International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

India's Legislative Framework for Data Protection in the Digital Age: A Comparative Study with EU and US Laws

Sanjay A. Mulik[1], Sachin S. Paralkar[2]

[1]Civil Judge Senior, Division Akola, High of Judicature Bombay
[2]Advocate, At Vadgaon, Maval Bar Association, Dist Pune

Abstract
During the past few decades, technology has grown rapidly around the world, as the internet has become a ubiquitous presence and has broken down geographical boundaries with regards to information flow. As our daily lives become increasingly connected with data, it has become a critical part of our lives. Data plays a vital role in every aspect of our daily lives, from social media to banking to retail. Individuals must have control over their personal data because of this increased interconnectedness, which comes with new and complex privacy challenges. Various sectors in India are being digitized and the digital India program has been launched, making it one of the largest and fastest growing economies in the world. There have been a number of legislations introduced by the Indian government as a reaction to growing concerns about protection of personal data. A major objective of this bill's preamble is to provide a legislative perspective on the protection of individual privacy rights and individual data in an environment which is rapidly growing in digital technology in India. Using data protection law as a case study, this research investigates how efficient it is and how challenging it is to apply. To determine the scope of improvements based on data protection principles, and to assimilate the nature of the different provisions of the law, the dissertation will also compare Indian law with that of the European Union and the United States. Individuals' rights, accountability measures for data processors, and remedies for data breaches include enforcement mechanisms, individual rights, rights for data processors, and cross-border data transfer provisions. We will try to improvise the Indian legal framework in order to gain insight into the grey area where it may have complex issues, as this is a critical issue in this digital age, and countries must take large steps towards resolving it.

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

1. INTRODUCTION

Technology and the internet are being used more and more in India, which is undergoing a digital transformation. Therefore, cyber attacks and data breaches have become more common, making cybersecurity and data protection measures necessary. The Indian internet market is expected to grow rapidly due to its 1.3 billion population and second-largest internet market in the world. As the data protection landscape has expanded, concerns about privacy have arisen and more stringent rules and regulations have been enacted to protect it. The world we live in is changing rapidly, and it has changed dramatically over the past few decades. Modern industrialized societies are dependent on data storage

and information storage due to globalization and international trade. Using low-tech methods for storing data, both public and private organizations routinely collect data, which is no longer just a power or a source of information. Due to the internet's never-ending nature, people have always been concerned about their privacy.

As a result of the new digital environment, we no longer have the right to privacy that we used to take for granted. The Internet has made it easy for the average person to carry out their routine online activities safely, but security breaches have resulted from unanswered questions about privacy and data security. Individuals and organizations are hesitant to disclose their data and information to third parties. Governments designed to regulate how businesses collect, store, and process client information in light of the increased concern about digital privacy in various sectors are passing new laws. It will be very beneficial for all players in this arena if they invest more resources into cybersecurity programs capable of protecting them against both known as well as new attacks. In the development and implementation of data protection laws and regulations, it is becoming increasingly important to strike the right balance between privacy and innovation.

Data breaches are a constant topic of discussion in India. Global Risk Report 2019 published by the WEF World Economic Forum shows that India is the country with the largest data breach. In a report published by the Internet and Mobile Association of India (IAMAI) (IAMAI, 2020), the country's cybersecurity workforce will need 1 million more qualified personnel by 2025 in order to meet the growing demand for digital services and secure data protection. Data protection is also increasingly important because of cyberattacks and breaches nationwide. Because of cyber-attacks in India in 2019, there were over 4 lakh incidents (CERT-In, 2019), a 37% rise from the previous year. Over 1.1 billion Indians' personal information was exposed in the Aadhaar data breach in the same year as the biggest data breach in history (Jain, 2018) due to a security hole in the country's biometric identity system.

The outdated Information Technology (IT) Act 2000 governs data protection laws in India, which is too insufficient to cope with the complexities of the modern digital environment. Academics and industry players have criticized the provisions of the IT Act, 2000 as insufficient, even though the Act was updated in 2008 to add provisions for data protection and cybersecurity. As part of the Indian government's effort to ensure complete data protection for Indian residents, the Personal Data Protection Bill 2019 has not been implemented and the new proposed Digital Personal Data Protection Bill, 2022 has not been passed into law.

