INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

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

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

 ISSN: 2582-6433

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.

 ISSN: 2582-6433

DATA PROTECTION IN THE ERA OF BIG DATA: A CRITICAL EVALUATION OF LEGISLATIVE SAFEGUARDS

AUTHORED BY - MS. SHIVANGI GUPTA[1]
Assistant Professor
Department of Law
United University, Prayagraj

ABSTRACT

Data privacy refers to the branch of data security concern with proper handling of one's data- which includes one's consent, notice and regulatory obligation. Information technology advancement have Highlighted concerns about data privacy and its impacts, and have motivated researchers to explore data privacy issues, including technical solutions as well as legal requirements to address these concerns. In this research paper, we apprise researchers about the present state of data privacy research. Recent analysis disclosed that concept data privacy is a having more than one level, but rarely studied as such and existing personal data protection bill doesn't have an extra territorial jurisdiction. Research on data privacy focuses on elaborating and predicting theoretical contributions, with few studies in journal articles focusing on design and action contributions. We advise that forthcoming research should contemplate diverse levels of analysis as well as multilevel effects of data privacy. We illustrate this with a different level of framework for data privacy concerns. There is a necessity to modify the present personal data protection bill in India so that it also there is a need of legislation keeping in view continuous technological advancement how important is to address the issue of Information privacy but many of them fails to take account of short coming in the proposed Bill, even those who oppose the law fail to specify the provisions that need to be changed or amended, and they fail to compare the bill to previous bills, such as the Data Protection Bill of 2018, Bill 2019 and now the current 2023 Bill removes the better provisions of the 2021 Bill. So, the present study focus on the areas of Bill which was less studied and need our attention.

KEYWORDS: Data Privacy, Information Technology, Data Breach, Level Of Analysis

 ISSN: 2582-6433

1. INTRODUCTION

[1] As a result of recent disclosures regarding Cambridge Analytica, WhatsApp, Facebook privacy sharing agreements, Apple-FBI conflicts, and the Snowden revelations, headlines are rife with worries about how personal information is shared. An important public policy question is how to balance the advantages of big data with the concerns of privacy infringement while using big data analytics. [2]According to some of these concerns, governments throughout the world have revisited their privacy laws and implemented extra safeguards It is time for a new standard of data protection in Europe to address today's privacy and contemporary technology issues, and the EU has adopted Regulation (EU) 2016/679 (GDPR). Data from European Union citizens held in the United States will be protected under the new Privacy Shield agreement, which the United States and Europe agreed upon in 2016 as a framework for data transfer[3]. Many studies on big data and privacy were commissioned by the Obama administration, and a slew of consumer privacy protections were implemented in the United States[4]. Two years after the reference in 2015, a court with nine judges Article 21 and other liberties granted by Part III of the Constitution are safeguarded by the right to privacy, a Supreme Court of India panel unanimously concluded.

[5] Article 21 of Constitution of India that guarantees citizen Right to Life also guarantees right to privacy, and governs both government and private intrusions. Technology improvements have led to the collection of enormous quantities of personal data about Indian citizens by several national and foreign businesses, websites, and applications. It is the responsibility of each individual to ensure that his or her personal information is protected against unauthorized access and use. This includes everything from a person's personal interests, habits, and activities to his or her familial, educational, and financial information. Data about a person that is incomplete, inaccurate, or misleading and that can be easily sent to an untrusted third party at a low cost and speed is dangerous because it has the potential to do harm. Many benefits may be gained from the greater use of personal data, but there are also a number of risks. Advances

---

1 Vrinda Bhandari and Renuka Sane, *Protecting Citizen FromThe State Post Puttaswamy: Analysing The PrivacyImplication of the Justice Srikrishna Committe Report* and The Data Protection bill 2018, *Review,* 15, 2145-169(2018).

2 Omer Tene and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63-69 (2012)

3 This agreement superseded the 16-year-old Safe Harbour Agreement, which was invalidated in October 2015 after Snowden's disclosures regarding the NSA's monitoring practices by the European Court of Justice in Maximillian Schrems v. Data Protection Commr., Case C-362/14 (2015).

4 The 2017 Consumer Privacy Protection Act (H.R. 4081) was proposed in the US Congress. The Consumer Privacy Bill of Rights Act was unveiled by the Obama administration in 2015 as a draft Bill.

5 Shiv Shankar Singh, *Privacy and the data protection in India: A critical Assessment*, 53Yale,663-8(2011)

 ISSN: 2582-6433

in technology also have a role. The emergence of new technologies has spawned new concerns about the preservation of individual privacy and the security of personal data. Technological advancements have made it possible to effortlessly access and share personal data. Conflicts between individual privacy and the need to safeguard personal information abound as a result. Individuals and organizations must be safeguarded so that their privacy rights are not breached in cases like the AADHAR Card problem of 2018, when the information of Indians were put at risk and the source of leakage was being probed. There is a critical need to tackle these concerns. Additional attention is drawn to the BHIM wallet app websites where PAN and bank details are stored. The IT sector in Germany and France, the EU's two largest members, is expected to be worth between €155 and €220 billion. The Government of India enacted the [6]Personal Data Protection Act 2023 because of the urgent need for data privacy legislation.

