INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

COMPARING INDIA'S DATA PROTECTION LAWS WITH THE EU AND US IN THE DIGITAL ERA

AUTHOR - SANJAY A. MULIK* & DR. R K GUPTA**

* RESEARCH SCHOLAR, NIILM UNIVERSITY, DEPARTMENT OF NIILM UNIVERSITY, KAITHAL

** RESEARCH GUIDE, NIILM UNIVERSITY, DEPARTMENT OF NIILM UNIVERSITY, KAITHAL

BEST CITATION – SANJAY A. MULIK & DR. R K GUPTA, COMPARING INDIA'S DATA PROTECTION LAWS WITH THE EU AND US IN THE DIGITAL ERA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (11) OF 2025, PG. 711-723, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

Globally, technology has developed rapidly in recent decades as the internet has become ubiquitous and has eroded geographic barriers to information flow. We have become increasingly dependent on data as our lives become increasingly connected. Data plays a crucial role in every aspect of our daily lives, from social media to banking to retail. Due to the increased interconnectedness, individuals must have control over their personal information. Various sectors in India are being digitized, and the digital India program has been launched, making it one of the world's largest economies. In response to growing concerns about personal data protection, the Indian government has introduced a number of laws. In its preamble, this bill's preamble seeks to explain how individual privacy rights, as well as individual data, are protected in a rapidly technologically developing country such as India. The purpose of this study is to investigate the efficiency and challenge of applying data protection law. This dissertation compares Indian law with that of the European Union and the United States in order to determine the scope of improvements based on data protection principles. Rights of individuals, accountability measures for data processors, and remedies for data breaches include enforcement mechanisms, individual rights, and rights for data processors. This will be a fundamental issue in this digital age, and countries must take major steps towards resolving it. We will try to improve the Indian legal framework to gain a better understanding of the grey areas where it may have complex issues.

Keywords: Digital Data Protection, Privacy, Data protection, European Union, Personal Data;

INTRODUCTION

A digital transformation is taking place in India, which is increasingly utilizing technology and the internet. The prevalence of cyber-attacks and data breaches has increased, so cyber security and data protection measures are more important than ever. India is the second-largest internet market in the world with 1.3 billion people. Increasingly stringent rules and regulations have been enacted to protect privacy as the data protection landscape has expanded. In recent decades, the world has undergone dramatic changes as a result of rapid technological advancements. Globalization and international trade make it necessary for industrialized societies to store data and information. Organizations of all sizes use low-tech methods to store data, which is no longer merely an information or power source. People have always been concerned about their privacy on the internet because it is a never-ending source of information.

We no longer enjoy the right to privacy that we used to due to the new digital environment. People can conduct their routine online activities safely thanks to the Internet, but

privacy and data security questions remain unanswered. Third parties are hesitant to access individuals' and organizations' data and information. In response to the growing concern about digital privacy in various sectors, governments are adopting new laws designed to regulate how businesses gather, store, and process client information. All players in this arena will benefit greatly if they invest more resources into cybersecurity programs that can protect them from both known and unknown threats. As data protection laws and regulations are developed and implemented, striking the right balance between privacy and innovation is becoming increasingly critical.

There is constant discussion in India about data breaches. India is the country with the largest data breach, according to the WEF World Economic Forum's Global Risk Report 2019. According to a report published by the Internet and Mobile Association of India (IAMAI) (IAMAI, 2020), India's cybersecurity workforce will need 1 million more qualified personnel by 2025. Data protection is also becoming increasingly important due to cyberattacks and data breaches across the country. There were over 4 lakh cyber-attacks in India in 2019, a 37% increase over the previous year (CERT-In, 2019). The Aadhaar data breach was the biggest data breach in history (Jain, 2018) and exposed over 1.1 billion Indians' personal information.

In India, data protection laws are governed by the obsolete Information Technology (IT) Act 2000, which is insufficient to deal with the complexities of today's digital environment. The IT Act, 2000 contains inadequate data protection and cybersecurity provisions, despite the fact that the Act was updated in 2008 to add these provisions. Despite efforts by the Indian government to ensure complete data protection for Indian citizens, neither the Personal Data Protection Bill 2019 nor the Digital Personal Data Protection Bill, 2022 have been enacted.