Businesses and governmental organizations will have to adhere to the Digital Personal Data Protection Bill 2022, which regulates the way personal data is acquired, stored, processed, and used. According to the Bill, personal data includes information that identifies an individual. Furthermore, it lays out several guidelines on data protection like purpose restriction, minimization of data, and accountability. In order to enforce the Bill's provisions, an independent regulatory organization called the Data Protection Authority (DPA) must be established. There has been a large amount of effort being made in India to reinforce its data security organization. The Digital Personal Data Protection Act, 2022, has the authority to investigate and punish businesses and government organizations. To support data security and privacy in India, the government launched the in 2015. Applied to society and the economy, the Digital India program was launched by the Ministry of Electronics and Information Technology (MeitY) in 2017. There are several data privacy and security measures covered in the program, such as creating safe digital infrastructure, promoting cybersecurity awareness, and facilitating cybersecurity research and development. Furthermore, a number of bodies have been set up by the government of India to oversee

data protection. In terms of data privacy and security, the most renowned organizations are the Data Security Council of India (DSCI) and the Indian Data Protection Authority (IDPA). Data protection policies and legislation are developed by the DSCI in collaboration with the government and other stakeholders, and business data protection advice and certification are provided.

There is no comprehensive data protection law in India; the Digital Personal Data Protection Bill 2022 is the fifth instance of the country's attempt to enact a data protection law.

2. LITERATURE REVIEW

Currently, India, Europe, and the United States have different legal protection frameworks for data protection.

A digital data protection bill for 2022:

It is the ministry responsible for electronic and technological development (MeitY). I In 2022, a bill will be introduced that will protect personal digital data. By highlighting key features and issues in the Digital Data Protection Bill, as well as comparing it with its predecessor, this draft provides a roadmap for the future lawn 2022. A research paper of this type will be of interest to researchers seeking to understand the previous bill and how it might affect data protection under the new bill.

General Data Protection Regulation, 2016/679:

Parliament of the European Union, and Council of the European Union. In 2016. It repeals Directive 95/46/EC (General Data Protection Regulation) on the protection of natural persons regarding the processing of personal data and the free movement of such data. The European Parliament passed Regulation (EU) 2016/679 on 27 April 2016. L 119, p. 1-88, European Union Official Journal.

Defining and protecting privacy and data in India

The article discussed how public servants in the name of "Procedure Established by Law "or" Public Duty are threatening privacy. 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.

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.

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.

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**.**

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

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

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.

India's Digital Personal Data Protection Bill, 2022: How Practical is Consent?

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.

Comments on the Draft Digital Personal Data Protection Bill, 2022 Submissions to the Ministry of Electronics and Information Technology.

This report provided recommendations made by the VDIHI Centre that cover several provisions and important definitions of the Digital Personal Data Protection Bill. The report thoroughly analyses the bill and important concepts such as the definition of data principles, deemed consent, and the application of the act. For research purposes, this report is important to understand the current nature of the provisions and the recommendations provided by the VDIHI Centre.

Shailesh Gandhi, ten instances show how the digital data protection bill will undermine the RTI Act. Scroll. In (2023).

This article discussed the two important provisions of the bill 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) of the Right to information act 2005.

S. Mehrotra, The Digital Personal Data Protection Bill, SSC online (2022).

This article provides a comparison between the relevant provisions of the Digital Personal Data Protection Bill 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.

3. METHOD

The research methodology incorporates the different strategies and procedures for directing an examination. Research is a specialty of logical examination. In other word research is a logical and orderly look for relevant data on a particular point. The rationale behind mulling over research system is that one can know about the technique and method received for accomplishment of the goal of the project.

"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 Personal Data Protection Bill, of 2019, 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.