The Data Protection Bill, as a piece of legislation, should be able to find a balance between promoting creativity and productivity and protecting people's privacy rights. Data Protection Bill, 2021 legislation was analyze from the angle that whether it maintains the balance in the present research. This report shows how the law fails in Indian data economy privacy-related concerns. Because personal data is become public property and given more state powers by this statute, it acts as a weapon for government involvement in people's privacy. [2]This will also result in rise of compliance costs for businesses in India market. The paper asserts that although preserving personal information is a priority, laws governing its protection must be more precisely drafted to guarantee individuals' legitimate rights to privacy without impeding a nation's ability to grow and develop.[2]This paper examines [7]"Privacy" jurisprudence of India going to older times long back. It mostly focus on harm of invasion of privacy. The jurisprudence of privacy changed in the year 2017, after the judgement of[8] Justice K.S.Puttaswamy v. Union of India the apex court held that the Constitution of India includes a fundamental right to privacy.[9] When the judges were examining the case[10], they gave various

6 The Personal Data Protection Bill, 2019, No 373, Act of Parliament,2019(India)

7 Richard Parker, *A Defination of Privacy*, 27 RUTGERS L.R. 275 (2001)

8 Justice K. S. Puttaswamy (Retd.) v. Union Of India (2017) 10 SCC 1; AIR 2017 SC 4161

9 Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth*?, Carnegie India (Mar 9,2022,9:29 PM) https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217

10 Six different views made up the ruling, with Justice Chandrachud writing the majority opinion—which was also the longest—on behalf of Chief Justice Khehar, Justice Nazeer, and Justice Agrawal. This decision, which was signed by just four judges, does not, however, represent the view of the majority and, unexpectedly, does not make reference to any of the concurring opinions of the other judges. Justice Chelameswar, Justice Bobde, Justice Nariman, Justice Sapre, and Justice Kaul have all issued further concurring opinions.

 ISSN: 2582-6433

development of [11]privacy jurisprudence, the main lacuna in the present jurisprudence is the lack of a "doctrinal formulation" that could help decide whether privacy is protected constitutionally or not. As a result, privacy law has shifted from being valued as a right that protects other interests to being prized as a goal and end in itself. [12] while giving the verdict in the Puttaswamy judgment Judges held the right to privacy as a fundamental right under right 21. But in this paper we will show the different view was adopted in the bill from the judgement. In the bill it was aimed at with the requirement that effective control of data usage by private players is necessary to ensure a person's informational privacy. According to its name, the measure aims to regulate the use of data. As a technological effort requiring correct mechanisms, this is no small undertaking. Data economy will be harmed, data rights as an intangible property are weakened, and state surveillance powers will be strengthened under the measure. Innovation and technological growth will be hampered, and the goal of safeguarding individual privacy will not be met as a result. This article provides a summary of the important incidents that have necessitated data protection laws. It puts the legislation in context and queries the Definition of privacy in the KS Puttaswamy[13] against Union of India judgement as part of India's larger discussion about privacy rights.[14]

A new concept of privacy has been proposed, but there is no clear legislative framework to address market failures in the digital economy, according to this research. [15] According to this report, the measure should be drastically reworked for three main reasons: In light of current technology improvements, a vast body of academic research shows that more disclosure requirements for consumers about the usage of their data are ineffectual. [16]This might lead to people assuming less responsibility for providing their data if these systems are relied upon. Then there's the preventative measure. Second, the preventative framework suggested by the law might lead to substantial compliance costs for private companies. The law sets substantial new compliance duties on the overwhelming majority of companies engaged and governs the use of data in every sector of the economy. For the most part, the costs of compliance will be

[11] Privacy serves both a normative and a descriptive purpose, according to Justice Chandrachud, para. 322 of his decision. On a normative level, privacy upholds the tenets that have stood the test of time and maintain the safeguards for life, liberty, and freedom. The concept of privacy postulates a group of rights and interests that serve as the cornerstone of restrained liberty. See also Puttaswamy, Justice Bobde p. 407.

[12] Justice K. S. Puttaswamy (Retd.) v. Union Of India (2017) 10 SCC 1; AIR 2017 SC 4161

[13] Ibid

[14] Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth*?, Carnegie India (Mar 9,2022,9:29 PM) https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-8121

[15] Ibid

[16] Ibid

 ISSN: 2582-6433

borne by both small and big businesses. This is a worry since most Indian businesses are tiny. Having to comply with such requirements would be very taxing on them. In addition, the government will be able to force companies to provide non-personal data under the terms of this measure. According to the paper, this might have detrimental long-term effects on economic development and creativity. The Data Protection Authority's planned structure is the measure's third major problem (DPA). The bill's provisions will be enforced by this authority, which will also be in charge of settling disputes.

