INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

PROTECTING PRIVACY IN THE DIGITAL AGE: A COMPARATIVE ANALYSIS OF INDIAN AND U.S. DATA PRIVACY LEGISLATION

AUTHORED BY - MD SHADMAN NOMANI

ABSTRACT

This is an era of Artificial Intelligence (AI) driven technological advancement which is very much intertwined with human being. It impacts us both positively and negatively. AI has raises many concerning issues but issue of Individual data privacy is of utmost importance. Intrusion into it by corporate and State has badly affect the Individual privacy and can be seen in socio-political arena of citizens residing in a country. This Research Paper has done comprehensive comparative study of specific data privacy legislation in two significant jurisdictions namely India and United States of America. In India Right to privacy is recognised as a Fundamental right by the Supreme Court. But the new Digital Personal Data Protection Act 2023 gives enormous power to the Government. The way the personal data is gathered by government and exemption given to certain class of companies and start-up would results in enormous control over the ordinary Indian citizens which without proper regulation would be unethical to a democratic framework and contrary to Right to Privacy judgement. Similarly in USA, individual privacy has been given importance since the Bill of right was passed in 1791. Due to its federal structures, different state having different privacy laws providing safety to only those people who reside there. In this paper the researcher critically analyse the first, strictest and comprehensive privacy law i.e. California consumer Privacy Act (CCPA). Thus the researcher sheds light on the evolving landscape of data protection in these distinct but interconnected nations by covering historical developments, important provision, regulatory processes, enforcement methods and challenges faced by it and Suggest for its improvements as right to privacy is linked to all our Fundamental Rights.

Keywords: *Right to Privacy, Digital Personal Data Protection Act 2023, California consumer Privacy Act*

ISSN: 2582-6433

CHAPTER: - I

INTRODUCTION

This era in which we are living in is an era of fast growing technological advancement. From technology what we really mean here is specifically data(personal Information) driven technology like mobile technology, social media and Artificial Intelligence which rapidly become so much intertwined with us that it affect the social and political life. These technology has affect us both positively and negatively, on one hand it makes us well informed, expand human capabilities and increase productivity but on the other hand in some way or other it create echo chamber, addiction, lack of attention span and intrusion in individual privacy.

The concerns of privacy are paramount in the sphere of technology. Supreme court of India recognized Privacy Right as Fundamental Right as extension of right under Article 21. But Privacy breach and Intrusion into Privacy by corporate and States are issues of immediate concern all around the globe. Social media are accused of stealing and processing Individuals' privacy for making them a commodity. In this background the safeguarding of individual data privacy has emerged as a paramount concern. There is a greater need than ever for strong legal frameworks to protect personal information as people and companies manage the complexities of an increasingly linked world.

In India the journey of Right to Privacy is recognized in Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. The nine judge Bench unanimously held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution". The court also in its Obiter dicta gives a need for a new law relating to data Privacy. The need was also felt by the legislature and new Data privacy law were come into force namely Digital Private Data Protection Act 2023. The researcher critically analyse the DPDP Act to understand the Data Privacy Regulation in India.

Similarly, in USA the discussion About Individual privacy was more or less started in Bill of Rights in 1791 and The Privacy Act of 1974. But unlike EU which has comprehensive data privacy laws known as General Data Protection Regulation (GDPR). There isn't a single statute in the US that protects the privacy of all kinds of data. Instead, it consists of a patchwork of statutes known by acronyms such as, VPPA, FERPA, GLBA, HIPAA ECPA, FCRA, and COPPA, which are intended to target certain categories of data under particular conditions.. Different types of data privacy, such as health data, financial information, or data gathered from children, are covered by separate federal and state regulations in the United States. Although certain state in the US have distinct comprehensive consumer privacy laws like California (CCPA and its amendment, CPRA), in

ISSN: 2582-6433

Virginia (VCDPA), and in Colorado (ColoPA) which guarantee protection for the individuals living in those state. Though it is not possible to analyse each statute in detail in this paper, so the researcher has only gives a bird eye view of above mentioned statute to understand the historical journey, and analyse in detail the first, strictest and most comprehensive privacy law i.e. CCPA and its amendment, CPRA in detail to understand the contemporary trend in US data privacy laws.