The Digital Personal Data Protection Bill 2022 regulates how personal data is acquired, stored, processed, and used by businesses and government organizations. Identifiable data includes information about an individual, as defined in the Bill. A number of guidelines are also included on data protection, such as limiting the use of data, minimizing data, and being accountable for it. It is necessary to establish an independent regulatory organization known as the Data Protection Authority (DPA) to enforce the Bill's provisions. The Indian government has made significant efforts to strengthen its data security organization. Business and government organizations are subject to the Digital Personal Data Protection Act, 2022, which has the authority to conduct investigations and punish violators. The Indian government launched the in 2015 as a means of protecting data security and privacy. In 2017, the Ministry of Electronics and Information Technology (MeitY) launched the Digital India program, which applies to society and the economy. The program includes a number of data privacy and security measures, such as creating a safe digital infrastructure, promoting cybersecurity awareness, and facilitating cybersecurity research. Moreover, the Indian government has established several bodies to oversee data protection. The Indian Data Protection Authority (IDPA) and the Data Security Council of India (DSCI) are the most renowned organizations in the field of data privacy and security in India. In collaboration with government and other stakeholders, the DSCI develops data protection policies and legislation, and offers business data protection advice and certification.

Digital Personal Data Protection Bill 2022 is India's fifth attempt to enact a comprehensive data protection law.

LITERATURE REVIEW

In terms of data protection, India, Europe, and the United States have different legal frameworks.

The 2022 digital data protection bill consists of the following provisions:

MeitY is the ministry responsible for electronic and technological development. A bill protecting personal digital data will be introduced in 2022. A roadmap for the future lawn 2022 is provided in this draft by highlighting key features and issues in the Digital Data Protection Bill as well as comparing it to its predecessor. Researchers interested in understanding how the previous bill might affect data protection under the new bill will find this research paper useful.

The General Data Protection Regulation, 2016/679, is as follows:

There is a European Parliament, and there is a European Council. As of 2016. The General Data Protection Regulation (GDPR) repeals Directive 95/46/EC (General Data Protection Regulation) regarding the protection of natural persons with regard to the processing of their personal data. The European Parliament passed Regulation (EU) 2016/679 on 27 April 2016, L 119, p 1-88, European Union Official Journal.

The definition and protection of privacy and data in India

Public servants are threatening privacy in the name of "procedure established by law" or "public duty.". The right to privacy is fundamental to a peaceful life and to dignity and liberty for all. With the increase in digitalization and usage of social media and the internet, data protection and privacy have become national issues. There is an interconnected relationship between data protection and privacy in the legal profession.

India's Privacy and Data Protection: A Critical Assessment

This paper discusses the conflict between the right to privacy and data protection in India and argues that the current Information Technology (Amendment) Act, 2008 does not adequately protect data. A debate on this topic is intended to be initiated by the author, who suggests separate legislation to protect data and privacy. In order to analyze the IT provision and amendment act of 2008, this data is used for the research.

An analysis of the current global trends in data protection laws, challenges and the need for reforms in India

In the article, the authors discuss the current state of global data protection laws, challenges, and the need for reforms in Indian data protection laws. As society becomes increasingly digitalized, it becomes increasingly important to protect and secure data. Also in the article, the author raises questions about who owns, who accesses, and how long virtual data lasts. Furthermore, it emphasizes the need for a law in India to address concerns about digital security, information assurance, and data protection. A comparison is also made between the General Data Protection Regulation (GDPR) in the EU and the Personal Data Protection Bill in India in the article.

Choosing the right laws and regulations to protect your personal information in India

In the article, the author discussed the protection of data and privacy in India. Individuals have a right to privacy, which is enshrined in the constitutions of many developed nations. In the 1970s, computerized systems were developed that could store and distribute large amounts of data, causing concerns regarding privacy and data protection. There is no explicit right to privacy in the Indian Constitution, but courts have interpreted other constitutional rights, such as life and liberty, to include a limited right to privacy. As a party to numerous international instruments, India recognizes the rights to privacy outlined in the Universal Declaration of Human Rights and the International Convention on Civil and Political Rights.

