IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CONSTITUTIONAL PROTECTION OF DIGITAL PRIVACY IN INDIA: ANALYSIS OF ARTICLE 21 WITH REFERENCE TO DPDP COMPLIANCE CHALLENGES

A. AFROSE

3rd year Ll.b student

Vels Institution of Science, Technology &Advanced Studies (VISTAS)

CHAPTER 1

1. Introduction:

Privacy is a fundamental concept of modern democratic states, which is deeply connected with the independent existence, dignity and autonomy of the individual. In a general sense, privacy refers to the right of an individual to be free from unwanted interference in his private life, information, communication and decision-making. It is one of the main elements of protecting the individual's autonomy.

Article 21 of the Constitution of India states that

"No person shall be deprived of his life or personal liberty except in accordance with the procedure established by law". The maker of the constitution initially accepted this article as a protection of physical liberty. That is, its main purpose was to protect citizens from illegal detention, arrest or state repression. But through active interpretation by the judiciary, this article gradually began to include a wide range of rights to human life.

Especially since the 1970s the Supreme Court has interpreted the word "Life" not only as the right to life, but also as the right to live with dignity. Various aspects of education, health, environment, dignity and personal liberty are included in Article 21. As technology advances, people's lives are increasingly shifting to digital platforms, the question of personal data protection comes to the force.

In today's era, a personal's identity, financial information, health information, communications, and even political opinions are saved as digital data. As a result, losing control over information means losing personal freedom. In this context, the question arises- Will digital information get constitutional protection?

This question was answered by the Puttaswamy judgment, where the court declared that privacy is an integral part of human dignity and it is included in Article 21. As a result, privacy is recognized as both a negative right (freedom from state interference) and a positive right (protection by the state)

1.1. Research Problem:

This study lies in examining the disconnect between the constitutional guarantee of the right to privacy under Article 21 and the practical implementation of data protection under the Digital Personal Data Protection (DPDP) framework in India. Although privacy has been judicially recognized as a fundamental right, there remains significant challenges in ensuring consistent compliance, including regulatory ambiguities, enforcement limitation, and rapid technological advancements. This creates uncertainty about the effectiveness of existing legal mechanisms in safeguarding digital privacy, raising concerns about whether constitutional protection are adequately realized in practice.

1.2. Research Question

1. How has the right to digital privacy evolved under Article 21 of the Indian Constitution?
2. What are the key features and limitations of the Digital Personal Data Protection (DPDP) Act, 2023?
3. What are the major challenges faced by organisations in complying with the DPDP Act, 2023?
4. How has the Indian judiciary contributed to the protection of digital privacy under Article 21?

1.3. Objectives of the study:

1. To Study the Evolution of Digital Privacy as a Fundamental Right Under Article 21
2. To critically examine key provision of the Digital Personal Data Protection (DPDP) Act 2023
3. To identify and analyze compliance challenges in Digital Personal Data Protection implementation
4. To critically evaluate the role of the judiciary in protection the right to Digital Privacy Under Article 21

1.4. Hypothesis:

While the puttaswamy judgment (2017) embeds digital privacy within Article 21 ‘s proportionality framework the Digital Personal Data Protection (DPDP) Act 2023 falls short of ensuring full constitutional compliance due to inadequate enforcement mechanisms, broad state exemptions, and weak fiduciary accountability, thereby undermining effective protection against digital surveillance and breaches.

1.5. Research Methodology:

The research adopts a doctrinal study to examine the constitutional protection of digital privacy in India under Article21 in relation to the Digital Personal Data Protection (DPDP) framework. It primarily relies on secondary sources such as constitutional provision, judicial decision, statutes, government reports, Reference books and scholarly articles to understand the evolution and scope of the right to privacy.

1.6. Research Limitation:

This study on constitutional protection of digital privacy under Article 21, focusing on DPDP compliance challenges, faces several limitations. It primarily relies on secondary judicial interpretations post-Puttaswamy, potentially missing unreported lower court decisions. The analysis remains India-centric, excluding comparative GDPR perspectives for deeper DPDP critiques. Rapid DPDP rule-making post-2023 limits access to empirical compliance data amid evolving notifications. Emphasis on legal-textual methods overlooks socio-economic effects on vulnerable data subjects. Finally, fast-evolving technologies like AI surveillance outpace Article 21's static proportionality tests, while classified government data restricts full surveillance evaluation.

1.7. Research Gap:

The existing literature on digital privacy in India largely focuses either on the constitutional recognition of the right to privacy under Article 21 or on the framework of the Digital Personal Data Protection (DPDP) Act as a standalone regulatory development. However, there is a limited integrated analysis that critically examines the intersection between constitutional principles and the practical realities of DPDP compliance. In particular, insufficient attention has been given to how enforcement challenges, institutional limitation, and evolving technological practices may weaken the effective realization of constitutionally guaranteed privacy rights. Additionally, there is a lack of in-depth evaluation of whether the DPDP framework adequately reflects the standards laid down by judicial interpretations of privacy. This gap highlights the need for a comprehensive study that bridges constitutional theory with regulatory practice in the context of digital data protection.

1.8. Literature of Review:

Books

Upendra Baxi, The Crisis of the Indian Legal System, discusses the expansion of fundamental rights in India and highlights the role of the judiciary in interpreting Article 21. The work is useful in understanding how the concept of privacy evolved as an essential part of the right to life and personal liberty.[1]

V.N. Shukla, Constitution of India, provides a detailed explanation of constitutional provisions, particularly Article 21, and its judicial interpretation. The book helps in analysing how the right to privacy has been incorporated into the broader framework of fundamental rights.[2]

Articles and journals

Ananta Kr Adhikari,“ Article 21 of the Constitution of India and The Right to Privacy in the Digital Era: An Analytical Review”, explains the transformation of privacy rights in the digital age. The article highlights the importance of protecting personal data and examines how constitutional principles are applied in the context of digital privacy.[3]

Jayeeta Mandal and Yoshita Mandal, “Analysis on Digital Personal Data Protection Act 2023”, Critically analyses the provisions of the DPDP Act. The Article discusses key concepts such as consent, data fiduciaries, and compliance challenge, which are important for evaluating the effectiveness of the Act.[4]

Report and Official Publications

Justice B.N. Srikrishna Committee Report (2018) plays a significant role in shaping India’s data protection framework. The report emphasizes the need for a comprehensive data protection law and has influenced the development of the Digital Personal Data Protection Act,2023.

Judicial Decisions

Justice K.S. Puttaswamy vs Union of India (2017)[5] is a landmark judgment that recognized the right to privacy as a fundamental right under Article 21 of the Constitution. This decision forms the foundation for analysing digital privacy protection in India and its relationship with constitution rights.

