non-profit organisations. FERPA ensures that the privacy of student's educational records is protected.207 The present law defines "educational records" as any records, files, documents, or other materials that pertain to a student and are kept by an educational agency or institution, or by an individual acting on behalf of such agency or

[107] *20 USC § 1232g*

[108] *15 U.S.C. § 1681e (2013).*

institution.208The term "educational agency or institution" refers to a public or private entity that receives funding through a government programme. This definition encompasses a wide range of organisations that provide educational services.209

7) **The Family Educational Rights and Privacy Act (FERPA[109])**

The Act mandates that educational institutions that receive government funding are obligated to provide parents or students who are over the age of eighteen with the privilege to examine and scrutinise the academic records of the students. The establishment of procedures for granting requests made by individuals to educational agencies or institutions is a directive that must be adhered to within a reasonable time frame, not exceeding forty-five days from the date of the request.210 The Family Educational Rights and Privacy Act (FERPA) requires educational institutions to obtain written consent from eligible students, parents, or guardians before disclosing personally identifiable information or education records to any individual, agency, or organization, except for a list of specifically excluded individuals and related state agencies or officials.

8) The Children's Online Privacy Protection Act (COPAA) 2000- [110]

The Act was enacted to provide protection to minors under the age of thirteen who utilise the Internet. Its primary objective is to regulate the manner in which websites collect, utilize, and disclose personal information pertaining to these minors. [111]According to the Children's Online Privacy Protection Act (COPPA), it is mandatory for a website's "operator" to disclose its data collection policies to the parent of a child and obtain parental consent prior to collecting any information. 215 The Children's Online Privacy Protection Act (COPPA) is a federal law that applies to websites that collect personal information from children. If the website operator has knowledge that the website is collecting personal information from children, COPPA applies to both children's websites and "general audience" websites.

9) **The California Consumer Privacy Act CCPA- 2020:**

The implementation of the California Consumer Privacy Act (CCPA) is a noteworthy privacy development in the United States. The CCPA has been compared to the General Data Protection Regulation (GDPR) and has been referred to as "California's GDPR" by some critics. The California Consumer Privacy Act (CCPA) is exerting a significant impact on businesses worldwide, owing to California's vast size and its status as the birthplace of Silicon Valley. Companies across the United States and beyond are currently evaluating the implications of this legislation for their operations.

The California Consumer Privacy Act (CCPA) was implemented on January 1, 2020, and swiftly established itself as the most comprehensive privacy and data protection legislation in the United States. The California Consumer Privacy Act (CCPA) is applicable to for-profit entities that engage in business activities within the state of California. Such entities are required to collect or determine how personal information is processed and must fall within one of three size categories as specified by the CCPA. The California

[109] 1974

[110] **15 U.S.C. §§ 6501, et seq,**

[111] **Robert Hasty Et.al, Data Protection Law In USA, Advocates for International Development, https://www.neighborhoodindicators.org/sites/default/files/coursematerials/A4ID_DataProtectionLaw%20.pdf**

Consumer Privacy Act (CCPA) enforces rigorous requirements for businesses that collect personal information from individuals residing in California, mandating the disclosure of privacy policies. The California Consumer Privacy Act mandates that businesses provide California residents with the right to access and delete their personal information, as well as the right to opt out of the sale of their personal information to third parties.

The regulation prohibits companies from selling the personal data of minors who are under the age of 16 without obtaining their explicit consent. The California Consumer Privacy Act (CCPA) establishes a legal entitlement for individuals to bring a lawsuit against a company in the event of specific data breaches resulting from the company's failure to adhere to and uphold acceptable security protocols and procedures. The California Consumer Privacy Act (CCPA) grants the California Attorney General the power to enforce the CCPA's provisions. Violations of the CCPA may result in statutory fines of up to $7,500 per infringement. The recently proposed amendment in COPA will amend the CCPA.