4. DISCUSSION

COMPARATIVE ANALYSIS

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 of data protection. It was proposed in 2016 and adopted on the 25th of May 2018.	India does not have comprehensive data protection law, but the Recently Prosped Digital Data Protection Bill, 2022 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.
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 number, location data and online identifier, and specific factor to physical, physical, genetic, mental, economic, cultural or social identity.	The bill 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.
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	Bill Processing of data for the lawful purpose and which is not forbidden by law

	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	
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 Bill 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, which means Data Localisation.	DPDPB, 2022 include the provision of cross-border data flow, where the entities require permission to use data.
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.	DPDPB 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	The DPDPB, 2022 Recognise the following rights, • Right to information about personal data • Right to correction

	processing • Right to data portability • Right to be forgotten • Right to object	and erasure of personal data • Right to grievance redressal • Right to Nominate in case of death and incapacity to exercise other rights
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 • Limitation on storage of personal data. However certain grounds have been mentioned that allow the 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	General Obligations • Compliance with the act • Made reasonable effort to ensure data protecion • Implement appropriate technical and organization measure • In case of a breach to notify the Data protection Board • Appoint the Data protecion officer • Provide the effective mechanism to ref=dress the grievances Additional On obligation in Children's case • Obtain parent consent • Undertake processing of personal data • Not monitoring the behavior of children
Consent	Provided that consent is required for the collection and processing of data.	DPDPB, 2022 Requires free, specific, and unambiguous prior consent for the process of data-by-data Fiduciary,

		however, it also mentioned the 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	The Bill 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
Enforcement Agencies	GDPR establishes three enforcement agencies for data regulation- • European Data Protection Board • supervisory authorities • 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-compliance.	DPDPB, 2022 provided the penalty for non-compliance 50 cr, failure to notify the board or non-fullfilment of obligation 200cr, failure of security measure 250cr, and can exceed up to 500 crore rupees.

Analysis Drawn from Comparison

An extensive picture of countries' data protection laws was offered by the comparison of the two laws. Digital personal data protection is India's proposed legislation for the protection of information privacy in the digital world, and the General Data Protection Regulations, of EU which was adopted and put into force in 2016. The comparison clarifies the following details:

- The GDPR contains the protection for sensitive personal data with the convenience of mentioning the definition, whereas the DPDPB, 2022 bill is more of a personal data protection legislation and does not include the protection for sensitive personal data.
- The DPDPB, 2022 lacks a clause relating to that data localization, whereas the GDPR made compliance with data localization a requirement for the companies.
- The GDPR and the DPDPB, 2022 both recognise consent of individuals as one of the legal bases for processing personal data, the latter has introduced the novel concept of 'consent managers.
- The GDPR and the Bill offer new legal bases for handling personal data. A distinguishing feature of the GDPR and the Bill in this regard is that the Bill recognises that a data principal is 'deemed' to have given consent for processing when the data principal voluntarily provides personal data to the data fiduciary and it is reasonably expected that the data principal would provide such personal data. To clarify this provision, the Bill provides an example in which a person who shares their name and mobile number with a restaurant for the purpose of reserving a table is deemed to have given consent to the restaurant (i.e. the data fiduciary) collecting their name and mobile number for the purpose of confirming the reservation.
- The DPDP, 2022 specifies 18 years as the minimum age for children, whereas the GDPR divides the age into two categories, the first of which is 13 years and the second of which is 16 years. The DPDPB, 2022 does not provide a separate set of guidelines for the processing of children's data, whereas the GDPR does.
- The GDPR includes the separate supervisory authority for conducting joint operations with members or staff of the supervisory authorities of other Member States, including joint investigations and joint enforcement measures. The DPDPB, 2022 established the Data Protection Authority as the enforcement agency. However, the GDPR includes three different enforcement agencies as well as the supervisory authority.

USA CCPA California Consumer Privacy Act of 2018 Act and Digital Personal Data Protection Bill, 2022 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	India does not have comprehensive data protection law, but the Recently Prosped Digital Data Protection Bill, 2022 is a set of regulations for data protection, The Proposed legislation has 6 chapters and a total 30 of chapters deal with the collection, regulation, storage, rights, duties, exemption, and penalty.

	protection	
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 dat is processed by individuals for personal and domestic purposes and contained recor existence for 100 years.
Definition of Personal Data	The CCPA defines "Personal Information as the " information that identifies 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	The bill 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.
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	DPDPB, 2022 defines the provision of cross-border data flow, where the entities require permission to use data.