[1] Upendra Baxi, “ The Crisis of the Indian Legal System”

[2] V.N. Shukla, “ Constitution of India, provides a detailed explanation of constitutional provisions, particularly Article 21, and its judicial interpretation”

[3] Ananta Kr Adhikari,“ Article 21 of the Constitution of India and The Right to Privacy in the Digital Era: An Analytical Review”,

[4] Jayeeta Mandal and Yoshita Mandal, “Analysis on Digital Personal Data Protection Act 2023”,

[5] Justice K.S. Puttaswamy vs Union of India (2017)

1.9. Chapters

Chapter 1-Introduction

Chapter 2 -The Evolution of Digital Privacy as a Fundamental Rights under Article 21.

Chapter 3-Legislative Framework of Digital Personal Data Protection Act 2023 Analysis

Chapter 4-Compliance Challenges and Implementation Gaps in the Digital Personal Data Protection Act, 2023

Chapter 5-Judicial Response to the Protection of Digital Privacy under Article 21

Chapter 6- Conclusion and Suggestions

CHAPTER 2

THE EVOLUTION OF DIGITAL PRIVACY AS A FUNDAMENTAL RIGHT UNDER ARTICLE 21

2. Introduction:

"Privacy is not an option and it shouldn't be the price we accept for just getting on the Internet". - Gary Kovacs, former CEO of Mozilla.[6]

Privacy is becoming one of the most pressing concerns of the digital age. We live in an era where every click, like, and share can be traced. The rapid advancement of technology has revolutionized the way we communicate and now even how we think, but it has also brought unprecedented challenges to our personal privacy. Form social media platforms harvesting data to governments implementing mass surveillance, the boundaries of privacy are continuously being tested and redefined. As we navigate this digital landscape, understanding our privacy rights and how to protect them is more crucial than ever. This article delves into the evolution of privacy rights.

2.1. Understanding Digital Privacy in the Modern Age:

Digital privacy refers to the right and ability of individuals to control how their personal information is collected, used, and shared in the digital world. It embodies the desire to navigate online spaces without fear of unauthorized data collection, misuse, or distribution, forming the essence of internet privacy. Digital privacy is crucial for several reasons. It empowers individuals by giving them control over their information and the freedom to interact with the digital world on their terms. It also helps prevent cybercrimes such as identity theft, fraud, and harassment. Additionally, it maintains a free and open society by protecting against undue intrusion and surveillance from both state and corporate entities.

The concept of privacy has evolved significantly with technological advancements. While privacy was once a straightforward concept, it has become more complex in the digital age. As individuals leave larger digital footprints, privacy now encompasses online interactions, behaviours, and activities.

Several challenges make maintaining digital privacy difficult. Widespread and often hidden data collection methods make it hard for individuals to understand what data is being collected and how it is used. Controlling the distribution of personal data across the internet is daunting. Additionally, many individuals lack the knowledge and tools to manage their digital privacy effectively.

[6] Ms. Adyasha Behera & Mr. Bhanu Pratap Singh; Safeguarding privacy in the Digital Era: Balancing Rights, Security, and Innovation; Chanakya Law Review (CLR); (Vol V, Issue 11July-Dec.,2024)

2.2. The Evolution of the Right to Privacy in India

2.2.1. Historical Perspective:

The concept of privacy, While intrinsic to human dignity and autonomy, was not explicitly articulated as a fundamental right in the India Constitution when it was adopted in 1950. This omission can be attributed to the framer's focus on safeguarding collective freedoms and ensuring socio-economic equity in a nascent democracy rather than emphasizing individualistic notions of privacy. However, as society progressed and the scope of personal liberties expanded, the absence of a clear constitutional guarantee for privacy led to judicial scrutiny and debate.[7]

- **The M.P. Sharma Case (1954): Rejection of Privacy**

  One of the earliest judicial engagements with the idea of privacy occurred in M.P. Sharma vs Satish Chandra (1954)[8], where the Supreme Court was called upon to interpret the scope of fundamental rights in the context of state search and seizure powers. The petitioners challenged the constitutional validity of searches conducted under the CrPC, claiming that such action violated their fundamental rights, including an implied right to privacy.

  The eight-Judge bench unequivocally dismissed the existence of a constitutionally guarantee right to privacy. The Court held that the drafters of the Constitution did not intend to include privacy as a separate fundamental right. Instead, the focus was on protecting tangible rights, such as property (Article 19(1)(f), later repealed)[9] and personal liberty (Article 21). The bench observed that any perceived right to privacy was secondary to the state's legitimate interests in maintaining law and order. This Judgment set as a precedent that limited the conceptual space of privacy within the Indian Constitutional framework for several years.

- **The Kharak Singh case(1964): Privacy as a Derivative Right**

The Supreme Court revisited the issue of privacy in Kharak Singh vs State of Uttar Pradesh (1964)[10], a case concerning police surveillance on a suspect without a judicial order. The petitioner contended that the police surveillance, which included domiciliary visits during the night, violated his fundamental rights under Articles 19 (1)(d) (freedom of movement)[11] and Article 21 (right to life and personal liberty).

In this case, the court displayed a divided stance. The majority rejected the idea of a distinct right to privacy, echoing the sentiment of M.P. Sharma. They argued that the Constitution guaranteed personal liberty and property but not an overarching right to privacy. However, the Court did recognize that domiciliary visits infringed upon personal liberty, as protected under Article 21, thereby providing limited protection to privacy in specific contexts.

Justice Subba Rao's dissent in this case marked a significant milestone. He argued that privacy was implicit in the right to personal liberty guaranteed under Article 21. Justice Rao emphasized that the state's intrusion into an individual's private sphere, particularly their home, could not be justified without substantial cause or legal authorization. His dissent laid the groundwork for the future recognition of privacy as a fundamental right.

[7]Dr. Tanveer Kaur ;"Right to privacy in Digital Age: A Study with Indian Context"; European Economic Letter; , Vol 14, Issue 4 (2004)
[8] M.P. Sharma vs Satish Chandra (1954)
[9] The Constitution of India ,1950 (Article 19(1)(f) and Article 21
[10] Kharak Singh vs State of Uttar Pradesh (1964)
[11] The Constitution of India, 1950 (Article 19(1)(d) and Article 21

- **Privacy in the Early Constitution Era**

The early judicial interpretation of privacy reflect a cautious and conservative approach, largely shaped by the socio-political realities of post-Independence India. The focus on collective welfare and national security often overshadowed individual-centric rights like privacy. Both M.P. Sharma and Kharak Singh underscored the judiciary's initial reluctance to extend the scope of fundamental rights to include privacy, viewing it as an ancillary rather than an intrinsic right.