CHAPTER V

V. COMPARATIVE APPROACH:

Introduction

In order to understand India's approach to data protection, it would be helpful to look at the practices used in other areas, with a particular emphasis on more recent frameworks that have been established. Two distinct paradigms regarding data protection are discernible from an analysis of international legal systems. While the American market system depends on industry-specific data protection laws, the European Union and other organizations that implement a similar framework provide comprehensive data protection legislation based on the principles of rights. The reason for this disparity can be traced to the distinct theoretical foundation that each legal jurisdiction places on the concept of privacy.[112] The two approaches towards data protection are discussed briefly below with the help of table:

5.2 European Union GDPR 2018 and the Recently Proposed Digital Personal Data Protection Bill, 2022 of India:

Basis of Comparison	EUROPEAN UNION	INDIA
Introduction	Regards the Several law for Data protection in the EU, GDPR is the most important regulation which has a huge impact in terms	India does not have comprehensive data protection law, but the Recently Prosped Digital Data Protection Bill, 2022

[112] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

	of data protection. It was proposed in 2016 and adopted on the 25th of May 2018.	is a set of regulations for data protection, The Proposed legislation has 6 chapters and a total of 30 sections deals with the collection, regulation, storage, rights, duties, exemption, and penalty.
Territorial Scope	Applicable on entities Established in the EU but data processing may or may not take place in the European Union. Not instituted in the European Union but processing personal data mostly related to the offering of goods or services of data subjects present in the EU. Instituted at a place beyond EU where member state law applies on account of Public International Law	Applicable on Processing of personal data within India. The processing of digital personal data outside the territory of India. Not applicable on- offline personal data, non-automated data Personal dat is processed by individuals for personal and domestic purposes and contained recor existence for 100 years.[113]
Subject matter scope	Personal information, so long as it isn't being processed by organizations like law enforcement or the national security apparatus, or by individuals for domestic or personal use. Anonymous data is beyond the scope of GDPR.	Personal information collected by the entities.
Definition of Data	GDPR Covers the Definition of Data in an exhaustive form not only personal data but also include senstitive personal data. It defines Personal Data as the information relating to an identified natural person, identified by name, identification	The Act covered the definition of Personal data as - any data about an individual who is identifiable by or in relation to such data , this defition is complex to define.

[113] Section 2 & 3 of The Digital Personal Data Protecion Act, 2023

	number, location data and online identifier, and specific factor to physical, physical, genetic, mental, economic, cultural or social identity.[114]	
Grounds for the Process of Data	• Processing of data on obtaining consent from the data subject. • Processing of data for the performance of a contract • Processing of data for legitimate interests and vital interests of the data subject or any natural person. • Processing of data for compliance with a legal obligation. • Processing of data for life interest. • Processing of data in the public interest	The Act Processing of data for the lawful purpose and which is not forbidden by law[115]
Authorities for data process and data collection.	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	The Act provided the three authorise responsible for data collection and processing • Data fiduciary • Significant Data Fiduciary • Data processor
Cross-border data	The GDPR mentions the exhaustive procedure, code of conduct, certificate mechanism, and rules for the cross-border flow of data and the strength of data collected in the country's local servers,	DPDP Act, 2023 include the provision of cross-border data flow, where the entities require permission to use data.

[114] Section 4 (1) of GDPR
[115] Section 4 of The Digital Personal Data Protection Act, 2023

	which means Data Localisation.	
Children's data	GDPR has a wider scope with special categories in terms of the process of children's personal data, the valid consent age for processing of data ranges from 13 to 16 years, and the responsibility levied on the entity for taking consent of the parents.[116]	DPDP Act, Consisted the 18 years as the valid age for the data processing and parent are permissible to grant consent on children's behalf
Data Principal Rights	The GDPR recognized the following rights: • Right to correction • Right to erase • Right to access • Right to restrict on processing • Right to data portability • Right to be forgotten • Right to object[117]	The DPDP Act, 2023 Recognise the following rights, • Right to information about personal data • Right to correction and erasure of personal data • Right to grievance redressal • Right to Nominate in case of death and incapacity to exercise other rights[118]
Data Fiduciary Duties	The GDPR defines Data Fiduciary as (Data controller) personal data has to comply with the following requirements and limitations under GDPR: • Specific purposes • limitation on collection	General Obligations • Compliance with the act • Made reasonable effort to ensure data protecion • Implement appropriate technical and organization