Thus this Research Paper embarks on a comprehensive comparative study of data privacy laws in two significant jurisdictions – India and the United States of America. The analysis encompasses historical developments, key provisions, regulatory mechanisms, enforcement practices, challenges, and recommendations, shedding light on the evolving landscape of data protection in these diverse yet interconnected societies. This research paper focused on the individual data privacy laws of India and the USA, exploring the evolution, scope, and effectiveness of their respective frameworks.

AIMS AND OBJECTIVE OF RESEARCH

- To understand the historical development of data privacy laws in India and the USA.
- To analyze the key provisions and principles governing individual data protection in both countries.
- To compare the enforcement mechanisms and regulatory bodies overseeing data privacy.
- To identify challenges and potential areas for improvement in the existing frameworks.

HYPOTHESES

1) Lack of adequate regulatory mechanism of Individual Data Privacy would result in abuse of power by the State.
2) By giving free hand over Individual Data to Big Tech companies would endanger democratic framework, civic freedom and turn citizens into a commodity.

ISSN: 2582-6433

CHAPTER: - II

HISTORICAL EVOLUTION OF PRIVACY LAWS

The aetiology of privacy laws is the results of an effort to secure the privacy, integrity and autonomy, of individuals in a democratic society. Technological advancement that has been going on is so massive and fast that classical laws and their amendments doesn't able to fulfil the gap, thus privacy laws creates a bridge between the classical notion of laws and technology. According to bygrave[1] there are mainly three reasons for evolution of privacy laws. They are as under:-

1) Technological and organisational developments: Through these inventions especially in Information and Communication Technology has made handling of big amount of Data very simple and government efforts to consolidate data for increasing efficiency, to control and to provide service (e.g. census). But circulation, use and re-use of data for some other purposes than those for which it firstly collected would raise issues of misinterpretation and misrepresentation of data. Now the development and use of automated learning in the form of machine learning has raises major concern and leads to its developments.

2) Fear regarding these developments: If it is kept unchecked, will subvert the very pillars of democratic and pluralistic society. And this resulted in autocracy which destabilizes the political due process of law. These thing are getting popularity through dystopian literature like Orwell's Nineteen Eighty-Four and A clockwork orange by Anthony burgess etc. the other fear is economic in nature as in the absence of data privacy laws, consumer would merely become a commodity in the hands of economic giant. Thus to overcome it and to gain public trust, data protection laws regime has started.

Legal factors: Absent perceived shortcomings in the capacity of pre-existing laws to effectively address the issues originating from concern discussed above, data privacy legislation would not have been established. Pre-existing laws were thought to exacerbate these issues to some degree. For example, with the advent of computerization, Sweden's long-standing, liberal, and legally entrenched freedom of information (FOI) system was seen to provide special privacy risks. Although pre-existing laws has paved the way for privacy laws by giving normative foundation and source of inspiration for it especially from Rule of law, natural justice doctrine, human rights and property law.

Thus the above mentioned three reasons has more or less led to the development of privacy

[1] LEE A BYGRAVE, DATA PRIVACY LAW AN INTERNATIONAL PERSPECTIVE 9-13(Oxford University Press,2014)

ISSN: 2582-6433

legislation all around the globe, so its impact can be seen in India and USA also follow the same track.

HISTORICAL TRAJECTORY IN INDIA

In India the journey of Right to Privacy was started from the case of M.P. Sharma & Ors. vs. Satish Chandra and Ors[2],and this issue was raised in Kharak singh v s. State of Uttar Pradesh[3] case in the later one the Indian Supreme Court ruled that the relevant sections permitting police to conduct domiciliary visits to "habitual criminals" or those who are prone to develop a criminal habit were unconstitutional. Kharak Singh (Plaintiff) was many times awakened from his sleep by the police officer when they would visit his place of residence at night. The petitioner's right to life may only be regulated by legislation, and not by executive directives like the Uttar Pradesh Police Regulations, the court reasoned, and the visits violated that right. *The petitioner claimed that his privacy was violated due to frequent visit, but the Court dismissed the argument and by strict interpretation of the Indian Constitution it says that constitution did not recognize privacy as a fundamental right*.

But in Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors[4]. The 9 judge Bench unanimously held that "right to privacy is protected and it is a part of the right to life and personal liberty enshrined under Article 21 and also as a freedoms guaranteed by Part III of the Indian Constitution". By this it overruled previous judgments of the SC in Kharak Singh, as the latter held that the privacy as a right was not recognised or protected under the Indian Constitution.
The court also in its Obiter dicta gives a need for a contemporary law relating to data Privacy.