These judgments established that privacy could only be indirectly protected through other fundamental rights, such as the right to personal liberty (Article 21) or the right to property (Article 19 (1)(f))[12]. The lack of explicit recognition of privacy allowed the state greater leeway in conducting searches, surveillance and investigation without stringent checks on intrusions into individual autonomy.

- **The Legacy of Early Privacy Jurisprudence**

Despite their limitations, the early rulings in M.P. Sharma and Kharak Singh shaped the trajectory of privacy jurisprudence in India. The dissenting voices and the partial recognition of privacy within the ambit of Article 21 hinted at the evolving nature of constitutional interpretation. These judgments laid the groundwork for subsequent judicial decisions, which progressively expanded the scope of fundamental rights to include privacy.

As India entered the digital age, the limitations of these early judgments became more apparent. The need for a robust legal framework to address privacy concerns grew, culminating in the landmark Justice K.S. Puttaswamy vs Union of India (2017) decision[13]. This case explicitly overturned the restrictive interpretations in M.P. Sharma and Kharak Singh**,** declaring privacy a fundamental right integral to human dignity and personal liberty.

2.3. Landmark Judgment in Privacy Right:

Justice K.S. Puttaswamy Vs Union of India.(" Aadhar Judgment")

The landmark judgment in this case ("Aadhar judgment")[14] fundamentally reshaped the discourse on privacy rights in India, particularly in the context of the digital age. The Supreme Court of India, in this historic ruling, declared that the Right to Privacy is a Fundamental Right protected under Article 21 of the Constitution, which guarantees the right to life and personal liberty. This judgment emphasized that privacy is an intrinsic part of the freedoms guaranteed by Part III of the Constitution.

A crucial aspect of the judgment is its recognition of informational privacy as an essential facet of the broader right to privacy. The Court acknowledged that in today's digital era, the regulation of personal data is paramount. The judgment highlighted several key facts of information that underscore the necessity for robust data protection laws:

1. **Nonrivalrous Nature of Information:**

Information can be used and consumed by multiple users simultaneously without diminishing its value. This characteristic make it imperative to protect how personal data is accessed and shared

[12] The Constitution of India ,1950 (Article 19(1)(f) and Article 21
[13] Justice K.S. Puttaswamy vs Union of India (2017)
[14] Justice K.S. Puttaswamy vs Union of India (2017) 10 SC 1

2. **Invisibility of Information Processing:**

Often, individuals are unaware of how their information is being collected , used , stored, or processed. This invisibility raises significant concerns about unauthorized use and breaches of privacy.

3. Recombinant Nature of Inform

Fragments of data collected from various sources can be combined to create comprehensive profiles of individuals. This ability to compile detailed personal profiles necessitates stringent data protection to prevent misuse.

The judgment further recognized that certain classes of information warrant a reasonable expectation of privacy, affirming the "right to be left alone". It pointed out the limitation of the existing legal framework under the Information Technology Act 2000, as amended in 2008, which recognizes "personal information" and "personally sensitive data or information". According to this framework, the collection or use of such data requires explicit consent from the user, who should have the choice to provide or withhold such information.

The Supreme Court stressed the importance of transparency in obtaining consent for the collection, use, retention, and processing of personal data. This emphasis on informed consent is crucial in ensuring that individuals are aware of and can control how their data is utilized. Moreover, the judgment underscored that any encroachment on privacy must be through legislated law that meets all constitutional requirements, thus ensuring that restrictions on fundamental rights are reasonable and justified.

Recognizing the dynamic and pervasive nature of digital data, the bench urged the legislature to adopt a comprehensive data protection regime. This regime should balance individual privacy interests with the legitimate concerns of the state. The judgment catalyzed the development of data protection laws in India, leading to the formulation of the India Digital Personal Data Protection Act 2023 (DPDP Act), which aims to provide robust protection of personal data in the digital age.

The Puttaswamy judgment is a seminal ruling that firmly established the Right to Privacy as a fundamental right in India, particularly emphasizing the need for strong data protection laws. By recognizing informational privacy as a critical component of personal liberty under Article 21, the judgment laid the groundwork for safeguarding individual privacy in the face of rapid technological advancements and pervasive digital data processing. The judgment's call foe legislative action has been instrumental in shaping the ongoing evolution of privacy protection laws in India.[15]

CHAPTER 3

LEGISLATIVE FRAMEWORK OF DIGITAL PERSONAL DATA PROTECTION ACT 2023 ANALYSIS

3.1. What is Data Privacy?

Data privacy refers to the protection of personal information, ensuring that individuals have control over how their data is collected, processed, stored, and shared. It encompasses the right of individuals to keep their information private and secure, limiting unauthorized acess or use by others.

"Data Privacy" usually refers to the handling of critical personal information, also called "personally identifiable information"(PII). This information can include social security numbers, health records, and financial data, including bank account and credit card number. In a business context, data privacy goes beyond

[15]Ms. Adyasha Behera & Mr. Bhanu Pratap Singh; Safeguarding privacy in the Digital Era: Balancing Rights , Security, and Innovation; Chanakya Law Review (CLR) (VOL V, Issue 11 July-Dec.,2024)

the PII of employees and customers. This could involve things like proprietary research, development data, or financial information.[16]

3.2. Why Data Privacy is so important?

I. Protection against identity theft and fraud:

Sharing personal information can leave you vulnerable to identity theft and financial fraud. Identity Theft is when cybercriminals illegally access personal and critical information about an individual and compromise the same with ulterior motives, which includes siphoning off money from bank accounts or creating fake social-media profiles and taking control of accounts for personal vengeance.

II. Protection against discrimination:

Data can be used intentionally for personal gain to discriminate against individuals based on the factors like race, religion, or political beliefs leading to instability of social & political ecosystem of a country.

III. Transparency and accountability:

Popular digital platforms and mobile apps collect extensive amounts of user data to offer personalized experiences, targeted advertising, and optimized services enhance navigation and provide recommendations but track user's movements, compromising their privacy.

IV. Data driven innovation and economic growth:

Protecting individual privacy while fostering data driven innovation can lead to the development of new technologies and services that benefit society as a whole

V. Protection against government surveillance:

Sometimes Government surveillance threatens individual privacy by undermining the principles of consent, transparency, and proportionality. It can create a chilling effect on free expression and association, as individuals may fear repercussions for expressing dissenting opinions or engaging in activities that are perfectly legal but perceived as threatening by authorities.