[116] *Article 8, Conditions applicable to child's consent in relation to information society services, GDPR*
[117] *Chapter 3, Rights of Data Subject, GDPR,*
[118] Chapter 3, of the Digial Personal Data Protecion Act, 2023

	• Limitation on storage of personal data. However certain grounds have been mentioned that allow sthe storage of personal data for a longer period. • Fair, legal, and open processing of personal data are required. • Personal data must be secured, it must be guaranteed. • Prior to the collection of personal data, the data subject must be given notice. • Personal data collected should be accurate • Implementation of security safeguards • Appointment of data protection officers[119]	measure • In case of a breach to notify the Data protection Board • Appoint the Data protecion officer • Provide the effective mechanism to reddress the grievances[120] Additional On obligation in Children's case • Obtain parent consent • Undertake processing of personal data • Not monitoring the behavior of children[121]
Consent	Provided that consent is required for the collection and processing of data.	DPDP Act, 2023 Requires free, specific, and unambiguous prior consent for the process of data-by-data Fiduciary, however, it also mentioned the

[119] *Article 5, Principles relating to processing of personal data*
[120] *Section 10 of the Digital Personal Data Protecion Act,* 2023
[121] *Section 9 of Digital Personal Data Protection Act, 2023*

		Deemed consent for the processing of personal Data.
Exemptions	The GDPR provides the following exemption- • The data can be processed for the purpose of national security Immigration exemption in case of prejudiced immigration matters section [122]	The Act provides the following exemption • To enforce any legal right • Court or tribunal • Interest of prevention, detection, investigation or prosecution of any offence. • Data principle not within Indian territory • State interest of sovereignty and integrity[123]
Enforcement Agencies	GDPR establishes three enforcement agencies for data regulation- • European Data Protection Board[124] • supervisory authorities[125] • Data Protection Authority	The bill grant power to the government to form Data Protection Board of India
Penalties	GDPR has a penalty of 10-20 million Euro or the2%-4% of the total worldwide annual turnover of the entity in case of data breach and non-	DPDP Act, 2023 provided the penalty for non-compliance 50 cr, failure to notify the board or non-fullfilment of obligation 200 Cr, failure of security

[122] *Article 26, GDPR*
[123] *Section 17 of the DPDP Act,2023*
[124] *Article 68, GDPR*
[125] *Article 62 of GDPR*

	compliance.[126]	measure 250 Cr, and can exceed up to 500 Crore rupees.[127]

5.2.1. Analysis Drawn from Comparison:

The comparison between India's Digital Personal Data Protection Act (DPDP) Act, 2023 and the European Union's General Data Protection Regulation (GDPR) of 2016 offers an extensive overview of data protection laws across countries. The comparison highlights the following details:

a) The GDPR provides protection for sensitive personal data by clearly defining it, whereas the DPDP Act, 2023 focuses more broadly on personal data protection and does not specifically address sensitive personal data.

b) Unlike the GDPR, which mandates data localization compliance for companies, the DPDP Act, 2023 does not include any data localization requirements.

c) Both the GDPR and DPDP Act, 2023 recognize individual consent as a legal basis for processing personal data. However, the DPDP Act, 2023 introduces the unique concept of 'consent managers.'

d) While both regulations establish new legal grounds for handling personal data, a notable distinction is that the DPDPB 2022 deems consent to be given when individuals voluntarily provide personal data and it is reasonably expected that they would do so. For example, if a person shares their name and mobile number with a restaurant to reserve a table, the DPDP Act, 2023 considers this as implicit consent for the restaurant to use this data for confirming the reservation.

e) The DPDP Act, 2023 sets 18 years as the minimum age for children, whereas the GDPR categorizes the age into two groups: one starting at 13 years and another at 16 years. Additionally, the GDPR provides separate guidelines for processing children's data, which the DPDP Act, 2023 does not.

f) The GDPR establishes a separate supervisory authority for conducting joint operations with other Member States' supervisory authorities, including joint investigations and enforcement measures. In contrast, the DPDP Act, 2023 designates the Data Protection Authority as the sole enforcement agency. The GDPR, however, includes three different enforcement agencies alongside the supervisory authority.