1.1 LITERATURE REVIEW

The General Data Protection Regulation (GDPR) of the European Union is centralized as its principles of user content, transparency of data and individual rights influence the international privacy regulations. Despite its substantial influence, the enforcement of GDPR is still varying among different European Union nations which disclose challenges in accomplishing the uniform compliance standards (Greenleaf, 2023).

The California Consumer Privacy Act (CCPA) is prevalent in the United States in the state-level privacy law. It provides rights like the right to accept, delete and withdraw data sharing to the California residents. It also a grants such rights in states such as Virginia and Colorado **(Okunade *et al.*, 2023)**. But the lack of centralized data privacy law reveals that companies are facing erratic standards amongst the states which are obscuring the compliance for those operative nationally **(Chandler *et al.*, 2021)**.

Apart from this, there is a Personal Information Protection Law in China which is meant to be the strictest law in Asia as it has vigorous data localization necessities and strict restrictions on cross-border transmission of data. The Personal Information Protection Law of Japan also underscores individual regulations but it is regarded as less obstructive for data sharing on international level presenting dissimilar regional priorities **(Raposo & Du, 2023)**. While in India, the Digital Personal Data Protection Act focuses on data localization and user consensus, it also permits for future modification so that the contemporary privacy challenges can be addressed displaying the progressing nature of laws in the region **(Privacy laws and business, 2023)**.

In Brazil, the Lei Geral de Protecao de Dados (LGPD) is similar to GDPR principles as it emphases on user privileges and corporate responsibility. It also enforces the prominence of

 ISSN: 2582-6433

personal data safeguard and it's prospective to disturb the international trade **(Norvel *et al.*, 2022)**. Whereas the Protection of Personal Information Act (POPIA) of South Africa consider lawful data processing and it encompass the privacy standards into African area although it's enforcement can be limited by inadequate resources **(Boissay *et al.*, 2021)**.

The emergence of Artificial Intelligence (AI) and Big Data Analytics has brought about novel challenges in privacy which results in intensified scrutiny on how these technologies affect the rights of users. The 'black box' nature of Artificial Intelligence often obscure the methods of data processing which advances concerns about transparency and bias **(Suherlan & Okombo, 2023)**. Big Data Analytics also has privacy concerns because immense data collection can result to widespread profiling and data security concerns (**Büchi *et al.*, 2020).**

Overall, the global data privacy legislations are expanding which reflect the prominence of addressing the privacy risks which ascends from the latest technology while guaranteeing the fortification of users. However, harmonizing privacy standards worldwide still remains a task because of presenting national priorities cultural values and economic pressures **(Karakhodjayeva, 2023)**.

1.2 STATEMENT OF PROBLEM

The present research deals with the critical analysis of the Data Privacy Law, 2023 along with the Supreme Court judgement to find out whether the Government has been given unregulated power.

1.3 RESEARCH OBJECTIVES

- To study whether unregulated power is given to the government under the Bill.
- To critically analyze data protection bill 2023 along with Supreme Court judgement.

1.4 RESEARCH QUESTIONS

- Does the Bill provide the government unrestricted power and dilute the concept of privacy as given under landmark judgement of Justice K.S. Puttaswamy (Retd.) vs. Union of India[17]?
- What are the laws present in other foreign countries relating to data privacy?

[17] Justice K. S. Puttaswamy (Retd.) v. Union Of India (2017) 10 SCC 1; AIR 2017 SC 4161

 ISSN: 2582-6433

1.5 RESEARCH METHODOLOGY

The present study is based on secondary data collected from the significant sources associated with the objectives of the study which have been collected from diverse sources linked with data privacy law.

1.6 THEORETICAL FRAMEWORK OF INFORMATION PRIVACY LAWS IN INDIA

Article 21 shall be considered as Fundamental Right. According to the Supreme Court's Puttaswamy decision, government access to personal data is a justifiable limitation on the right to privacy for valid national security reasons. Such exceptions must be tightly defined and must fit the four-fold criteria outlined in the ruling, however, as reaffirmed by Apex Court. Following that, we'll see whether the traceability requirement passes the four-pronged evaluation. Four-step test put down by Justice Chandrachud and Kaul as follows[18]:

- *Legitimate Aim Stage*: The court will examine whether right to privacy is infringed or not.
- *Rational Nexus Stage*: The court will examine the balanced between the infringement of the right and reasonable restriction.
- *Necessity Stage*: Court will ensure that there should be less restrictive or equally effective to meet the aim in terms of restrictions on the right.
- *Balancing stage*: The State should balance between the rights and restrictions.

The following four requirements must be satisfied for Article 21 to be violated:

India does not yet have any data protection laws in force. Individual data security and privacy in India are governed by the Information Technology (Sensitive Personal Data or Information) Rules of 20111 and the Information Technology (Sensitive Personal Data or Information)[19] Act of 2000.