Critical Commentary on the Digital Personal Data Protection Bill, 2022: Soft Tone, Tiger Claw.

As the DPDPB 2022 evolves from the lengthy Personal Data Protection Bill 2019, the commentary provides valuable insight into the evolution of the bill. This commentary examines

several important aspects of the bill, including digital citizens' rights and responsibilities, children's privacy rights, and redress mechanisms for data fiduciaries. Furthermore, the commentary thoughtfully analyzes ambiguous clauses related to deemed consent, which has been a subject of debate. This research will use commentary to grasp the complex concept and compare it with other concepts in order to grasp a complete understanding of it.

There are 12 major concerns with the Data Protection Bill, 2022, in India. Media

Researchers who are interested in analyzing the 12 major concerns with the digital data protection bill 2022 and assessing their relevance to its provisions are invited to read this article.

A Practical Look at India's Digital Personal Data Protection Bill, 2022: Does Consent Work?

A brief discussion of consent is presented in this article, highlighting the key issues associated with consent in the Digital Personal Data Protection Bill and emphasizing the importance of understanding the concept of consent in different countries' legislation.

Digital Personal Data Protection Bill, 2022: Comments submitted to the Ministry of Electronics and Information Technology.

The report provided recommendations made by the VDIHI Centre regarding several provisions and important definitions of the Digital Personal Data Protection Bill. The report analyzes the bill thoroughly and discusses important concepts such as the definition of data principles, deemed consent, and the application of the act. A thorough understanding of the VDIHI centre's recommendations and current provisions is essential for research purposes.

As Shailesh Gandhi points out in ten instances, the digital data protection bill threatens the RTI Act. Scroll. In (2023).

In this article, we discussed two important provisions of the bill and how they affect the Right to Information Act, section 8(1) j, which exempts the disclosure of personal information. This study will utilize the article to provide more comprehensive information on Section 8 (1) (j) of the Right to Information Act 2005 and the Digital Personal Data Protection Bill,2022.

In S. Mehrotra, et al., The Digital Personal Data Protection Bill, published in SSC online (2022).

The purpose of this article is to compare the relevant provisions of the Digital Personal Data Protection Bill with those of the General Data Protection Regulation of the European Union. Furthermore, the study will analyze and compare the important provisions of the bill in a broader sense. For an understanding of how the two pieces of legislation may impact data protection, it is vital to know their similarities and differences.

METHOD

Methodologies for conducting an examination encompass a wide range of strategies and procedures. Logic examination includes research as one of its specialties. As a result, research is the process of logically and orderly gathering information on a particular topic. One reason for contemplating a research system is to understand the techniques and methods received for accomplishing the project's goal.

A Doctrinal Research framework was utilized by the author for the purpose of this study. The framework involves analyzing legal documents and literature, including statutes, case law, and scholarly articles. In addition to primary sources, the author draws upon secondary sources as well. Among the primary sources are Indian, European Union, American, and Canadian legislation, including the Information Technology Act, 2000, the Personal Data Protection Bill, 2019, and the General Data Protection Regulation, 2016, as well as case law and judicial decisions. Data protection experts and organizations provide secondary sources such as scholarly articles, books, and reports. In addition, a comparative study method is employed for analyzing the different topics in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

the research and comparing Indian, European Union, and American laws. As part of this method, data protection, privacy, and enforcement laws and regulations of India are compared to those of the European Union and the United States. As a result, it is possible to examine the strengths and weaknesses of the Indian legal framework and its potential implications compared to other jurisdictions' data protection laws.

DISCUSSION

Comparative Analysis

A comparison between the GDPR 2018 of the European Union and the recently proposed Digital Personal Data Protection Bill 2022 of India

Basis of Comparison	EUROPEAN UNION	INDIA
Introduction	There are several laws in the EU for data protection, but GDPR is the most important one with a huge impact on data protection. On May 25, 2018, it was adopted after being proposed in 2016.	A comprehensive data protection law is not in place in India, but the Digital Data Protection Bill, 2022, is a set of regulations. A total of 30 sections are included in the proposed legislation, which covers collection, regulation, storage, rights, duties, exemptions, and penalties. The proposed legislation has six chapters and six sections.
Territorial Scope	It applies to entities established in the EU, but whose data processing may or may not take place within the EU. Not established in the European Union, but processing personal data primarily related to goods or services offered by EU residents. An institution established outside the EU under the Public International Law of member states	This policy applies to the processing of personal data within India. Extending the processing of digital personal data outside of India's borders. On-offline personal data, non-automated data are not applicable There is a 100-year record of personal data processed for personal and domestic purposes by individuals.
Subject matter scope	Information about an individual or organization, as long as it isn't being used by law enforcement or national security organizations. In accordance with GDPR, anonymous data is not subject to its provisions.	Information collected by the entities about individuals.