[126] *Article 83(5), General Conditions for imposing administrative fine, GDPR*
[127] *Section 33, Chapter VIII, under the Schedule I of DPDP Act, 2023*

The comparison illustrates the nuanced differences and similarities between the data protection frameworks of India and the European Union, shedding light on their respective approaches to safeguarding personal data information in the digital era.

5.3 USA CCPA California Consumer Privacy Act of 2018 Act and Digital Personal Data Protection Act, 2023 of India:

Basis of Comparison	UNITED STATES	INDIA
Introduction	The United state has a bunch of data protection laws on the federal and state level. For comparison with the Indian law, the California Consumer Privacy Act CCPA 2018 has been taken into consideration because it's a Framework similar to GDPR, 2016 and covers the personal data protection of the consumers. The US government also taking the initiative to strengthen this framework and amended it for strong protection of Personal information and data protection	India does not have comprehensive data protection law, but the Recently Digital Data Protection Act, 2023 is a set of regulations for data protection, The legislation has IX Chapters and a total of 44 Section deal with the collection, regulation, storage, rights, duties, exemption, and penalty.
Scope	CCPA protects information and introduced a new set of sensitive personal information for protection. applicable to the business that collects consumer data or personal information jointly or alone or with other, the business of $25M+ annual revene from anywhere or derives 59% of relieve from selling consumer data and Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes	Applicable on Processing of personal data within India. The processing of digital personal data outside the territory of India. Not applicable on- offline personal data, non-automated data Personal data is processed by individuals for personal and domestic purposes and contained recor existence for 100 years.[128]
Definition of Personal Data	The CCPA defines "Personal Information as the " information that identifies	The Act covered the definition of Personal data as - any data about an

[128] Section 2 & 3 of The Digital Personal Data Protecion Act, 2023

	directly or indirectly a particular consumer or household. Personal information includes the name, postal address, UPD, Internet Protocol address, email address, account name, SSN, Driver's license number, or other similar identifiers. The definition also includes audio, electronic, visual, thermal, olfactory, professional or employment, education sensitive personal related Information[129]	individual who is identifiable by or in relation to such data , this defition is complex to define.
Authorities for data process and data collection.	Controller or processor Service Provider Third parties	Data fiduciary Significant Data Fiduciary Data processor
Cross-border data	Only applicable to the entities doing business in California that collects consumer data or personal information jointly or alone or with other, the business of $25M+ annual revenue from anywhere or derives 59% of relief from selling consumer data and annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes	DPDP Act, 2023 defines the provision of cross-border data flow, where the entities require permission to use data.[130]
Children's data	Defined child age as 13- 16 years opt-in requirement for selling the personal information of minors between 13 and 16 years old, while parents or legal guardians are required to opt-in for minors under 13.	DPDP Act Consisted the 18 years as the valid age for the data processing and parent are permissible to grant consent on children's behalf
Data Principal Rights	The CPRA Grants the following rights to	The DPDP Act, 2023 Recognise the following

[129] *Section 1798.140 v (1)*
[130] Section 16 of DPDP Act, 2023

	consumers- • Right to Delete Personal Information [131] • Right to correct inaccurate personal information [132] • Right to know what personal data is being collected (Right to access personal information)[133] • Right to know What Personal Information is sold, shared, and to whom[134]. • Right to opt out of the sale or sharing of Personal information[135] • Right to Limit the use and disclosure of Personal information[136] • Rights of no Retaliation following opt-out exercise of other rights [137] • Right to Action – to seek actual damages or stator damages in case of company failure to resolve the case.	rights, • Right to information about personal data • Right to correction and erasure of personal data • Right to grievance redressal • Right to Nominate in case of death and incapacity to exercise other rights[138]
DATA FIDUCIARY DUTIES	• To provide notice in reasonable form for the collection or use of data • provide notice to consumers at or before data collection	General Obligations • Compliance with the act • Made reasonable effort to ensure data protecion • Implement

[131] *Section 1798.105*
[132] Section 1798.106
[133] *Section 1798.110*
[134] *Section 1798.115*
[135] *Section 1798.120*
[136] *Section 1798.121*
[137] *Section 1798.125*
[138] Section 11 of the DPDP Act, 2023