3.3. How Digital Personal Data Protection (DPDP) Act 2023 formed :

The first law that was enacted to secure the digital information of individuals was Information Technology Act 2000. Later in the year 2011, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 came into force to secure the sensitive personal data or information of individuals. Further, the Ministry of Electronic and Information Technology codified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 to balance the privacy rights in the interest of national security and public order.[17]

In the case of Karmanya Singh Sareen and Ane vs Union of India and Ors.(2016), WhatsApp's 2016 privacy policy to permit WhatsApp to share data with Facebook was challenged before the Delhi High Court, Wherein the High Court upheld WhatsApp's policy and directed them to delete the data of the users who have opted out from this service.

[16] International Centre for Information Systems and Audit , 9th edition, e-journal Data Protection and Data Privacy
[17] https://blog.ipleaders.in/digital-personal-data-protection-act-dpdpa-2023/#

In the case of Justice K.S. Puttaswamy vs Union of India (2012), the 9 judge's bench of the Supreme Court of India declared that the right to privacy is a fundamental right of the person under Article 21 of the Constitution of India. Following this, the B.N. Shrikrishna committee was formed to report on the concerns regarding the digitalization of personal data and propose solutions. The Draft Personal Data Protection Bill, 2018 was referred to the joint parliamentary committee foe examination and was for public comments.

Now, after 5 years of extensive submissions, discussions, recommendations, consultations, customizations, and deliberation, a final draft of the Digital Personal Data Protection Bill 2023, which after approval from the cabinet, was finally ready to be presented before the houses of the parliament and finally got passed in the lower house.

3.4. Digital Personal Data Protection Act:

The Government of India has enacted the Digital Personal Data Protection Act, 2023 to protect data in the digital era. This Act is considered to be India's first comprehensive data protection framework.[18]

The main feature of the Act is "consent- based data processing". That is, an organization is obliged to obtain the explicit consent of the user before collecting personal data. It defines the citizen as the "Data Principal" and organization collecting the data as the "Data Fiduciary"

According to this Act, the rights of the citizen are;

1. Right to know the purpose of use of the data,
2. Right to rectify the data,
3. Right to delete the data,
4. Right to lodge a complaint.

Violation of the Act has provided for huge financial penalties against the organization, which increases corporate liability.

However, there are some limitations to this Act. The government can exempt some provisions of the Act in certain cases- due to national security, public order or state interest. Critics say the provision increases the potential for state surveillance and could conflict with the principle of proportionality enshrined in the Puttaswamy judgment.

Another criticism is that the powers of independent data protection authorities are limited. As a result, the future of how effective the actual implementation will be remains to be seen.

Nevertheless, the DPDP Act is an important step towards India's digital constitutionalism, as it recognizes citizen's data as a legally protected asset for the first time.

3.5. Objectives of the Digital Personal Data Protection Act, 2023

The main objective of the DPDP Act are:[19]

- To recognize and protect the right of individuals to their personal data in the digital environment.
- To regulate the processing of digital personal data in a lawful, fair, and transparent manner.
- To impose clear obligations and accountability on entities processing personal data.

[18] Anantha Kr Adhikari ;" Article 21 of the Constitution of India and the Right to Privacy in the Digital Era: An Analytical Review"; International Journal of Creative Research Thoughts (IJCRT);" Volume 14, Issue 3 March 2026

[19] Jayeeta Mandal and Yoshita Manral; " Analysis on Digital Personal Data Protection Act 2023."(academike article on legal issues) ; , www.lawctopus.com,

- To establish an effective enforcement mechanism through the data protection Board of India.
- To provide for penalties and remedies in cases of non- compliance and personal data breaches.
- To balance individual privacy with legitimate business, governance, and public interest needs.

3.6. Applicability and Scope of the Act :

According to Section 3, the Digital Personal Data Protection Act applies to the processing of "digital personal data" in India, including personal data that is collected in non-digital form but is subsequently digitised. It also has extra- territorial reach and applies to processing outside India if such processing is connected with offering goods or services to individuals in India. At the same time, the Act does not apply to personal data processed or domestic purposes, nor to personal data that is made publicly available by the individual herself or under a legal obligation.[20]

3.7. Definitions under the DPDP Act Framework

The DPDP Act contains a detailed definition clause in section 2.[21]

❖ **Digital Personal Data (Section 2(n)):**

This means personal data that exists in digital form. The DPDP Act mainly deals with this category of data, such as data stored on computers, mobile phones, servers, or cloud platforms.

❖ **Data Principal (Section 2(j)):**

A Data principal is the individual to whom the personal data relates. If the individual is a child or a person with disability, the term also includes the parent or lawful guardian acting on their behalf.

❖ **Data Fiduciary (Section 2(i)):**

A Data Fiduciary is any person or entity that decides the purpose and means of processing personal data. In practical terms, this is the organisation or person who is in control of why and how the data is used

.

❖ **Data Processor (Section 2(k)):**

Data processor is any person or entity that processes personal data on behalf of a Data Fiduciary. For example, a cloud storage provider or an IT service company processing data for another company is a Data Processor.

❖ **Processing (Section 2 (x)):**

Processing means any operation performed on digital personal data, such as collecting, or deleting the data.

[20] Jayeeta Mandal and Yoshita Manral; "Analysis on Digital Personal Data Protection Act 2023". (academike articles on legal issues); www.lawctopus.com,

[21] Digital Personal Data Protection Act ,2023

❖ **Consent Manager (Section 2(g)):**

Consent Manager is a person registered with the Data Protection Board who helps a Data Principal give, manage, review, and withdraw her consent through an accessible and transparent platform.

❖ **Significant Data Fiduciary (Section 2(z)):**

A Significant Data Fiduciary is a class of Data Fiduciaries that may be notified by the Central Government under section 10. Such entities are subject to additional compliance duties under the Act.

3.8. Legislative Developments in India and Current Scenario

In the digital age, privacy protection in India is a dynamic and multifaceted issue. While various legislative and regulatory framework exist, a significant advancement was made with the enactment of the India Digital Personal Data Protection Act 2023 (DPDPA). This landmark legislation, effective from September 1, 2023, aims to safeguard individual's privacy in the digital realm by imposing rigorous privacy and data protection standards on all organizations processing personal data in India. The following outlines the current landscape of privacy protection legislation in India.

1. **Information Technology Act,2000 (IT Act):**

The Information Technology (IT) Act,2000 [22]was India's first major legislation addressing privacy and cybersecurity concerns in the digital realm. While it provided a foundational framework, the Act is often criticized for being outdated and inadequate to handle the challenges of the modern digital landscape

These sections deal with compensation for failure to protect data and punishment for breach of confidentiality and privacy, respectively.

- **Section 43A** :

Requires companies to compensate individual for the failure to protect sensitive personal data.

- **Section 66**:

Addresses computer-related offenses, such as hacking.

- **Section 72**:

Penalize unauthorized disclosure of personal information.