1.7 RELEVANT SECTIONS OF THE IT ACT

- It is stated in Section 43A of the Information Technology Act that companies that hold, own, or operate computer resources that include sensitive personal data may be held responsible for damages to anyone impacted by such an act.

---

[18] *Ibid.*

[19] Rule 3 of the 2011 Rules provides a list of items that are to be treated as "sensitive personal data", and includes inter alia information relating to passwords, credit/ debit cards information, biometric information (such as DNA, fingerprints, voice patterns, etc.

 ISSN: 2582-6433

- If a person (including an intermediary) has access to any material that contains personal information about another person, intending to cause or knowing that he is likely to cause wrongdoing, he or she will be punished under Section 72A of the IT Act[20] if he or she discloses such material to any other person.
- Customers have access to their sensitive personal information thanks to new regulations on information technology, which mandate that companies make their online privacy policies publicly available. Law enforcement, for example, may revoke a person's agreement to release sensitive personal information, but the individual has the right to view and update their personal information.

1.8 LIMITATIONS OF THE PRESENT PROVISIONS

- While the Indian Information Technology Act's[21] data protection provisions have a limited scope and application, the IT Act's provisions fail to identify any specific governmental body that would be responsible for data protection; and
- The IT Act[22] was not passed with data protection as its primary goal.
- Further than Section 72 A, there are no other penalties for data breaches under the IT Act[23], which only apply to a limited set of sensitive personal data.
- The IT Rules[24] only apply to information that is generated or transmitted electronically. A contract may easily evade the IT Rules, which only apply to bodies corporate when no other contractual arrangement is in place. This does not apply to state or federal governments.

A committee to create the proposed data protection legislation was constituted by Retd. Justice B. N. Srikrishna[25] in response. The Indian government created the Personal Data Protection Bill 2[26] in response to the committee's findings and recommendations (referred to as "the Bill"). This bill, if passed by both houses of Parliament, would be the first in India to deal with the subject of protecting the privacy of individuals' personal data.

Here, we've discussed three types of personal information and the laws now protecting them,

[20] The Information Technology Act, 2000,No. 21,Act of Parliament,2000(India)
[21] Ibid
[22] Ibid
[23] Ibid
[24] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[25] Ministry of Electronics and Information Technology, White Paper of the Committee of Experts on a Data Protection Framework for India
[26] The Personal Data Protection Bill, 2019, No 373, Act of Parliament,2019(India)

 ISSN: 2582-6433

as well as the proposed revisions in the Bill.

For example, the definition of "sensitive personal data" in the IT Act[27] is unnecessarily restrictive, despite the fact that this was a Nobel attempt at data security at the time. Additional to that, the IT Act does not cover the government. According to the TCPA's Section 43A, Congress has the power to enact legislation aimed at improving data security. Weaknesses include an absence of specifics on how it will be implemented and the consequences for breaking it. This is why Section 45 of the Indian Penal Code dictates that the victim be paid with ₹25,000, which is also insufficient. In addition, these laws only apply to Indian firms.[28]

1.9 THE PERSONAL DATA PROTECTION BILL, 2019[29]

India's government introduced the Personal Data Protection Bill on December 11, 2019, after more than two years of intense discussion over its content and its implementation. Instead of enacting the measure immediately, India's information technology minister Ravi Shankar Prasad submitted it to a joint parliament committee. When the Indian Parliament publishes a committee report on a contentious bill in 2020, the proposal will be enacted into law. This legislation has far-reaching repercussions due to the fact that it establishes data governance that is expected to affect any organization doing business in India.

1.10 DATA PRIVACY ACT, 2023

After receiving approval from both houses of Parliament and obtaining the President’s assent, the Digital Personal Data Protection Bill of 2022 has officially become the Digital Personal Data Protection (DPDP) Act of 2023. The DPDP Act will be enforced once the central government issues a notification. Upon coming into effect, it will regulate the processing of digital personal data in India, regardless of whether the data was originally collected in a digital or non-digital format and subsequently digitized. The legislation aims to enhance data protection and accountability for entities such as internet companies, mobile apps, and businesses that handle citizens’ data. Additionally, the DPDP Act will impact India’s trade negotiations with other nations, aligning with global data protection standards and drawing inspiration from models like the EU’s GDPR and China’s PIPL.

---

27 The Information Technology Act, 2000,No. 21,Act of Parliament,2000(India)

28 Louis Lusky, Invasion of Privacy A Clarification of Concepts, 72 *Columbia L.R.* 693 (1972).

29 The Personal Data Protection Bill, 2019, No 373, Act of Parliament,2019(India)

30 The Digital Personal Data Protection Act,2023, No. 22, Act of Parliament,2023 (India)

 ISSN: 2582-6433

1.11 INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: KEY PROVISIONS

Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals' privacy rights. Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.