Definition of Data	Under GDPR, the definition of data includes not only personal data, but also sensitive personal data. Generally, Personal Data consists of information about an individual, identified by name, identification number, location data, and online identifier, as well as factors associated with their physical, genetic, mental, economic, cultural, or social identity.	A person's personal data is defined in the bill as any information that can be used to identify that individual, however this is a complex concept.
Grounds for the Process of Data	Consent is obtained from the data subject for the processing of their data. Contractual data processing The processing of data in order to protect the legitimate interests and vital interests of the data subject. Complying with a legal obligation through the processing of data. Life interest data processing. Public interest data processing	Legally permissible processing of data for a lawful purpose
Authorities for data process and data collection.	Those who process personal data on behalf of the controller, whether they are natural or legal persons, public authorities, agencies or other bodies	Data collection and processing were delegated to three authorities under the bill Fiduciary responsibility for data Fiduciary responsibility for significant data Processor of data
Cross-border data	It mentions the exhaustive procedure, the code of conduct, the certificate mechanism, and the rules that govern data flow across borders, referred to as Data Localization.	There is a requirement that entities be able to use data across borders as part of the DPDPB, 2022.

Children's data	There are special categories of data that have a wider scope in GDPR, including the processing of children's personal data, the consent age ranges from 13 to 16 years, and the responsibility for obtaining parental consent.	In accordance with DPDPB, the valid age for data processing is 18 years and parents are permitted to grant consent on behalf of their children
Data Principal Rights	According to the GDPR, the following rights are recognized: Corrections are allowed Erasure rights Access to information Restrictions on processing rights The right to portability of data The right to be forgotten Objections are allowed	In 2022, the DPDPB recognizes the following rights: Information about personal data is a right Personal data correction and erasure rights Grievance redressal rights The right to nominate in the event of death or incapacity to exercise other rights
Data Fiduciary Duties	According to GDPR, a Data Fiduciary must comply with the following requirements	Obligations of a general nature Act compliance Protected data in a reasonable manner Ensure appropriate technical and organizational measures are implemented The Data Protection Board should be notified in the event of a breach Identify and appoint a data protection officer Readdress grievances in an effective manner In the case of children, additional obligations apply Consent must be obtained from the parents Process personal data Monitoring children's behavior is not done
	and limitations: The purpose of the project The collection of data is limited Limitations on the storage of personal data. Certain grounds, however, allow the storage of personal data for a longer period of time. The processing of personal data must be fair, legal, and open. The security of personal data must be guaranteed. Data subjects must be notified before their personal data is collected. Accurate personal data should be collected Security safeguards are implemented Data protection officers are	

	appointed	
Consent	As long as consent is required for data collection and processing.	DPDPB, 2022 requires free, specific, and unambiguous prior consent for data-by-data fiduciary processes, but also mentions deemed consent for the processing of personal data.
Exemptions	GDPR provides the following exemptions: If immigration matters are prejudiced, the data may be processed for national security purposes	In the Bill, the following exemptions are provided: In order to enforce a legal right Tribunals or courts Any offence should be prevented, detected, investigated, or prosecuted. Indian territory is not covered by the data principle Sovereignty and integrity of the state are paramount
Enforcement Agencies	For data regulation, GDPR establishes three enforcement agencies:	Among the provisions of the bill is the power for the government to form a Data Protection
	Data Protection Board of the European Union Authorities responsible for supervision Regulatory Authority for Data Protection	Board of India
Penalties	A data breach and non-compliance with GDPR can result in a penalty of 10-20 million Euro, or 2%-4% of the entity's total annual worldwide turnover.	In the DPDPB, 2022, penalties for non-compliance are 50 crores, for failure to notify the board or for non-fulfillment of obligations 200 crores, and for failure to take security measures 250 crores, with a maximum penalty of 500 crores.