Also, the pre-existing laws have been proved insufficient to address the dynamic and fast growing data driven technology. "The Information Technology Act 2000 and IT (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 SPDI Rules" were not able to address the issue completely. So from 2018 onward there have been efforts to legislate a stand-alone Data Protection Law to fill the lacunas. The Government have came up with a multiple draft between 2018 to 2021 but these Bill was Scrapped and Finally The Digital Personal Data Protection Bill, 2023 was introduce in Lok Sabha on Aug.3rd , 2023 and published in the official

[2] M.P. Sharma & Ors. v. Satish Chandra and Ors, (1954) 1 SCR 1077.
[3] Kharak singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[4]Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, (2017) 10 SCC 1, AIR 2017 SC 4161

ISSN: 2582-6433

gazette on 11th Aug. 2023[5] and become law of the land. The reason for the enactment is to "provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto".

HISTORICAL TRAJECTORY IN UNITED STATE OF AMERICA

In US the discussion About Individual privacy was more or less started in Bill of Rights in 1791 in which 4th Amendment talks About "Right of people to be secure in persons...., against unreasonable searches and seizure. Furthermore The Privacy Act of 1974 sets forth guidelines for federal agencies' collection and use of personal data inside its record-keeping system. There isn't a single statute in the US that protects the privacy of all kinds of data. Rather, it contains a combination of laws like

HIPAA ("Health Insurance Portability and Accountability Act") that provides data privacy and security provisions for safeguarding medical information.

FCRA (The Fair Credit Reporting Act)-1970, that controls the gathering of consumer credit data and the availability of credit reports, ensuring the privacy, accuracy, and justice of the personal data kept in the credit reporting companies' files.

FERPA ("The Family Educational Rights and Privacy Act")-1974, that protects the privacy of student educational records.

GLBA ("Gramm-Leach-Bliley Act")-1999, that reform the financial services industry, and addressed concerns relating to consumer financial privacy. Similarly, ECPA, COPPA, and VPPA also intended to target only specific types of data to deal with special circumstances.

Although some state in the United State of America have distinct comprehensive consumer privacy laws, but California always stand at the forefront in the arena of Privacy legislation. The right to privacy was added to the list of "inalienable" rights for all persons in 1972 when the California Constitution was revised. The California Legislature passed a law in 2002 requiring businesses that electronically retain customer data to notify their clients in California of any security breach of their computer system if the business knows or has reasonable suspicion that the client's unencrypted data has been compromised. The California Legislature passed many legislation pertaining to privacy between 2002 and 2017, such as the "California Data Breach Notification Law, the Online Privacy Protection Act", "the Shine the Light Law" and "Privacy Rights for California Minors in

[5] The Digital Private Data Protection Act, 2023, § 1, No.22, Acts of Parliament, 2023(India)

ISSN: 2582-6433

the Digital World"[6]. This legacy has been continued and California was the first state in the USA who enacted comprehensive California Consumer Protection Act of 2018.

Following the same track many states of USA also came up with Data privacy legislation similar to California privacy regulation[7].

[6] Yunge Li, The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth?, 32 LOY. CONSUMER L. REV. 177 (2019).

[7]The International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited Mar.21,2024)

ISSN: 2582-6433

CHAPTER: - III

COMPARATIVE ANALYSIS OF KEY PROVISIONS IN DPDPA AND CCPA

The comparison between the "California Consumer Privacy Act" (CCPA) and India's Data Protection and Privacy Act (DPDPA) in detail, covering various aspects such as scope, rights of individuals, data processing principles, cross-border data flow, enforcement mechanisms, and the role of data protection authorities etc. are discussed below.

1) SCOPE AND APPLICABILITY OF THE ACTS.

The Data Protection Act is applicable to the extracting and filtering of digital personal data, both inside and beyond territorial limit of India, provided that this is to support any activity involving the provision of offering services to Data Principals within India. However, Digital Private Data Protection Act doesn't address the processing of personal data of data principle situated beyond India.

Whereas CCPA[8] is applicable on any for-profit company handling "personal information" on a customer that meets minimum one of the following requirements is subject to the CCPA:(1) has the personal data of at least fifty thousand households, customers, or devices; (2) generates more than half of its yearly income from the sale of consumers' personal information; or (3) has gross sales exceeding $25 million annually. Businesses who haven't a physical location in California but have a online website that caters services to Californians are required to adhere.