Although these provisions offer some degree of protection, they lack the specificity and comprehensiveness required to address evolving data privacy challenges, particularly in areas like social media, artificial intelligence and cross-border data flows.

- **IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:**

These rules define what constitutes sensitive personal data and outline the security practices companies must follow to protect such data.[23]

- **The Information Technology (Intermediary Guidelines and Digital Media Ethics Codes) Rules, 2021:**

This rule mandates that companies collecting information must adhere to specific requirements to ensure the security of private data.[24]

[22] The Information Technology Act, 2000

[23] IT (Reasonable Security Practices And Procedures and Sensitive Personal Data or Information) Rules,2011

[24] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021

The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule,2011 define "Sensitive personal and mandate security safeguards. Further, the IT (Intermediary Guidelines and Digital Media Ethics Codes) Rules, 2021 impose due diligence obligation on intermediaries. These provisions support digital privacy but remain limited in scope, creating compliance challenges when measured against the broader protection guaranteed under Article 21.

2. **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016**[25]

The primary aim of this law is to secure targeted delivery of benefits, subsidies and services funded from the consolidated fund of India to rightful beneficiaries, for receiving which Aadhaar may be required. While ensuring that, the Act also incorporates strong privacy and security measures, drawing from internationally accepted principles including purpose, collection and use limitation.

- **Section 29:**
  Restricts the sharing of core biometric information.
- **Section 30:**
  Classifies biometric information as sensitive personal data.
- **Section 33:**
  Allows disclosure of information in the interest of national security upon direction by an officer not below the rank of joint Secretary.

While the Act introduces safeguards, such exceptions raise concerns about potential infringement of privacy under Article21, particularly regarding proportionality and oversight

3. **Right to Information Act, 2005(RTI Act)**

The Right to Information Act,2005 (RTI) [26]is a landmark legislation ensuring transparency and accountability in governance, empowering citizens with the right to know. The Digital Personal Data Protection Act,2023(DPDPA), passed in the wake of the K. S. Puttaswamy judgment upholding privacy as a fundamental right under Article 21, seek to protect personal data. However, Concerns arise that amendments under DPDPA, particularly to Section 8(1)(j) of RTI, may dilute transparency and restrict public access to vital information.

- **Section 8(1)(j):**
  Exempts personal information from disclosure if it has no relationship to any public activity or interest, or if it would cause an unwarranted invasion of privacy unless the larger public interest justifies the disclosure.

4. **The Bharatiya Nyaya Sanhita,2023:**

The Bharatiya Nyaya Sanhita,2023[27] offences such as cheating, criminal breach of trust, and theft apply to digital assets where dishonest intent and property elements are established. These provision can extend to misuse of personal data , offering indirect protection to digital privacy by criminalizing wrongful handling of information, thereby supporting the broader constitutional right to privacy under article 21.

[25] The Aadhaar (Targeted Delivery of Financial and Others Subsidies, Benefits, and Services)Act 2016
[26] Right to Information Act , 2005
[27] The Bharatiya Nyaya Sanhita, 2023

- **Section 314 and 316(1):**
  Address dishonest misappropriation of property and breach of trust, which can relate to misuse of personal information.

5. **Consumer Protection Act 2019:**

The Digital Personal Data Protection Act,2023 (DPDP Act) and India's Consumer Protection Act, 2019(CPA)[28], along with the Consumer Protection (E-Commerce)Rules,2020 , together govern the rights of consumers in the digital economy. While the DPDP Act secures information privacy, consumer protection law addresses fair trade, transparency, and grievance redressal.

- **Consumer Protection Act**

  Protects against unfair trade practices, misleading advertisements, defective goods/ services.

- **Consumer Protection (E-Commerce) Rules, 2020:**
  Includes provisions related to the protection of consumer data in e-commerce transactions.

6. **Telecom Regulatory Authority of India (TRAI) Regulations:**

The Telegraph Regulatory Authority of India (TRAI) regulates data privacy in the telecommunications sector. It has specific guidelines to prevent telecom companies from misusing customer data. These guidelines ensure customer information is handled responsibly and securely, safeguarding privacy rights

- **Telecom Commercial Communications Customer Preference Regulations,2018:[29]**
  Aims to curb unsolicited commercial communication and protect user data in the telecom sector.

7. **Sector-Specific Guidelines:**

- **Reserve Bank of India (RBI) Guidelines**
  The Reserve Bank of India issues guidelines for banks and financial institutions regarding data protection and cybersecurity. [30] Based on the Payment Data Localization policy, payment system operators, such as payment gateways and banks, are required to store all payment-related data entirely within India. This includes;

  1. Information like transaction details, customer information, and payment credentials.
  2. Foreign processing is permitted for specific purposes, such as fraud detection, but data copies must remain stored in India

  These rules ensure that financial data critical to national security is readily available to Indian regulators and protected from foreign jurisdictions.

[28] The Consumer Protection Act, 2019
[29] The Telecom Commercial Communications Customer Preference Regulations,2018
[30] Reserve Bank Of India (RBI)Guidelines, available at https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721

- **National Health Data Management Policy, 2020:**

  Provides guidelines for the protection of sensitive health data.[31] It protect sensitive health data by ensuring informed consent, data minimization and secure handling information. It supports the right to privacy under Article 21 by safeguarding confidentiality and individual control over health data.

8. **The Digital Personal Data Protection Act, 2023:**
   - The Digital Personal Data Protection Act [32]safeguards personal data processed within India, irrespective of its origin. Additionally, the Act extends its protection to the personal data of India citizens, even if the processing occurs outside India.

CHAPTER 4

COMPLIANCE CHALLENGES AND IMPLEMENTATION GAPS IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

4.1. Criticism of Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act,2023 (DPDP Act) is an landmark step towards safeguarding personal data in India's rapidly evolving digital landscape. Critics argue that the Act's definitions lack clarity, its provisions for government exemptions and cross-border data transfers are overly discretionary, and its enforcement mechanisms are inadequate to deter large-scale data breaches. Moreover, the DPDP Act's limited focus on emerging technologies such as artificial intelligence and biometrics leaves critical privacy risks unaddressed. Digital Personal Data Protection, while essential, has faced criticism and scrutiny for various reasons. Here are some common criticisms of data protection efforts:[33]

4.2. Definitional Issues (Section 2)

Section 2's definitions have drawn criticism foe being imprecise, which could cause confusion in interpretation and application. For example, the definition of "harm" in Section 2(12) is too broad and encompasses ambiguous expressions like "reputational harm" and "denial of service".[34]

Furthermore, it is unclear from the word "personal data" if encrypted, derived, or pseudonymized material is included, which may cause data fiduciaries to interpret it differently. Additionally, the idea of "significant data fiduciaries" is not well defined, lacking any precise criteria or boundaries for categorization, which may result in uneven implementation across sectors.