By comparing the two laws, a comprehensive picture of countries' data protection laws was provided. Digital personal data protection is India's proposed legislation to protect information privacy in the digital world, and the General Data Protection Regulations of the EU that were adopted in 2016. Following are the details clarified by the comparison:

- As opposed to the GDPR, the DPDPB, 2022 bill contains more personal data protection legislation and does not contain the protection for sensitive personal data.
- Unlike the GDPR, the DPDPB, 2022 does not contain a clause requiring

companies to comply with data localization.

- Both GDPR and DPDPB 2022 recognize consent as one of the legal bases for processing personal data, with the latter introducing the concept of consent managers.
- There are new legal bases for handling personal data under the GDPR and the Bill. The GDPR and the Bill differ in this regard in that the Bill recognizes that a data principal is considered to have given consent for processing when he or she voluntarily provides personal data to the data fiduciary and it is reasonable to expect that the data principal would do so. This provision is clarified by the Bill, which uses an example in which a person who shares their name and mobile number with a restaurant to reserve a table is deemed to have given consent to the restaurant (i.e. the data fiduciary) collecting their name and mobile number to confirm the reservation.
- In the DPDP, 2022, the minimum age for children is 18 years, while in the GDPR, the age is divided into two categories, the first of which is 13 years and the second of which is 16 years. There is no separate set of guidelines for the processing of children's data in the DPDPB, 2022, whereas the GDPR does.
- As part of the GDPR, there is a separate supervisory authority that conducts joint operations with supervisory authorities of other Member States, including joint investigations and joint enforcement measures. A Data Protection Authority was established as an enforcement agency under the Data Protection and Privacy Board, 2022. GDPR, however, includes three separate enforcement agencies as well as the supervisory authority.

A comparison between the USA's CCPA California Consumer Privacy Act of 2018 and India's Digital Personal Data Protection Bill, 2022

- Through the comparison of the two laws, an extensive picture of the countries' data protection laws was provided. Information privacy in the digital world is protected by India's proposed legislation on digital personal data protection, as well as California's Consumer Privacy Act 2018. According to the comparison, the following details are clarified:
- The CCPA and the DPDP Bill both aim to protect the data privacy of their respective citizens. Individuals have control over their personal data under these two laws, which require companies to be transparent with their data practices. In addition, both laws allow individuals to request that their data be deleted or not shared with third parties.
- The CCPA and DPDP Bill also impose heavy fines on companies that fail to comply with their regulations, showing how seriously lawmakers are taking these issues. DPDP imposes a higher penalty than CCPA, however
- The DPDP regulates the cross-border flow of data, but this is not included in the CCPA, which only regulates business entities within the US.
- Although both CCPA and DPDP contain provisions regarding children's data collected by business entities, the criteria are different under the law. The CCPA recognizes children between the ages of 13 and 16, while the DPDP recognizes children below the age of 18 as children.
- In terms of rights granted to individuals, the CCPA has the much wider scope than the DPDP bill, which grants only limited rights.
- As part of the CCPA as well as the DPDP bill, consent is mandatory for data collection and processing. In case of children's data, parental or legal guardian consent is required. In addition

to recognizing special rights under certain circumstances under which a business entity can process children's data without their consent, the CCPA also recognized those rights.

- A Consumer Privacy Fund (CPF) is established in the State Treasury's General Fund under the CCPA. CCPA enforcement costs are covered by the AG's office and state courts. Any civil penalties assessed by the AG will go to the CPF at a rate of 20%.

CONCLUSION

As privacy concerns become more prevalent in the digital age, India's efforts to establish robust data protection legislation are crucial. Although the proposed data protection frameworks mark substantial progress, a comparison with the European Union's GDPR and the United States' sectorial approach reveals areas for improvement. In addition to enhancing individual rights, data processing accountability, and cross-border data transfer mechanisms, the GDPR offers valuable lessons. However, in regulating diverse industries, the U.S. approach emphasizes the importance of flexibility. India can develop a balanced framework that aligns with its socioeconomic and technological landscape, ultimately protecting individual privacy while fostering innovation and growth in its burgeoning digital economy by integrating elements from both systems.