	of more than 50,000 consumers, households, or devices for commercial purposes	
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.	DPDPB 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 consumers- • Right to Delete Personal Information • Right to correct inaccurate personal information • Right to know what personal data is being collected (Right to access personal information) • Right to know What Personal Information is sold, shared, and to whom. • Right to opt out of the sale or sharing of Personal information • Right to Limit the use and disclosure of Personal information • Rights of no Retaliation following opt-out exercise of other rights • Right to Action – to seek actual damages or stator damages in case of company failure to resolve the case.	The DPDPB, 2022 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
DATA FIDUCIARY	• To provide notice in	General Obligations

DUTIES	reasonable form for the collection or use of data • provide notice to consumers at or before data collection • 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.	• Compliance with the act • Made reasonable effort to ensure data protecion • Implement 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 ref=dress the grievances Additional On obligation in Children's case • Obtain parent consent • Underate processing of personal data • Not monitoring the behavior of children

	• 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 profile, insurance coverage, and need for extra coverage.	
CONSENT	CCPA mandates that consent compulsory for the process of data by the business.	DPDPB, 2022 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.
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 Bill 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
ENFORCEMENT AGENCIES	California Attorney General's power to assess a violation of the CCPA	Data Protection Board of India
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 consumer under 16 years old.	provided the penalty of for non-compliance 50 cr, failure to notify the board or non-full filment of obligation 200cr, failure of security measure 250cr, and can exceed up to 500 crore rupees.

Analysis drawn from the comparison

- An extensive picture of countries' data protection laws was offered by the comparison of the two laws. Digital personal data protection is India's proposed legislation for the protection of information privacy in the digital world, and the California Consumer Privacy Act 2018. The comparison clarifies the following details
- Both the CCPA and DPDP Bill are aiming to protect the data privacy of their respective citizens. The two laws require companies to be transparent with their data practices and give individuals control over their personal data. Additionally, both laws have provisions for 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 the seriousness, of these issues being taken by lawmakers. However, the DPDP imposes a high penalty as compared to CCPA
- The DPDP regulates the cross-border flow of data, however, such provision is not shown under the CCPA, it only regulates the data within the US and covers particular business entities.
- Both CCPA and DPDP include the provision related to children’s data collected by the business entities, however, the criteria of the different under the law, where CCPA recognised 13-16 years as children age the DPDP recognised below18 years as the Children age
- In terms of rights granted to individuals the CCPA has the much wider scope the DPDP bill grants the limited number of rights to the data principles as mention earlier in the comparison.
- The CCPA and DPDP bill both made consent mandatory for the process and collection of data even in case of children’s data the consent from the lawful guardian or parents are required, however, the CCPA also recognized the special rights under special circumstance under which the business enties can process the children’s data without the permission.
- CCPA establishes a Consumer Privacy Fund (CPF) in the State Treasury's General Fund. The fund covers the AG's office's and state courts' CCPA-enforcement costs. The CPF will get 20% of any AG civil penalties.

5. CONCLUSIONS

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 create lots of data that can be personal or sensitive. Data protection is a very important issue in India right now. Chapter 2 establishes the origin and

development of privacy and the right to privacy in India Throughout the analysis it is found that privacy has been a crucial aspect of human life that has been highly valued. It lets people have control over their own lives and keep others from interfering. This means they can speak their minds without being judged or punished. As society and technology have changed, the recognition of privacy as a legal right has also evolved. As per Article 21 of the Constitution of India, the right to privacy is recognized as a fundamental right that ensures that no individual shall be deprived of their personal liberty or life. India is a digitally empowered society and a knowledge-based economy. the Aadhaar card initiative has been a big help in improving identification in India. It gives every citizen a unique ID number and is connected to their biometric information. The program has the MyGov platform that allows citizens to take part in governance and offers a safe and confidential means of communication. The Supreme Court of India acknowledged 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. The court noted that the right to privacy encompasses the right to manage one's own personal information. India has acknowledged the significance of data protection and put in place various laws and regulations to ensure the safety of individuals' personal data.