	• create procedures to respond to requests from consumers to opt-out, know, and delete. o For requests to opt-out, businesses must provide a "Do Not Sell My Info" link on their website or mobile app. • verify the identity of consumers who make requests to know and to delete, whether or not the consumer maintains a password-protected account with the business. • Check network security requirements, especially for consumer PI collection and storage. • Increase network security as needed. • Find suitable encryption solutions and policies. • Find cyber security laws and standards including HIPAA, GLBA, NIST, CIS, ISO, COBIT, and PCI DSS. • Privilege cyber security program assessment and mapping to legal criteria and standards. • Refine incident reaction plan. • Governance challenges include executive leadership's cyber security management and independent directors' involvement. • Assess corporate risk	appropriate technical and organization measure • In case of a breach to notify the Data protection Board • Appoint the Data protecion officer • Provide an effective mechanism to redress the grievances[139] Additional On obligation in Children's case • Obtain parent consent • Underate processing of personal data • Not monitoring the behavior of children[140]

[139] *Section 9 of the Digital Personal Data Protecion Act*, 2023
[140] *Section 9 of Digital Personal Data Protection Act, 2023*

	profile, insurance coverage, and need for extra coverage.	
CONSENT	CCPA mandates that consent compulsory for the process of data by the business.	DPDP Act, 2023 Requires free, specific, and unambiguous prior consent for the process of data-by-data Fiduciary These provisions give consumers greater control over their personal data and allow them to make informed decisions regarding their privacy, however, it also mentioned the Deemed consent for the processing of personal Data.[141]
Exemptions	The CCPA categorically does not apply when other specified privacy laws apply, such as information covered by the Health Insurance Portability and Accountability Act of 1996 (1798.145(c)(1)), Fair Credit Reporting Act (1798.145(d)), Gramm-Leach-Bliley Act (1798.145(e)), Driver's Privacy Protection Act of 1994 (1798.145(f)), and more.	The Act provides the following exemption • To enforce any legal right • Court or tribunal • Interest in the prevention, detection, investigation or prosecution of any offense. • Data principle not within Indian territory State interest of sovereignty and integrity[142]
ENFORCEMENT AGENCIES	California Attorney General's power to assess a violation of the CCPA	Data Protection Board of India[143]
PENALTIES	penalty fine up to $7,500 for each intentional violation or $2,500 for each violation, with an additional $7,500 for each violation involving a	provided the penalty of for non-compliance 50 cr, failure to notify the board or non-fulfilment of obligation and breach in

[141] Section 6 of the DPDP Act, 2023
[142] *Section 17 of the DPDP Act,2023*
[143] Section 18 of the DPDP Act,2023

	consumer under 16 years old.	relation to children 200cr, failure of security measure 250cr, and can exceed up to 500 crore rupees.[144]

5.3.1 Analysis Drawn from Comparison:

The comparison between India's proposed Digital Personal Data Protection Bill (DPDP) Act, 2023 and the California Consumer Privacy Act (CCPA) 2018 provides an extensive overview of data protection laws in different countries. The analysis highlights the following key points:

a) Both the CCPA and the DPDP Act, aim to protect the data privacy of their respective citizens. These laws require companies to be transparent about their data practices and grant individuals control over their personal data. Both laws also include provisions that allow individuals to request the deletion of their data or to prevent their data from being shared with third parties.

b) The CCPA and DPDP Act, both impose substantial fines on companies that fail to comply with their regulations, reflecting the seriousness with which lawmakers view these issues. However, the penalties imposed by the DPDP Act, are higher compared to those under the CCPA.

c) The DPDP Act, includes regulations on the cross-border flow of data, a provision not found in the CCPA, which only regulates data within the United States and covers specific business entities.

d) Both the CCPA and the DPDP Act, include provisions related to the collection of children's data by business entities. However, they differ in their criteria: the CCPA defines children as those aged 13-16 years, while the DPDP Act, defines children as individuals under 18 years.

e) In terms of the rights granted to individuals, the CCPA has a broader scope, whereas the DPDP Act, grants a more limited set of rights to data principals.

f) Both the CCPA and the DPDP Act, mandate consent for the processing and collection of data, including children's data, where consent from a lawful guardian or parent is required. However, the CCPA also recognizes special rights under specific circumstances that allow business entities to process children's data without permission.

g) The CCPA establishes a Consumer Privacy Fund (CPF) within the State Treasury's General Fund to cover the enforcement costs of the Attorney General's office and state courts. This fund receives 20% of any civil penalties imposed by the Attorney General under the CCPA.