Indian privacy laws have become increasingly concerned with data protection due to the rapid development of technology. The internet and digital devices are being used more and more, which creates a lot of data that can be sensitive or personal. The issue of data protection is very important in India at the moment. Through the analysis of the second chapter, it is found that privacy has been a crucial aspect of human life that has been highly valued throughout history. Through IL, people can keep control over their own lives and prevent others from interfering with them. Therefore, they are free to express themselves without fear of judgment or punishment. As society and technology have evolved, privacy has also been recognized as a legal right. Privacy is recognized as a fundamental right under Article 21 of the Indian Constitution, which ensures that no individual shall be deprived of their lives or personal liberty. Knowledge-based economies and digital empowerment are hallmarks of the Indian economy. Indian identification has been greatly improved by the Aadhaar card initiative. Using biometric information, it gives every citizen a unique identification number. In addition to providing a safe and confidential means of communication, the program has the MyGov platform that allows citizens to participate in governance. It was in Justice K.S. Puttaswamy (Reid.) and Another y that the Supreme Court of India recognized the right to privacy as a fundamental right under the Constitution. Other than the Union of India. According to the court, the right to privacy includes the right to manage one's own personal information. The government of India recognizes the importance of data protection and has implemented various laws and regulations to ensure the safety of the personal information of individuals.

In India, there is no comprehensive law on data protection. The Personal Data Protection Bill, 2018, and its updated version, the Personal Data Protection Bill, 2019, are intended to establish a framework for data management that safeguards people's privacy. In addition to defining important terms such as consent, data, data fiduciary, data principal, data processor, personal data, sensitive personal data, and transgender status, the bill also includes rules for consent, data fiduciary relationships, and enforcement. Data protection requirements are outlined in the bill, including restrictions on data collection, legal processing, storage limits, and fiduciary accountability. There are separate legal bases for processing sensitive and personal data, including that of children, and it recognizes data subjects' rights to access, rectification, and erasure. A few instances of data processing are exempt from the bill.

Furthermore, it establishes a Data Protection Authority to supervise the actions of data fiduciaries, control international data transfers, and issue fines and compensation. The proposed legislation, however, did not become law.

This law would control personal information in India under the Digital Personal Data Protection Bill of 2022. The bill requires that all organizations that handle Indian personal data comply with its requirements. The measure applies to all organizations that handle personal information, including governmental bodies, for-profit companies, and non-profit organizations. As a result of the trend toward data localization, there are no guidelines for data localization in the law. Businesses that fail to properly protect customer data will face steep fines under the measure. The proposed legislation is consistent with international standards for data privacy and protection, including the General Data Protection Regulation (GDPR), which emphasizes the importance of gaining individuals' informed consent before collecting and using their personal information.

A Data Protection Officer (DPO) is an important step towards protecting people's privacy. A DPO manages the organization's data protection policies and procedures and responds to any questions or concerns data principals may have. Data principals have the right to information in order to ensure accountability and transparency in data processing activities. Under the proposed Data Protection Bill, the Board is empowered to impose fines up to 500 cores in six main areas. Only customer complaints are subject to investigation by the Board.

RECOMMENDATION

After examining the Personal Data Protection Bill 2018 and 2019, as well as the Digital Personal Data Protection Bill 2022, the Suggestions were drawn up. A comparative analysis is also conducted between the DPDP Bill 2022 and the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The following recommendations are based on this analysis.

Digital Personal Data Protection Bill 2022 represents a significant step forward in regulating the collection and processing of personal data in the digital sphere. The Act is intended to give individuals greater control over their personal data and hold companies accountable for how they handle and use it. As compared to the previous bill, the penalty giver is increased and the scope of rights for data subjects is expanded. Although some adjustments will be required for the bill to be implemented, it ultimately aims to create a safer and more secure digital environment.