By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age. Key provisions of the DPDP Act, 2023[30] are as follows:

•**Definitions:** Although many concepts in the DPDP Act closely resemble those found in the EU's General Data Protection Regulation (GDPR), framework, there are differences in how terminology is used.

a) Data fiduciary: This refers to the entity that, either independently or in collaboration with others, establishes both the purpose and the methods for processing personal data (similar to a data controller). The government can classify any data fiduciary or a specific group of data fiduciaries as 'significant data fiduciaries' (SDFs). The criteria for this classification as an SDF includes he nature of processing activities (such as the volume and sensitivity of personal data involved and the potential impact on data principals' rights) to broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The designation of SDF comes with heightened compliance obligations as explained below.

b) Data processor: This is an entity responsible for processing digital personal data on behalf of a data fiduciary.

c) Data principal: These are individuals whose personal data is gathered and processed (equivalent to a data subject).

d) Consent manager: A person registered with the Data Protection Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform.

•**Applicability**: The DPDP Act applies to all data, whether originally online or offline and later digitized, in India. Additionally, the Act applies to the processing of digital personal data

 ISSN: 2582-6433

beyond India's borders, particularly when it encompasses the provision of goods or services to individuals within the Indian territory.

Age verification mechanisms will be necessary for all companies in India (telcos, banks, e-commerce, etc.) under the new DPDP law, per reporting from *The Economic Times*. The compliance requirement is not just limited to social media platforms. This is essential to record the verifiable consent of users per legal experts.

- **Personal data breach**: This means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises the confidentiality, integrity, or availability of personal data.
- **Individual consent to use data and data principal rights**: Under the new legislation, personal data will be included and processed only with explicit consent from the individual, unless specific circumstances pertaining to national security, law, and order require otherwise. Under data principal rights, individuals also have the right to information, right to correction and erasure, right to grievance redressal, and right to nominate any other person to exercise these rights in the event of the individual's death or incapacity. Currently, there is no specified timeline for the implementation of grievance redressal and data principal rights.
- **Additional obligations of SDFs**: Depending on the quantity and sensitivity of the data they manage—data fiduciaries deemed as SDF are subject to additional obligations under the DPDP Act. Every significant data fiduciary is required to appoint a Data Protection Officer (DPO) responsible for addressing the inquiries and concerns of data principals—those individuals whose data is collected and processed. Regarding international data transfers, the DPDP Act permits data fiduciaries to transfer personal data for processing to any country or territory outside India. However, the central government can impose restrictions through notifications. These restrictions will be determined after assessing relevant factors and establishing necessary terms and conditions to ensure the maintenance of data protection standards during international processing.
- **Establishment of a Data Protection Board**: The Data Protection Board will function as an impartial adjudicatory body responsible for resolving privacy-related grievances and disputes between relevant parties. As an independent regulator, it will possess the authority to ascertain instances of non-compliance with the Act's provisions and impose penalties accordingly. The appointment of the chief executive and board members of the Data Protection Board will be carried out by the central government, ensuring a fair and transparent selection process. To provide an avenue for customers to challenge decisions made by the Data Protection Board, the government will establish an appellate body. This appellate body may be assigned to the

 ISSN: 2582-6433

Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which will be responsible for adjudicating disputes related to data protection and hearing appeals against the decisions made by the Data Protection Board.

- **Voluntary undertaking**: Under this provision, the Data Protection Board has the authority to accept a voluntary commitment related to compliance with the DPDP Act's provisions from any data fiduciary at any stage of complaint proceedings. This voluntary undertaking may entail specific actions to be taken or refrained from by the concerned party. Furthermore, the terms of the voluntary undertaking can be modified by the Board if necessary. The voluntary undertaking serves as a legal barrier to proceedings concerning the subject matter of the commitment, unless the data fiduciary fails to adhere to its terms. In the event of non-compliance, such a breach is considered a violation of the DPDP Act, and the Board is authorized to impose penalties for this infringement. Additionally, the Board has the discretion to require the undertaking to be made public.
- **Alternate disclosure mechanism**: This mechanism will allow two parties to settle their complaints with the help of a mediator.
- **Offence and penalties**: Data fiduciaries can face penalties of up to INR 2.5 billion for failing to comply with the provisions. These include: penalties of up to INR 10,000 for breach of the duty towards data principals; penalty up to INR 2.5 billion for failing to take reasonable security safeguards to prevent breach of personal data; fines up to INR 2 billion for failure to notify the Data Protection Board and affected data principals in case of a personal data breach; penalties of up to INR 2 billion for violation of additional obligations related to children's data; penalty of INR 1.5 billion for failure to comply with additional obligations of significant data fiduciary; penalty of INR 500 million for breach of any other provision of the DPDP Act, 2023 and rules made thereunder.
- **Conflict with existing laws**: The provisions of the DPDP Act will be in addition to and not supersede any other law currently in effect. However, in case of any conflict between a provision of this Act and a provision of any other law currently in effect, the provision of this Act shall take precedence to the extent of such conflict.