[144] *Section 33 of DPDP Act, 2023*

This analysis illustrates the similarities and differences between the data protection frameworks of India and California, emphasizing their respective approaches to protecting personal information in the digital age.

CONCLUSION

The rapid advancement of technology has made data protection a crucial aspect of privacy in India. As more people use the internet and digital devices, they generate vast amounts of personal or sensitive data. Data protection has become a very important issue in India. Chapter 2 of the analysis establishes the origin and development of privacy and the right to privacy in India. It highlights that privacy has always been a highly valued aspect of human life, allowing individuals to control their lives and prevent interference from others. This control enables them to express their thoughts freely without fear of judgment or punishment.

As society and technology have evolved, the recognition of privacy as a legal right has also progressed. According to Article 21 of the Constitution of India, the right to privacy is recognized as a fundamental right, ensuring that no individual shall be deprived of their personal liberty or life. India, as a digitally empowered society and a knowledge-based economy, has initiatives like the Aadhaar card, which provides every citizen with a unique ID number linked to their biometric information. The MyGov platform allows citizens to participate in governance and offers a safe and confidential means of communication. The Supreme Court of India affirmed the right to privacy as a fundamental right under the Constitution in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, recognizing that the right to privacy includes the right to manage one's personal information.

Before August 2023, India did not have a comprehensive law for data protection. The Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2019, the Digital Personal Data Protection Bill 2022, and its updated version, the Digital Personal Data Protection Act 2023, aimed to establish a framework for data management that safeguards people's privacy. The Act defines key terms such as consent, data, data fiduciary, data principal, data processor, personal data, sensitive personal data, and transgender status. It includes rules for consent, data fiduciary relationships, and enforcement. The Act outlines requirements for data protection, including restrictions on data collection, legal processing, storage limits, and data fiduciary accountability. It establishes distinct legal bases for processing both sensitive and personal data, including that of children, and acknowledges data subjects' rights to access, rectification, and erasure. Certain instances of data processing are exempt from the Act, particularly for government agencies and the courts. Additionally, it creates a Data Protection Authority to supervise the actions of data fiduciaries, control the transfer of data across international borders, and issue fines and compensation. However, the 2023 Act still has shortcomings, such as the absence of a specific timeline for reporting data breaches.

The Digital Personal Data Protection Act, 2023, is a law that governs the control of personal information in India. The Act requires compliance from all organizations managing personal data of Indian citizens, including governmental bodies, for-profit companies, and non-profit groups. The lack of data localization guidelines in the law contrasts with the global trend toward data localization. The Act imposes

precise obligations on data management and strict fines on businesses that fail to protect customer data adequately. The proposed legislation aligns with international standards for data privacy and protection, such as the General Data Protection Regulation (GDPR), emphasizing the importance of obtaining individuals' informed consent before collecting and using their personal information.

A significant step towards protecting people's privacy is the requirement to appoint a Data Protection Officer (DPO). The DPO will manage the organization's data protection policies and procedures and respond to concerns or questions from data principals. The right to information ensures accountability and transparency in data processing activities by informing the data principal about the collection, processing, and use of their personal data. With a maximum fine of 500 crore rupees, the Data Protection Board is empowered to impose fines in six main areas under the legislation. However, the Board's ability to conduct investigations is limited to handling customer complaints. Despite the efforts of comprehensive data protection legislation in the form of various data protection bills, India still lacks an adequate set of laws and regulations for data protection.

India has implemented several legislations for data protection, including the Information Technology Act, 2000, and various proposed legislations such as the Data Protection Bill 2006, Personal Data Protection Bill 2018, revised Personal Data Protection Bill 2019, and the JPC recommendations Bill 2021. The newly proposed Digital Personal Data Protection Bill 2022 and the Digital Personal Data Protection Act 2023 also aim to enhance data protection. Therefore, it cannot be said that India lacks regulations for data protection. However, comprehensive data protection is still evolving, and continuous efforts are being made to improve the legislation. India's laws are not as comprehensive and sufficient in terms of protection and enforcement as compared to the EU and USA."