2) LANGUAGE AND STRUCTURE OF THE ACT

Considering its scope and technical nature of the subject, Digital Private Data Protection Act, language and structure is more simple in comparison to CCPA to facilitate a clear understanding of all the sections. It establishes out different definitions, including those for gain, loss, harm, data processors, data fiduciary and data principal, etc. These definitions aid in providing a thorough grasp of the character and extent of the Act's provisions.

[8] CALIFORNIA LEGISLATIVE INFORMATION, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375 (last visited Mar. 22, 2024)

ISSN: 2582-6433

3) RIGHT GRANTED TO INDIVIDUALS

Under the Digital Private Data Protection Act, specific **rights of data principals**[9] are as follows:

(i) Right to Information about Personal Data: data principals shall have the right to know a gist of the personal information processed, the name of companies with whom their personal data has been shared, and the types of personal data shared.

(ii) Right to Correction and withdraw consent: The data fiduciary is required to update and modify the data as requested. Data principals can request that their personal data processed by a data fiduciary be corrected, completed, updated, or erased; deletion can be refused if retention is mandated by law.

(iii) The Right to File a Grievance: Data principals are entitled to easily accessible channels for grievance redress from data fiduciaries regarding any action or inaction on their part with regard to fulfilling their duties concerning the data principal's personal information or exercising her/his rights.

(iv) Right to Nominate: This right cannot be seen in any Privacy legislation including GDPR , so it is a **unique right available to Data Principal** that they can nominate a person to exercise his rights upon their demise or incapacity and prevent it from making it available in public domain.

Under **California Consumer Protection Act gives** the following **five rights**[10] of California consumers:

i) **Right to know**[11]: Under the CCPA, businesses shall have to reveal, at or before collection, the types of personal information they collect and the actual purposes for which the personal information may be used. It includes the right to know, what are the personal information (PI) that the business has disclosed or sold, and to whom such information is disclosed or sold.

ii) **Right to Access**[12]: The company is required to provide the following information upon a verifiable consumer request: (1) the Personal Information, which company has gathered about the consumer; (2) the class of personal information the firms or business has gathered or sold about that customer; (3) the reason(s) for the collection or sale of the categories of personal information; and (4) the information about the third parties to whom the company has sold the personal information. The types of personal data that the company sells to outside parties have to be disclosed as well.

---

[9] *Id*. at 5, §.11-14
[10] CAL. CIV. CODE § 1798.100. (2018)
[11] *Id*. § 1798.100
[12] *Id.* §§ 1798.110,115

ISSN: 2582-6433

iii) **Right to Delete**[13]: Customers have the right to request that any personal data they may have provided to a business be deleted. Companies covered by the Act must let the customer know that she has the option to delete. The company must remove the information from its records and instruct any service providers to do the same upon a genuine customer request.

iv) **The right to say no to the sale of personal information**[14]: The California Consumer Protection Act gives consumers the" right to opt out of a business", or sale of its Personal Information and restricts the business from inquiring them to change that decision for at least twelve months. It is mandatory for businesses to display a "Do Not Sell My Personal Information" button to alert customers of their right to opt-out and give them a way to do so. Additionally, before selling their Personal Information, firms must formally seek authorization from consumers between the ages of thirteen and sixteen as well as parental approval from youngsters under the age of thirteen. Companies may also reward customers for the use of personal data by offering "financial incentives" on an opt-in basis; however, this is only allowed if these financial incentives are not "unjust, unreasonable, coercive, or illicit in nature" i.e. they follow rule of law principle.

v) **The right to equal service and price, even if privacy rights are invoked**[15]: The California Consumer Protection Act does not permit a business to differentiate among consumer just because the consumer has avail any of the rights set forth in the provision of the Act, that means they do not deny goods and services, nor charge different price or rates for good and not provide different level or quality of goods who do not provide personal information.

4) DATA PROCESSING PRINCIPLE

The CCPA outlines several data processing principles that businesses must abide to, including transparency principles, purpose, limitation, data minimization, security safeguards, and accountability. Similarly, DPDPA lays down principles similar to CCPA, comprising legality, equity, and openness; purpose restriction; data reduction; precision; storage restriction; integrity, secrecy; and accountability.. Thus, both the Act gives guiding principles, offer a strong basis for processing data in an ethical and responsible manner. It lays down the norms and processes that must be followed, clearly establishing accountability towards individuals in control of personal data.