4.3. Data Breach Notification (Section 9):

The lack of urgency in Section 9(4)'s requirement that data fiduciaries notify the Data Protection Board in the event of a data breach is a significant departure from the GDPR, which requires breach notifications within 72 hours (Article 33)[35]. Additionally, the Act does not distinguish between minor and major breaches and does not offer specific guidance on notification formats, risk assessment, or content requirements. Lastly, there is no mandatory requirement to notify affected individuals about breaches, which limits transparency and prevents individuals from taking proactive measures to mitigate potential harm.

[31] National Health Data Management Policy, 2020: available at hiips://abdm.gov.in:8081/uploads/health_management_policy_bac9429a79.pdf

[32] The Digital Personal Data Protection Act, 2023

[33] Mr. Abishek Tiwari ; "A step forward? Upacking the Gaps and government overreach in the Digital Personal Data Protection Act,2023"; Indian Journal of Integrated Research in Law ; Volume V Issue V .

[34] Digital Personal Data Protection Act,2023

[35] Digital Personal Data Protection Act,2023

Although it is first step towards India's data protection framework, the DPDP Act needs to be greatly improved in order to fill important loopholes. To guarantee strong privacy protection, efficient compliance, and significant recourse for impacted parties, the Act must be in line with international best practices like the GDPR, which are characterized by extensive government exclusions, ambiguous definitions, and law enforcement mechanisms. For the Act to successfully protect digital privacy in India, these issues must be resolved.

4.4. Ineffectiveness of Regulations:

Critics argue that the DPDP Act's regulatory framework could not be sufficient to fully address privacy infractions and data breaches. Although the Act lays forth data protection principles, businesses that engage in careless or malevolent data practices may not necessarily be strongly discouraged by its enforcement procedures and penalties.

- The DPDP Act's Section 25 outlines penalty for non-compliance, which can reach Rs.250 crore. However, unlike the GDPR, which levies fines of up to Euro 20 million or 4% of global revenue (Article 83), there are worries that this flat penalty method ignores the extent of harm or the global turnover of giant digital businesses,
- Reactive enforcement, in which infractions are dealt with only after harm has been caused, may result from the absence of clear norms for proactive monitoring and auditing of businesses data activities.

Although there aren't many significant precedents under the DPDP Act in India, cases like Cambridge Analytica (UK)[36] show how weak enforcement can make privacy violations worse. In some jurisdictions, tech companies were able to misuse personal data without incurring significant penalties.

4.5. Emerging Technologies and their Challenges:

Critics point to the Digital Personal Data Protection Act's lack of vision in tackling the problems presented by cutting-edge technologies pose particular risks, such as:

- The potential misuse of biometric data, like facial recognition, for unauthorized surveillance or identity theft.
- The absence of specific provisions for automated decision-making, which may affect data principal's rights.
- Profiling and behavioural tracking which are common in AI system and result in discriminatory outcomes.

There are gaps in oversight for cutting-edge data applications because the Digital Personal Data Protection Act does not specifically provide safeguards for automated decision-making and profiling, unlike the GDPR, which addresses these cases under Article 21. Section 4 describes the general principles of processing but does not go into regulating advanced technologies like AI.

- **Challenges:**

  As seen by international incidents like Clearview AI (USA)[37]. Where face recognition technology was used for mass monitoring, creating serious privacy issues, the lack of specific regulations for developing technologies result in regulatory uncertainty and possible harm.

[36] Info. Comm'r's Off., Investigation into the Use of Data Analytical in Political Campaigns (Nov6,2018), https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

[37] ACLU VS Clearview AI, Inc., No. 2020-CH-04353(III. Cir. Ct. May 28, 2020)

4.6. Government Intervention:

The Central Government is given discretionary rights by the Act, including the ability to categorize important data fiduciaries. There may be worries about possible government meddling in data protection issues as a result of this discretionary power. It will be essential to strike the correct balance between business liberty and regulatory scrutiny. Although the Act's current version appears to protect personal data, there may be issues with how the requirements are practically implemented.

For example, Section 36 gives the Central Government the authority to request "such information" from the Board or any Data Fiduciary or intermediary as it sees fit. When examined through a legislative perspective, such broad vocabulary and extensive power would demonstrate the Central Government's long-standing desire to monitor.

Furthermore, Section 17(2)(a) gives the Central Government the authority to exclude any state instrumentality from the strictures of the laws pertaining to the processing of personal data[38].

Furthermore, the RTI Act's balance between privacy and informational rights will be lost because Section 44(3) of the Act amends Section 8(1)(j) of the Right to Information Act,2005 (RTI Act). This is because the authority of a Public Information Officer (PIO) has been expanded, allowing them to deny an application submitted under the RTI Act on the grounds that the information requested pertains to personal data.

4.7. Enforcement Mechanisms:

A key component of the DPDP Act is the creation of the Data protection Board of India (Section 19) as the main regulatory body. However, the Board's operational independence, resources, and transparency are critical to its effectiveness.

Concerns:

- ★ A single centralized authority may not be able to manage the scope and complexity of data protection issues in a diverse nation like India, according to critics.
- ★ Limited Redressal Mechanisms; Although the Board handles complaints, the absence of provisions for local supervisory bodies (akin to the GDPR'S decentralized system under Article 51) may make it more difficult for people in rural areas to access the board.
- ★ Judicial oversight; Fairness and accountability issues may arise if there are unclear rules for judicial review of the Board's judgments.

The Supreme Court of India stressed the significance of a strong data protection regime in justice K.S. Puttaswamy vs Union of India (2017) in order to preserve the basic right to privacy. Critics fear that the Board's limited independence and authority may not be entirely consistent with the values outlined in the ruling.

4.8. Consent Management

To guarantee their efficacy in managing and rescinding consent, the notion of consent managers, which was introduced in the Act, needs more explanation. The ability of data principals to manage their data may be impacted by ambiguities in this area. Before processing children's data, 2023 data fiduciaries are required by Section 9 of the DPDP to get parent's or guardian's verifiable consent. Targeting for children and damaging data processing are also prohibited by the Act. However, certain organizations, such as healthcare and educational institutions, may be exempt from age gating regulations and the needs for verifiable parental agreement. Additionally, based on the particular reason they must treat a child's data, certain entities may be excused from the rules on a limited basis.