India has enforcement mechanisms for data protection and imposes obligations on entities dealing with data. However, there is a lack of comprehensive data protection and a separate enforcement agency for data regulations. The newly proposed bill and existing legislative framework are not as effective as the EU GDPR 2018 or the USA's California Consumer Protection Act in terms of protective measures for personal data. Indian law lacks a clear definition of sensitive data and non-personal data protection. The definition of personal data is not comprehensive, and the newly proposed bill does not specify what information is covered under data protection as compared to the EU GDPR. The Digital Personal Data Protection Act, 2023, is effective in covering cross-border data transactions but imposes limitations on data localization and lacks a timeline for reporting data breaches. Therefore, the duties and rights under Indian law are more limited.

In summary, while India has made significant strides in data protection legislation, there are still areas that require improvement to match the comprehensiveness and effectiveness of data protection laws in the EU and USA.

SUGGESTIONS

Suggestions for Improving the Digital Personal Data Protection Act, 2023. The following recommendations are drawn from the examination of the Personal Data Protection Bill 2018, 2019, the Digital Personal Data Protection Bill 2022, and the Digital Personal Data Protection Act 2023. Additionally, a comparative analysis

with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) provides further insights.

1. Definition of Personal Data:

The DPDP Act, 2023 requires a more comprehensive definition of personal data. The definitions provided by the GDPR and CCPA can serve as a reference to clearly outline the types of information that fall under personal data.

2. Data Localization:

Data localization, which allows countries to maintain complete control over their data, should be incorporated. The GDPR's provisions for data localization can be adapted to India's context to ensure effective data monitoring within the country.

3. Protection of Children's Data:

Age Range Adjustment: The DPDP Act includes children up to the age of 18, whereas GDPR and CCPA set the age range at 13-16 years. The Act prohibits tracking, behavioral monitoring, and targeted advertising directed at children, as well as any data processing likely to cause harm. Exceptions may be prescribed by the government.

Refinement of Provisions: These provisions should be refined to balance protection with practicality, considering psychological and developmental perspectives.

4. Sensitive Personal Data:

Recognition and Protection: The current DPDP Act does not adequately recognize sensitive personal data such as DNA samples, healthcare records, and credit card information. Aligning the Act with the GDPR and CCPA, which emphasize the protection of sensitive personal data, is necessary.

5. Expansion of Individual Rights:

Enhanced Rights*: The DPDP Act of 2023 restricts individual rights compared to the GDPR and CCPA. A review to expand these rights is essential to establish a robust framework that empowers individuals in managing their data.

6. Enforcement Mechanisms:

Diversified Enforcement: While the DPDP Act proposes a single board for investigating and prosecuting data breaches, more adaptable enforcement mechanisms should be considered. Drawing from the GDPR and CCPA, multiple methods of enforcement can provide greater flexibility and effectiveness.

7. Timeliness in Data Breach Notification:

Specific Timeline: The DPDP Act does not specify a timeline for notifying the Data Protection Board (DPB) in the event of a data breach. Unlike other statutes that stipulate precise time limits, the Act should mandate a specific timeframe for breach notifications to ensure timely responses and mitigation.

8. Appointment of Data Protection Officers (DPO):

DPO Requirement: Mandating the appointment of a Data Protection Officer to oversee data protection policies and procedures within organizations can enhance compliance and address data principals' concerns effectively.

9. Alignment with International Standards:

Global Consistency: Aligning the DPDP Act more closely with international standards like the GDPR and CCPA will not only enhance data protection within India but also facilitate cross-border data flow and cooperation.

10. Penalties and Fines:

The Act has increased penalties compared to previous bills, demonstrating a serious commitment to data protection. This approach should continue to ensure companies are held accountable for data misuse and non-compliance.

By implementing these recommendations, the Digital Personal Data Protection Act, 2023 can be refined to provide comprehensive data protection, enhance individual rights, and align with global standards, thereby creating a safer and more secure digital environment in India.