In India, there is no comprehensive law for data protection, A framework for data management that safeguards people's privacy is intended to be established by the Personal Data Protection Bill, 2018, and its updated version, the Personal Data Protection Bill, 2019. The bill defines important words such as consent, data, data fiduciary, data principal, data processor, personal data, sensitive personal data, and transgender status in addition to including rules for consent, data fiduciary relationships, and enforcement. The bill 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 things like access, rectification, and erasure. Certain instances of data processing are exempt from the bill. 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, both the proposed bill failed to convert into the act.

The Digital Personal Data Protection Bill, of 2022 is a law that would control of personal information in India. The bill requires compliance with its requirements, by all organizations managing personal data belonging to Indian people. All organisations that handle personal data, including governmental bodies, for-profit companies, and non-profit groups, are covered by the measure. The lack of data localization guidelines in the law is probably a result of the trend toward data localization. The measure puts precise obligations on data management and stiff fines on businesses that don't appropriately protect customer data. The proposed legislation is consistent with international standards for data privacy and protection, such as the General Data Protection Regulation (GDPR), which emphasizes the significance of gaining individuals' informed consent before collecting and using their personal information.

An important step towards protecting people's privacy is the requirement for the appointment of a Data Protection Officer (DPO). The DPO will manage the organization's data protection policies and procedures and respond to any concerns or questions data principals may have. The right to information ensures accountability and transparency in data processing activities by enabling the data principal to be informed about the collection, processing, and use of their personal data. With a maximum fine of 500 crores, the Board is empowered to impose fines in six main areas under the proposed Data Protection Bill. The Board's ability to conduct investigations is restricted to handling only customer complaints.

6. RECOMMENDATION

The Suggestions are drawn after the examination of the Personal Data Protection Bill 2018 and 2019, as well as the Digital Personal Data Protection Bill 2022. Additionally, a comparative analysis is conducted between the DPDP Bill 2022 and the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). Based on this analysis, the following recommendations are proposed.

Overall, the Digital Personal Data Protection Bill 2022 is a significant step forward in terms of regulating the collection and processing of personal data in the digital sphere. It is intended to give individuals greater control over their personal data and to hold companies accountable for the way they handle and uses that data. The penalty giver under the act is increased as compared with the previous bill and the scope of rights of the data subjects is also given in broad ambit. While the implementation of the bill requires some adjustments, it is ultimately aimed at creating a safer and more secure digital environment for all.

The DPDP bill of 2022 requires a revision of the definition of personal data. This is because the previous bill, as well as the GDPR and CCPA, have provided a comprehensive definition of personal data that specifically outlines the types of information that fall under this category. Data localization is a concept that is gaining popularity, as it allows countries to have complete control over their data. The General Data Protection Regulation (GDPR) includes provisions for data localization, which can be adopted by India to effectively monitor data within the country.

The impact of the internet on children is a growing concern, as determining the appropriate age for online activity is complex from a psychological perspective. both GDPR and CCPA have set the age range for children at 13-16 years old. The DPDP bill has expanded the scope by including children up to the age of 18. Which prohibits the tracking and behavioral monitoring of children, targeted advertising directed at children, and any form of data processing likely to cause harm to children. Exceptions may be prescribed by the government.

The protection of sensitive personal data has become increasingly important in today's world. This type of data includes information such as DNA samples, healthcare records, and credit card information. However, the current DPDP bill does not recognize the significance of sensitive personal data. Therefore, it is necessary to revise the bill to align with the GDPR and CCPA, which both acknowledge the importance of protecting sensitive personal data.

The DPDP bill of 2022 restricts the rights of individuals in comparison to the GDPR and CCPA, indicating a need to review these rights to establish a robust framework for individual rights expansion.

The GDPR and CCPA offer various methods of enforcement, while the DPD bill only presents a single board for investigating and prosecuting data breaches appointed by the government. However, this board can be modified to allow for more adaptable enforcement largely be dictated by the government.

Time is crucial in the data breach the DPDPB 2022 does not have specific time for the controller to the DPB in case of a breach, however, the other statues have mentioned the time limit for the notification of data breach. Therefore, the data protecion law need to be mentioned the specific time in case of breach.

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 Handbook 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