Exemptions under the DPDP Act:

- To enforce legal rights and claims.
- To perform judicial or regulatory functions.
- To prevent, detect, investigate, or prosecute offences.

 ISSN: 2582-6433

- To process in India personal data of non-residents under foreign contract.
- For approved merger, demerger, etc.
- To locate defaulters and their financial assets etc.

How can companies prepare for compliance under the Digital Personal Data Protection Act?

By following the below steps, companies can prepare for compliance with India's DPDP Act and protect personal data in line with regulatory guidelines.

Assess and build data privacy:

– Evaluate current compliance status.

– Create a phased action plan covering governance, technology, people, and processes.

– Establish a privacy organization with defined roles, including the DPO, especially if your entity's status is an SDF.

Inventory personal data systems:

– Identify critical data storage and processing systems.

Identify data processors:

– List third parties handling personal data.

– Update agreements and communicate responsibilities.

Draft DPDP Act-compliant documents:

– Create approved data privacy policies and processes.

– Update necessary documents.

– Develop privacy notices, consent forms, and standard contract clauses.

Design consent mechanisms:

– Define consent types.

– Develop user-friendly consent processes.

– Implement efficient consent management tools.

Establish data principal rights handling:

– Set up processes for addressing data principal rights.

– Develop procedures for request handling.

– Use tools for efficient rights management.

Implement data breach response:

– Create breach management processes.

– Integrate with incident management.

 ISSN: 2582-6433

Define data retention periods:

– Categorize data and align retention periods with requirements.

Evaluate and implement privacy technologies:

– Choose suitable tech solutions.

– Assess compatibility and scalability.

– Implement chosen solutions.

1.12 DATA PROTECTION AND REGULATION AROUND THE WORLD

1.12.1 EUROPEAN UNION

[30]*In 2016, the EU's General Data Protection Regulation (GDPR) was finalized and entered into effect on May 25, 2018, resulting in two distinct kinds of international standards for data protection. May 2021 survey*[31]*, it is clear that the GDPR has set up a new "global benchmark" for data privacy protection (sometimes referred to as the "gold 1 standard"), to which non-EU nations are already attempting to match their new and amended legislation in a variety of ways. This "3rd generation" of data privacy regulations is still in its infancy and it is difficult to predict which of the GDPR's 18 or so improvements will be completely adopted. Those nations wishing to gain or maintain unfettered transfers of personal data from the EU will need to comply with a new, more specific "international standard," which will be made possible by the GDPR taking full effect in 2018. It is necessary for the European Commission to give them an assurance that they 'ensure an adequate level of protection' (GDPR art. 45), but the precise content of that 'adequacy standard' (including which of the GDPR's 18 innovations are required) can only emerge from decisions of the European Commission, Opinions of the European Data Protection Board, and (most importantly) decisions of the Court of Justice of the EU (CJEU). Too far, the Commission has only completed one favorable nation evaluation. A two-year reevaluation of Japan's safety net was mandated in January 2019 after it was found to be acceptable (i.e. in 2021).*

In 2020, Japan will enact new legislation that is more in line with the GDPR. It is expected that the Commission will evaluate the 'new' nation of South Korea in 2021, after its major

[30] Graham greenleaf, *Global Data Privacy Laws 2021: Uncertain Paths for International Standard,169* Privacy Laws & Business International Report 23-27(2021)

[31] G. Greenleaf ‘Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance’ (2021) 169 Privacy 1 Laws & Business International Report, 1, 3-5.

 ISSN: 2582-6433

changes in 2020[32] *and it's planned two more reforms in 2021. However, the recent CJEU decision regarding "certain programs enabling access by US public authorities" did not meet the requirements for essentially equivalent protections as are provided under EU law and did not "grant data subjects' actionable rights before the courts against the U.S. authorities"*[33] *has created considerable confusion about adequacy. As a result of Brexit, the interim six-month agreement includes a high priority for a judgment on the UK's adequacy. The GDPR requires that countries that currently hold sufficient status under the 1995 Directive4 renew it within four years (i.e. by 2022)*[34] *Uruguay, Jersey, and Guernsey, three of the five countries, have all extensively altered their legal frameworks by 2019, and Argentina and New Zealand have subsequently followed suit. Canada and Israel are now working on reform legislation. These revisions have yet to fulfill the 'adequacy threshold' of the GDPR, but the Commission's conclusions on these seven nations (plus the UK and Korea) should give substantial insight on which parts of the GDPR are necessary for an adequacy assessment.*

1.12.2 UNITED STATES

[35]*The laws governing data protection in the US have often been called "patchy." 69 Contrary to the EU, the private sector's restrictions and operations are not governed by an all-encompassing regulation. Historically, it has been industry-specific laws and regulations. Additionally, the United States has a history of adopting a laissez-faire or hands-off policy toward the private sector, which implies that they often rely on industries to self-regulate. According to attorney Michael Ryan, the private sector's use of personal information has often been "ambiguous" in its scope and operations, placing consumer privacy and user personal data at the mercy of tech businesses that frequently fail to implement any necessary data protection rules.*

PRIVACY IN THE U.S.