5) DATA TRANSFERS AND CROSS-BORDER DATA FLOW

[13] *Id.* § 1798.105
[14] *Id*. § 1798.120
[15] *Id.* § 1798.125

ISSN: 2582-6433

Unlike GDPR, CCPA does not specifically restrict or address cross-border data transfers, but imposes obligations on businesses to disclose if they sell personal information to third parties, including those outside of California[16].

Whereas under Digital Private Data Protection Act can transfer data outside India, but on certain Information restrictions can be imposed by the Board on cross-border data transfers, stating that sensitive personal data must be kept and processed only within Indian territorial jurisdiction unless certain conditions or exemptions apply[17].

6) ENFORCEMENT MECHANISM

India's Digital Private Data Protection Act establishes a Data Protection Board of India (DPBI) responsible for monitoring compliance, enforcement, providing guidance, and resolving disputes related to data privacy. The Act was intended to establish the Data Protection Board of India the previously proposed Independent Authority; however, there have been numerous discussions regarding the board's independence; it is now known that the central government has significant control over the board, over its operations and formation. As a result, many people are concerned that the central government would have broad authority that will resemble a surveillance state[18].

Also, Enforcement of the CCPA primarily falls under the jurisdiction of the California Attorney General, who has the power to impose penalties for non-adherence, including fines for violations, but AG and its board members were appointed the Governor, an executive head. Thus it has similar limitation as that of Digital Private Data Protection Act.

7) PENALTIES FOR NON-COMPLIANCE

Under California Consumer Privacy Act, Privacy breaches not rectify under less than 30 days after notice were served to the company, then the California Attorney General may charge statutory penalties “up to $7,500 for purposeful violations and up to $2,500 for inadvertent violations”. The California Consumer Privacy Act also gives customers to some extent a **private right of action** in the event that a business violates their obligation to maintain and implement a reasonable security procedures and practices, allowing unauthorized access, exfiltration, theft, or disclosure of some of their personal information.

---

[16] *Supra*. at 8

[17] *Id.* at 5 § 16

[18] Ashneet Hanspal , *India: Analysis of The Digital Personal Data Protection Act, 2022*, (Mondaq, 4 January 2023) https:/ /www.mondag.com/india/data-protection/1267190/analysis-of-the-digital-personal-dataprotection-Act-2022, accessed , Feb.26, 2024

ISSN: 2582-6433

Whereas under the maximum penalty up to 250 crore Rupees can be imposed for non compliance on data principals, Data fiduciaries, significant Data fiduciaries and consent Managers. It has adopted a layered Penalty mechanism from severe data breaches to violation of rules of the Act (50 crore)[19]. The Act has also **imposed penalties of INR 10000 on Data principal** for non-fulfilment of duties which has no reference point in any of the Data protection Statute. Duties can be imposed but the penalties on Data principal for breach of duties while exercising rights or suppress any material information while providing data due to any reason is against the very purpose of the Act i.e. the right of Individual to protect their personal data.

8) EXEMPTION PROVISIONS

The California consumer Privacy Act enumerates a number of exemptions, such as (1) Adhere to national, state, and local laws; (2) Fulfil civil, criminal, and regulatory requests or procedures; and (3) Assist law enforcement. Also the amendments in Sept. 2018 remove wording that restricted these exemptions to circumstances in which the laws clashed with the California consumer Privacy Act (CCPA), so expanding the exemptions for data acquired, processed, sold, or revealed in accordance with the "Gramm-Leach-Bliley Act" and the "Driver's Privacy Protection Act" . Consequently, information protected by these statutes is no longer subject to the California consumer Privacy Act. The amendments also broaden or add exemptions pertaining to protected medical trial data, the applicability of the provision to health service providers in specific circumstances, and an exemption for data processed, sold, collected, or disclosed in accordance with the "California Information Privacy Act".

Whereas under Digital Private Data Protection Act the exemptions[20] under the title of "certain legitimate uses" is similar to California consumer Privacy Act like in matter of medical treatment or emergency, compliance with judgements, and law enforcement etc. However, other exemptions were so expansive that they watered down the very consent of the Data Principal, which is a crucial component of the legislation, and gave the Central government the authority to grant exemption for a specific period of time to certain class of data fiduciaries, start-ups, and employers over their employees.. It would be unethical to a democratic framework and contrary to Right to Privacy judgement.