[38] Digital Personal Data Protection Act, 2023

Issues:

- ★ Although the statute establishes safeguards for kid data, such as parental consent, issues with age verification and determining what constitutes harm to children still exist.
- ★ Careful handling is necessary when parents withdraw their consent or when youngsters attain the legal age of consent.
- ★ Implementation challenges may arise from things like storing biometric data and guaranteeing compatibility across multiple devices.
- ★ One of the main issues facing the business is that the legislation itself makes no recommendations about how platforms can implement age-gating.
- ★ How to accurately create a child's relationship with his or her parents is another difficulty.

The primary cause of the delay in the release of the data protection regulations, which are necessary for the DPDP Act to be operationalized, is the inability to reach a definitive decision regarding the verifiable parental consent provision. The Act's modalities depend on at least 25 of these provisions

4.9. Government Exemptions:

The Central Government has broad authority under Section 17 of the DPDP Act, which allows it to exempt any government agency from any or all of the Act's obligations. The government may provide such exclusions under Section 17(1) in the name of "public good", "public interest," "national security", or other nebulously defined goals. Critics contend that these phrases ambiguity poses serious risks of abuse or arbitrary application. For example, the wide notion of "public interest" may be used to excuse surveillance operations or exempt organizations engaged in dubious data methods. Moreover, there are no oversight procedures in place for the exemptions process. Without independent review, public consultation, or parliamentary approval, exemptions can be granted through straightforward government notices.

The DPDP Act does not outline such protections, in contrast to GDPR Article 23, which requires that exemptions adhere to fundamental privacy rights and be subject to stringent proportionality and necessity testing. The potential of long-term abuse is increased when approved exemptions are not subject to frequent evaluations. The GDPR, on the other hand, makes sure that exemptions are routinely reviewed to verify their necessity. Concerns are also raised by Section 17(2), which permits exemptions for statistical, archival, and research reasons. Such exclusions could be utilized to avoid compliance under the pretence of acceptable reasons if they lack clear definitions and bounds.

Global instances like as the PRISM surveillance program (USA), where a lack of accountability measures resulted in widespread privacy violations, demonstrate the potential for abuse of exclusions. The right to privacy, which was upheld as a basic right in justice K.S. Puttaswamy vs Union of India (2017), may be threatened by comparable situations under section 17 in India, according to critics.

4.10. Data Localization and Cross-Border Transfers

Cross-border data transfers are governed by Section16, which allows transfers to nations and territories that the Central Government notifies. The Act does not, however, specify any particular standards or guidelines for identifying these "notified" nations. This ambiguity casts doubt on the decision-making process's impartiality and transparency, especially when working with countries that might not have strong data protection laws.

The DPDP Act lacks such comprehensive requirements, in contrast to the GDPR's Article 44 – 47, which set up a strict adequacy assessment system for cross-border data transfers. According to the GDPR, third countries must exhibit sufficient data protection standards through evaluations that take into account their legal frameworks, enforcement strategies, and judicial remedies. Transfers to nations with inadequate or non-existent data are nevertheless possible because the DPDP Act lacks such requirements.

The absence of a data localization requirement for important person data is another source of dispute. The final version of the Act has weakened the stricter localization requirements included in earlier drafts. This may make it easier for global corporations to conduct business, of data breaches or disputes in other countries.

Consequences:

As demonstrated in cases such as Schrems II (CJEU,2020), where cross-border data transfers from the EU to the US were declared illegal due to insufficient protection against surveillance, the lack of strict localization and transfer measures might result in jurisdictional issues. In the absence of strong frameworks, India would encounter comparable difficulties in guaranteeing responsibility for data breaches that take place elsewhere.

4.11. Data Protection Board Structure:

The primary authority for implementing data protection regulations is the Data Protection Board of India (DPBI), which was founded in accordance with Section 19. However, there are serious questions about its independence and impartiality raised by its appointment procedure and institutional makeup. There are no legal safeguards guaranteeing the Board's independence, and it is wholly selected by the government.

The lack of particular qualifications for Board members is a point of contention. The Data Protection Board of India does not impose the same standards as the GDPR, which guarantees that supervisory authorities are made up of people with the necessary technical, legal, and privacy skills. Additionally, important stakeholders like the court, civil society, and technical specialists are not represented, which raises concerns about bureaucratic domination and possible conflicts of interest.

The Board's perceived independence and neutrality are compromised by the government's exclusive authority over the selection and removal processes. The supervisory authorities under the GDPR, on the other hand, are set up to operate without interference from the government and have explicit measures in place to avoid conflicts of interest.

Consequences:

In the absence of sufficient protections, the Data Protection Board of India runs the risk of becoming a weak regulator that cannot hold public or private organizations responsible. In nations like the UK, where the Information Commissioner's Office (ICO) has shown how crucial independence is to efficient oversight and enforcement, lessons can be learned.

CHAPTER 5

JUDICIAL RESPONSE TO THE PROTECTION OF DIGITAL PRIVACY UNDER ARTICLE 21

5.1. The Data Protection Board of India:

The Data Protection Board of India is established under Chapter V of the Digital Personal Data Protection Act,2023. Under Section 18 of the Act, the Board is established as a statutory body. It is a body corporate, having perpetual succession and a common seal, with the power to acquire, hold, and dispose of property, and to sue or be sued in its own name.[39]

[39] Jayeeta Mandal and Yoshita Manral; "Analysis on Digital Personal Data Protection Act 2023". (academike articles on legal issues) ; www.lawctopus.com,

5.2. Nature and Composition of the Board:

The Board shall function as a digital office, meaning that its proceedings and operations are conducted in an electronic mode rather than through traditional physical hearings. The Act allows the Board to regulate its own procedure, provided it follows the principles of natural justice.

According to Section 19, the Board should consist of a Chairperson and such other Members as the Central Government may notify. The Government prescribes their qualifications, method of appointment, terms of service, and other conditions. Members are expected to possess knowledge and experience in fields such as data governance, information technology, law, public administration, or related areas.

5.3. Powers and Functions of the Board

The Board has important powers to:

- Inquire into complaints filed by Data Principals regarding violations of their rights.
- Inquire into personal data breaches reported under Section 8(6) of the Act.
- Issue directions to Data Fiduciaries or other persons to ensure compliance with the Act.
- Call for information, documents, and records necessary for conducting an inquiry.
- Summon and examine persons relevant to the proceedings.
- Impose monetary penalties where non-compliance is established.
- Issue a warning or impose costs on the complainant if the Board finds that a complaint is false or made with malicious intent,

The Board also has powers similar to those of a civil court while conducting inquiries. Under Section 28, the Board has the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in matters relating to:

- Summoning and enforcing the attendance of any person and examining them on oath.
- Requiring the discovery and production of documents.
- Receiving evidence on affidavits,
- Requisitioning public records from any office.