[36]*Despite being often emphasized in the 1960s and 1970s, in contrast to the EU, where it is*

---

[32] Park, KB et al 'Korea amends Personal Information Protection Act' (2020) 163 Privacy Laws & Business International Report 2 21-3.

[33] Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, Case C-311/18, European Data Protection Board, "Frequently Asked Questions on the ruling of the Court of Justice of the European Union 3 in Case C-311/18,"13 July 2020

[34] This is implied by the joint effect of GDPR arts. 45(3) and 45(9). Otherwise they would have 'indefinite adequacy'.

[35] Chrisann Nateish Campbell, *A REVIEW OF DATA PROTECTION REGULATIONS AND THE RIGHT TO PRIVACY: THE CASE OF THE U.S. AND INDIA, https://academicworks.cuny.edu/* (last visitsed on 9 Mar 2022, 10:45 PM)

[36] Chrisann Nateish Campbell, Supra note 107

 ISSN: 2582-6433

officially established, the US does not have a fundamental right to privacy. The right to privacy is often referenced in the Fourth Amendment of the United States Constitution, which bars any intrusion on a person's person or property. According to the Fourth Amendment, a person is shielded against "arbitrary searches and seizures," such as those conducted by the government or police without a warrant, on their person, their property, or their documents.

When "unreasonable searches and seizures without a warrant" occurred, the Supreme Court ruled in Katz vs. US[37] *that the fourth amendment of the Bill of Rights protected "individual privacy," not the "right to private." The FBI had wiretapped a public phone and finally arrested Charles Katz, the focus of the inquiry. The court's decision in favor of Katz overturned the prior findings of the circuit and district courts. Since wiretapping and listening in on a person's conversation are now considered intruding "private speech," the Supreme Court ruled that the FBI required a warrant to tap public lines. It was also formed and used in significant cases such as Carpenter v. the United States*[38] *and Whalen v. Roe*[39] *to protect "personal problems" and "physical matters" information privacy. It was decided in Carpenter vs. United States that FBI agents had not obtained a warrant for Carpenter's arrest, who had been plotting a bank break-in with six other men. Cell phone carriers' location data helped the FBI locate Carpenter and bring him to justice.*

American citizens should enjoy the right to privacy in their "whole body motions," the Supreme Court said. By allowing the government access to cell-site information, the F.B.I.'s actions were thwarted. Patients complained that their personal information was being shared and shown on prescriptions and laptops. This new state law was approved by the Supreme Court, which ruled that obtaining personal information did not violate the Fourth Amendment. There was no immediate risk, and it was no different from other means of acquiring and maintaining information, if gathering personal information would assist decrease drug consumption. No "constitutionally protected private rights" were violated, since the new legislation was solely meant to benefit a small number of people and was guarded against abuse by many measures. Cases relating to federal government data collection have been the most common in prior US cases on the subject of informational privacy. As a result, many of the rules that govern data privacy today were originally designed to protect American citizens from their government.

[37] *Katz v. United States,389 U.S. 347 (1967)*
[38] *Carpenter v. the United States* 138 S. Ct. 2206, 2018 (USA)
[39] *Whalen v. Roe,429 U.S. 589,1977(USA)*

 ISSN: 2582-6433

Despite the fact that lower courts have recently taken a more favorable stance toward people being granted some level of informational privacy, the Supreme Court never really attempted to assert informational privacy as a right, according to congressional research on the Data Protection Law: An Overview.

1) CHINA

Laws enacted in 2017 and 2015, as well as 2012's "Decision on Strengthening Network Information Protection" and 2013's "National Standard of Information Security Technology" were in charge of China before this year's Cybersecurity Law. The scope of data processing and data subjects' rights will be enhanced under China's 2020 draft Personal Information Protection Law, which is expected to go into effect in 2021. This law contains the necessary provisions to ensure the privacy of user data.

WHAT INDIA SHOULD INCORPORATE:

- The provision related to protection of Data Protection is incorporated under China's Constitution (Art 1). Likewise, India should take this matter very urgently and should incorporate under Indian constitution to make it more effective and should declare as matter of right.
- In China both public and private sector under the same obligation to obey the data privacy in case of threat both will face same consequence under Article 37. Likewise, India should also treat sate as well as private sector as same entity. Data privacy legal framework should be followed during State surveillance as well.

2) SWITZERLAND

According to a study, this nation boasts some of the best privacy regulations in the world. In Switzerland, Article 13 of the constitution protects the right of people to privacy and is especially strict in enforcing data privacy rules. It's hard to go wrong with either Resorit or Cloud when it comes to secure cloud storage. It uses zero encryption, so no one else can view the data you keep there, not even the firm you use.