[19] *Id*. at 5 § 33(1)
[20] Id. at 5 § 7

ISSN: 2582-6433

CHAPTER: - IV

CONCLUSION AND SUGGESTIONS

As has been discussed in great depth previously, there is space for improvement in both the Statute to address a variety of problems and accomplish the intended goals. The fundamental distinction between US and European regulatory approaches to data privacy is highlighted by Kirby's conclusions here: in general, "US regulations are less stringent than European ones. Thus, US law allows for a more market-centric approach while drafting national data privacy laws"[21].

Also, India's Privacy law is more tilted toward US as compared to the European GDPR Both the Act lists certain rights related to privacy. These laws, which give citizens larger authority on their personal data, lessen the knowledge and power disparity that exists between people and corporations. People gain from this, but society as a whole also gains from it. A democracy, which acknowledges and relies on the sovereignty of the people who make it up, is especially dependent on the ability of individuals to enjoy their right to privacy.

Also, not everything in the DPDP Act is as it seems, despite acclaim for its capability to act as a stand-alone data protection framework. The fact that the Central Government still has the power to take decision on many important clauses in the Digital Private Data Protection Act raises concerns. This feature brings up pragmatic concern about the possibility of despotic and unrestrained rule-making, which may leads in ambiguities and possible loopholes in the regulatory system. Furthermore, it is arbitrary that the Digital Private Data Protection Act places obligations on data principals for a piece of legislation meant to actually safeguard their rights.

In conclusion, both the Act marks a critical turning point in their respective nation and gives benchmark and act as a lighthouse in their respective subcontinent in attempts to create a thorough legal framework for safeguarding private information. The aforementioned recommendations would be very beneficial in boosting the legislation's efficacy. In addition to defending people's right to privacy, a well-balanced and well-crafted data protection law would encourage corporate innovation and trust, which would help later in the global digital economy.

Lastly, the researcher has made some suggestion for the improvement and getting insight from the comparative analysis of the Statute in both countries. They are as follows

[21]LEE A BYGRAVE, *Supra* note 1,at 110

ISSN: 2582-6433

SUGGESTIONS

1) Available rights and its impact is mainly depend on awareness and how simple it is for consumers or Data Principle to know and exercise their rights in time of their dire need.
2) Effective compliance mechanism is lacking in CCPA, which need to be enumerated and Data Protection Impact Assessment as in DPDPA at least from significant data fiduciaries within a certain span of time can be a better option.
3) There is no comprehensive guideline expressing how the training should be done and should be implemented in both the statute which must be consider while making rules.
4) There is need of a balance between Cost-Benefit approach and Risk-Based approach, so that the tech giant cannot overlook legislative compliance as the cost of compliance is higher than penalty and sacrifice citizens Privacy over business interest.
5) There is also a need to look how and where the data of personal information is accumulated and it is mandatory for Data Fiduciaries to store data within the territorial boundary, so that it is easier to sue them.
6) Enforcement agency like DPBI and CAG must be made an independent body free from executive interference, so that coercive action can't work and privacy of Individual is ascertained which is necessary for a healthy Democracy.

BIBLIOGRAPHY

BOOKS

1) Lee A Bygrave, Data Privacy Law An International Perspective (Oxford University Press,2014)
2) Jamie Bartlett, The People vs Tech: How the internet is killing Democracy and how we can save it (Ebury Press,2018)
3) Data Protection in a Profiled World (Springer,2010)
4) Jamie susskind, Future Politics(Oxford University Press,2018)

STATUTE

1)Constitution of India,1949
2) Constitution of United State of America
3) The Digital Private Data Protection Act, 2023, § 1, No.22, Acts of Parliament, 2023(India)
4)CAL. CIV. CODE § 1798.100. (2018)

ISSN: 2582-6433

5) Information Technology Act,2000

CASE LAWS

M.P. Sharma & Ors. v. Satish Chandra and Ors, (1954) 1 SCR 1077.

Kharak singh v. State of Uttar Pradesh, AIR 1963 SC 1295

Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, (2017) 10 SCC 1, AIR 2017 SC 4161

RESEARCH PAPER

Yunge Li, The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth?, 32 LOY. CONSUMER L. REV. 177 (2019).

Khilansha Mukhija & Shreyas Jaiswal, Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR, 4 JUS CORPUS L.J. [638] (2023

WEBSITE AND URL

1) The International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker

2)California Legislative Information, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

3) Ashneet Hanspal , India: Analysis of The Digital Personal Data Protection Act, 2022, (Mondaq, 4 January 2023) https:/ /www.mondag.com/india/data-protection/1267190/analysis-of-the-digital-personal-dataprotection-Act-2022,