A revision to the definition of personal data is required by the DPDP bill of 2022. In addition to the GDPR and CCPA, the previous bill provided a comprehensive definition of personal data that specifically outlines the types of information that fall into this category. It is becoming increasingly popular to localize data, since it allows countries to have complete control over their data. Data localization is included in the General Data Protection Regulation (GDPR), which can be adopted by India to effectively monitor data within the country.

There is a growing concern about the impact of the internet on children, since determining the appropriate age for online activity is challenging from a psychological standpoint. According to GDPR and CCPA, children must be 13-16 years old. As a result of the DPDP bill, children up to the age of 18 are included in its scope. Any form of data processing that is likely to harm children is prohibited, including tracking and behavioral monitoring of children. It is possible for the government to prescribe exceptions.

In today's world, it has become increasingly important to protect sensitive personal data. The types of data that fall under this category include DNA samples, healthcare records, and credit card information. However, the current DPDP bill does not recognize the importance of

sensitive personal data. To align with GDPR and CCPA, both of which acknowledge the importance of protecting sensitive personal information, the bill must be revised.

As compared to GDPR and CCPA, the DPDP bill of 2022 restricts the rights of individuals, indicating that a robust framework for enhancing individual rights is needed. Data breaches can be investigated and prosecuted in various ways under GDPR and CCPA, but the DPD bill only proposes one board for investigation and prosecution. This board can, however, be modified to allow for more adaptable enforcement largely determined by the government. The DPDPB 2022 does not specify a time limit for the controller to report a data breach to the DPB, however, other statues mention a time limit for notification. It is therefore important to specify the specific timeframe in the data protection law if a breach occurs.

REFERENCE

- Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).
- *Data Protection Law: An Overview*, Congressional Research Service, R45631 (n.d.).
- Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, Santa Clara Univ. Sch. of L. (July 1, 2020).
- EUROPEAN DATA PROTECTION SUPERVISOR, *Government Access to Data in Third Countries: Final Report*, EDPS/2019/02-13 (2019).
- EUROPEAN DATA PROTECTION SUPERVISOR, *Handbook on European Data Protection Law* (2018).
- G. L. Maffei, *Roman Art*, Harry N. Abrams (2002).
- H. Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32 (2011).
- J. P. Balsdon, *Roman Private Life and Its Survivals*, in *Roman Civilization: Selected Readings* 231 (D. Kagan & G. Viggiano eds., Columbia Univ. Press 1960).
- Jan Holvast, *History of Privacy*, NL - Landseer: Holvast & Partner, Privacy Consultants.
- M. R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31 LAW & CONTEMP. PROBS. 272 (1966).
- M. R. Lefkowitz, *Women's Life in Greece and Rome: A Source Book in Translation*, JHU Press (2020).
- Naomi Rosenbium, *A History of Women Photographers*, Abbeville Press (2010).
- NAT'L INST. FOR TRANSFORMING INDIA, *Data Empowerment and Protection Architecture (DEPA): A Policy Framework for Empowering Residents with Control over their Personal Data* (2020).
- Nicholas III Palmieri, *Data Protection in an Increasingly Globalized World*, 94 IND. L.J. 7 (2019).
- Nikhil Pahwa, *The Problem with India's Proposed Intermediary Liability Rules*, Quartz India (Dec. 28, 2018).
- Paul Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*.
- *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190, 50 S.E. 68 (1905).
- Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
- Shiv Shankar Singh, *Privacy and Data Protection in India: A Critical Assessment*, 53 JSTOR 4 (2011).
- Sjoerd Keulen, *Chapter Title*, in *Handbook Privacy Studies* 21 (Editor's Name ed., Amsterdam Univ. Press).
- Upasana Sharma & Aniket Singhania, *The Personal Data Protection Bill, 2019: An Overview*, Mondaq (Jan. 13, 2020).

- Vijay Pal Dalmia & Rajat Jam, *Compliances by an Intermediary Under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 - Social Media - India*, Mondaq (May 9, 2022).
- William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).
- Woodrow Hartzog & Neil M. Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020).
- WORLD BANK & CGAP, *Data Protection and Privacy for Alternative Data*, GPFI-FCPL Sub-Group Discussion Paper - Draft (May 4, 2018).
- Yashraj Bais, *Privacy and Data Protection in India: An Analysis*, 4 INT'L J.L. MGMT. & HUMAN. (2021).