WHAT INDIA SHOULD INCORPORATE:

- India should also incorporate this provision and made special provision under constitution which specially deals with Data privacy by then only this issue will be address efficiently.

 ISSN: 2582-6433

- India should come up with strong cloud storage with strong VPN then only customer data will get exploited. The customer data should be prevented from the eyes of private as well as public entity.

3) ROMANIA

This problem should be taken extremely seriously by Romanian and Indian legislation, which should implement data protection laws, E-privacy, and E-commerce. The scope of data protection cannot be summarized under a single regulation, hence several laws should be implemented to preserve privacy.

4) PANAMA

As a result of the country's stringent legal framework, including the constitution, judicial code, and criminal code, residents and non-citizens alike may feel secure knowing that their personal information is secured in Panama. Additionally, India should include unique provisions in the Constitution, Code of Civil Procedure[40], and Code of Criminal Procedure[41] and impose penalties for violating data privacy laws.

WHAT INDIA SHOULD INCORPORATE:

- Like Panama, India should also incorporate under constitution for protection of private document. Private conversations should only be recorded if there is a warrant.
- Under Criminal Code special provision should be incorporated to make privacy law more stringent in case violation of data breach.

CONCLUSION

The study focused on the areas of the Bill related to data privacy which was less studied and need our attention as there is a necessity to modify the present personal data protection bill in India so that it also there is a need of legislation keeping in view continuous technological advancement how important is to address the issue of Information privacy but many of them fails to take account of short coming in the proposed Bill, even those who oppose the law fail to specify the provisions that need to be changed or amended, and they fail to compare the bill to previous bills, such as the Data Protection Bill of 2018, Bill 2019 and now the current 2021 Bill removes the better provisions of the 2018 Bill. India should take inspiration from other

[40] The Code of Civil Procedure, 1908, Act No 5, Act of Parliament (India)
[41] The Code of Criminal Procedure, 1973, No 2, Act of Parliament (India)

 ISSN: 2582-6433

nations like China, Switzerland, Panama, etc. in this regard. As in Switzerland, Article 13 of the constitution protects the right of people to privacy and is especially strict in enforcing data privacy rules. It's hard to go wrong with either Resort or Cloud when it comes to secure cloud storage. It uses zero encryption, so no one else can view the data you keep there, not even the firm you use. India should also incorporate this provision and made special provision under constitution which specially deals with Data privacy by then only this issue will be address efficiently. India should come up with strong cloud storage with strong VPN then only customer data will get exploited. The customer data should be prevented from the eyes of private as well as public entity. Similar to Panama, India should also incorporate under constitution for protection of private document. Private conversations should only be recorded if there is a warrant. Under the Criminal Code, special provisions should be incorporated to make privacy law more stringent in case violation of data breach. After taking up these steps, data privacy of users of the country can be ensured.

REFERENCES

Boissay, R., et al. (2021). Data privacy frameworks in Africa and the Middle East: A comparative review. African Journal of Law and Technology.

Briefing, I. (2024, July 15). *India's Digital Personal Data Protection (DPDP) Act, 2023*. India Briefing News. *https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html*

Büchi, M., et al. (2020). The privacy implications of big data analytics. Big Data and Society.

Chander, A., et al. (2021). The comparative impact of GDPR and CCPA on data privacy standards. World Journal of Advanced Research.

Greenleaf, G. (2023). Global data privacy laws 2023: A critical analysis. Privacy Laws & Business.

Karakhodjayeva, S. (2023). Toward a harmonized approach to global data privacy. Journal of International Law.

Norval, A., et al. (2022). Data protection in Latin America: The case of Brazil's LGPD. International Journal of Data Protection.

Okunade, D., et al. (2023). The California Consumer Privacy Act and the U.S. data privacy landscape. WJARR.

Privacy Laws & Business. (2023). Global data privacy laws 2023: 162 national laws and 20 Bills. Retrieved from: PRIVACY LAWS & BUSINESS ps://www.privacylaws.com/reports-gateway/articles/int181/int181_2023/).

 ISSN: 2582-6433

Raposo, R., & Du, Y. (2023). Data privacy in Asia-Pacific: PIPL and regional developments. WJARR.

Shroff, C. (2023, August 4). *The DPDP Bill Overview: A new dawn for data protection in India | India Corporate Law*. India Corporate Law. *https://corporate.cyrilamarchandblogs.com/2023/08/the-dpdp-bill-overviewa-new-dawn-for-data-protection-in-india/*

Suherlan, Y., & Okombo, J. (2023). AI and data privacy: Technological impact on user rights. Journal of Ethics in Technology.

What is India's Digital Personal Data Protection (DPDP) Act? Rights, Responsibilities & Everything You Need to Know. (n.d.). Digital Guardian. *https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you*