REFERENCES

1. Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021
2. Solove, D. J. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006, 154 (3), 477-560
3. Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011
4. M. R Konvitz, Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2. (1966) p. 272
5. Keulen Sjoerd., Algemene Rekenkamer. "Chapter Title." In Handboek Privacy Studies, edited by Editor's Name, 21-56. Amsterdam: Amsterdam University Press.
6. Jan Holvast, Holvast & Partner, Privacy Consultants History of Privacy, NL - Landseer, The Netherlands
7. Professor Eric Goldman, An Introduction to the California Consumer Privacy Act (CCPA) Santa Clara University School of Law July 1, 2020,
8. M. R. Lefkowitz, Women's Life in Greece and Rome: A Source Book in Translation; JHU Press: Baltimore, 2020
9. J. P Balsdon, V. D. Roman Private Life and Its Survivals. In Roman Civilization: Selected Readings; Kagan, D.; Viggiano, G., Eds.; Columbia University Press: New York, 1960; pp 231-248.03
10. G. L Maffei,. Roman Art; Harry N. Abrams: New York, 2002

11. H Nissenbaum,. A Contextual Approach to Privacy Online. Daedalus, 140 (4), 32-48 2011
12. Naomi Rosenblum, A History of Women Photographers (Abbeville Press 2010).
13. Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905).
14. Samuel D Warren., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5): 193-220 (1890
15. L William Prosser. "Privacy." California Law Review 48, no. 3): 383-423(1960)
16. World Bank and CGAP. Data Protection and Privacy for Alternative Data. GPFI-FCPL Sub-Group Discussion Paper - Draft - May 4 2018.
17. F Nicholas. III Palmieri, Data Protection in an Increasingly Globalized World, 94 IND. L.J. 7 (2019),
18. Woodrow Hartzog & Neil M. Richards, Privacy's Constitutional Moment and the Limits of Data Protection, 61 B.C. L. REV. 1687 (2020),
19. European Data Protection Supervisor. Government access to data in third countries: Final report (EDPS/2019/02-13). Brussels: European Data Protection Supervisor, 2019.
20. Data Protection Law: An Overview." Congressional Research Service, R45631 (n.d.).
21. Nikhil Pahwa, The Problem with India's Proposed Intermediary Liability Rules, Quartz India (Dec. 28, 2018),
22. Upasana Sharma & Aniket Singhania, The Personal Data Protection Bill, 2019: An Overview, Mondaq (Jan. 13, 2020),
23. National Institution for Transforming India. (2020). Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data. New Delhi: NITI Aayog.
24. Vijay Pal Dalmia and Rajat Jain, Compliances by an Intermediary Under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - social media - India, Mondaq (May 9, 2022),
25. European Data Protection Supervisor, Handbook on European Data Protection Law (2018),
26. Hustinx, P., EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation
27. Shanaz, Asifullah Samim and Mohammad Edris Abdurahim Zai, Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information, Trinity Law Review, Volume-3, Issue-2, 2023.
28. Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground'

BIBLIOGRAPHY

Legislation

- The Constitution of India
- Information Technology Act 2000

- Personal Data Protection Bill 2006
- Personal Data Protection Bill 2018
- Personal Data Protection Bill 2019
- Personal Data Protection Bill 2021
- Digital Personal Data Protection Bill 2022
- Digital Personal Data Protection, Act 2023
- SPDI Rules 2011
- Intermediary Guidelines 2011
- Intermediary Guidelines and Digital Ethics Rule 2021
- General Data Protection Regulation, 2016
- HIPPA (Health Insurance Portability and Accountability Act) 1996
- Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003
- The Fair Credit Reporting Act FCRA 1976
- Electronic Communications Privacy Act, 1986
- The Children's Online Privacy Protection Act (COPAA), 2000
- The California Consumer Privacy Act CCPA 2018

Website/Journal

- The University of Pennsylvania Law Review
- NITI Aayog.
- Mondaq
- SSRN
- Research Gate
- Hein Online
- Harvard Law Review
- California Law Review
- Congressional Research Service
- Privacy Studies, edited by Editor's Name, 21-56. Amsterdam
- JSTOR