5.4. Penalties and Consequences of Non-Compliance

Section 33 provides that if the Board finds a breach of the Act, it may impose monetary penalties as specified in the Schedule. Below is a summary of the penalties provided in the Schedule:

Type of Violation	Maximum Penalty
Failure to take reasonable security safeguards to prevent personal data breach (Section 8(5))	Up to Rs.250 crore
Failure to notify the Board and affected Data principals of a personal data breach (Section 8(6))	Up to Rs.200 crore
Failure to fulfil additional obligations in relation to children's data (Section 9)	Up to Rs.200 crore
Failure to fulfil additional obligations of significant Data Fiduciaries (Section 10)	Up to Rs. 150 crore
Failure to comply with the duties of the Data Principal (Section 15)	Up to Rs. 10,000

Breach of any other provision of the Act not specifically listed above	Up to Rs. 50 crore

The Act follows a civil penalty model, meaning penalties are monetary and not criminal in nature.

5.5. Appellate Structure:

If a person or organisation is aggrieved by an order of the Data Protection Board, Section 29 provides the right to appeal before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within sixty days from the date of receipt of the order. The Tribunal has the power to confirm, modify, or set aside the Board's order. Further appeal lies to the Supreme Court of India on substantial questions of law.

5.6. Compliance Roadmap Under The DPDP Act And Rules

With the notification of the DPDP Rules on 14 November 2025, India's digital personal data protection framework became fully operational and entered a phase-wise compliance timeline that gives organisations and other entities time to adjust systems and adopt responsible data practices. The Rules specify an 18-month phased compliance period to allow a smooth transition to full enforcement.

Implementation Timeline:

- **14 November 2025:** Rules 1-2 (Title & Definitions) and Rules 17-21 (Administrative rules for Data Protection Board setup) are immediately active and enforceable.
- **13 November 2026:** Rules 4 (Registration of consent Managers) becomes active.
- **13 May 2027:** The 18-month compliance deadline for all substantive obligations under the DPDP Act and the Rules, such as notices, consent mechanisms, security safeguards, breach reporting, data principal rights, and obligations for Significant Data Fiduciaries (SDFs), becomes effective.

5.7. Challenges In Implementation:

Some key challenges are:

- **Updating Existing Systems:**
  Many organisation will need to redesign their websites, apps, consent forms , privacy policies, and internal systems to meet the new notice and consent requirements.
- **Managing User Rights Efficiently:**
  Companies must create simple systems for users to access, correct, erase, or withdraw consent. Handling large volumes of such requests can be difficult.
- **Data Security Readiness:**

  Organisations must strengthen their technical safeguards such as encryption, access controls, logging, and monitoring. Smaller businesses may struggle with the cost and expertise required.
- **Breach Detection and Reporting:**
  The law requires quick reporting of personal data breaches. Companies must have proper internal processes to detect breaches and inform the Board and affected individuals without delay.
- **Awareness and Training:**
  Employees and management must understand their responsibilities under the Act. Lack of awareness may lead to accidental non-compliance.

5.8. Judicial Interventions in Privacy Protection:

5.8.1. Aadhaar and Privacy:

The Aadhaar program, designed as a biometric based identity system, has been a focal point of privacy debates in India. While Aadhaar facilitates welfare delivery and financial inclusion, critics argue that mandatory linkage with bank accounts, mobile numbers and other services infringes on privacy. In **Puttaswamy vs Union of India (2018)[40],** the Supreme Court upheld Aadhaar's constitutionality but imposed limitations on its mandatory use, restricting it to Welfare Schemes. The judgment emphasized the importance of ensuring that data collection and usage comply with privacy principles.[41]

5.8.2. Pegasus Spyware Case:

The Pegasus Spyware [42]controversy raised serious concerns about unauthorized surveillance and state overreach. Reports alleged that journalists, activists, and political opponents were targeted using the sophisticated Pegasus spyware, developed by the Israeli company NSO Group. This spyware exploited vulnerabilities in devices to gain access to sensitive personal data, communications, and even control device features like cameras and microphones. These allegations led the Supreme Court of India to appoint a judicial commission to investigate the matter. The Court emphasized the importance of transparency, accountability, and adherence to constitutional principles when deploying surveillance tools, reiterating that privacy is central to a functioning democracy[43].

5.8.3. Shreya Singhal vs Union of India (2015):

The Supreme Court's judgment in **Shreya Singhal vs Union of India (2015)[44]** marked a milestone in protecting free speech and privacy in the digital era. The case involved the controversial Section 66A of the Information Technology (IT) Act, which criminalized offensive online content. Critics argued that the provision was vague and arbitrary, leading to misuse by authorities to suppress dissent. The Court struck down Section 66A, emphasizing that laws restricting free speech must not override fundamental rights. The ruling reinforced the importance of privacy and freedom of expression in the digital age.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

6.1. Conclusion:

The digital age presents both opportunities and challenges for privacy rights and data protection. The landmark Puttaswamy judgment marked a significant step forward by recognizing the right to privacy as fundamental under Article 21 of the India Constitution, setting a precedent for the protection of personal data. However, the journey towards comprehensive data protection is far from complete. The current legislative framework, including the Information Technology Act, 2000, and its amendments, needs to be strengthened to address the complexities of data privacy in today's interconnected world.

The right to privacy is a cornerstone of individual autonomy and human dignity, particularly in the digital age, where personal data is a valuable commodity. India has made significant strides in recognizing privacy as a fundamental right through landmark judgments and legislative initiatives. However, challenges such as

[40] Justice K.S. Puttaswamy vs Union of India
[41] Dr. Tanveer Kaur; "Right to Privacy in Digital Age: A study with Indian Context ";European Economic Letters;Volume 14, Issue 4 (2024)

[42] Anderson.J, (2021) The Pegasus Syware: Challenges for Global Privacy Protection. International Journal of Privacy and Surveillance ,13(2),78-95
[43] Chandrachud,D.Y.(2021). Privacy and Surveillance in India: Lessons from Pegasus. Indian Law Journal,18(1), 45-46
[44] Shreya Singhal vs Union of India (2015)

data breaches, surveillance and cybersecurity threats underscore the need for robust privacy laws. By adopting global best practices and fostering a culture of accountability, India can strike a balance between individual rights and national interests, ensuring a secure and inclusive digital future.

6.2. Recommendations:

Enact Comprehensive Privacy Legislation:

Accelerate the formulation and implementation of a robust data protection law that comprehensively addresses address issues of consent, data accountability, and user rights. The legislation should align with global standards while catering in India's unique socio-political and technological landscape.

Strengthen Regulatory Framework

Establish an independent and empowered Data Protection Authority (DPA) with the necessary autonomy and resources to enforce privacy regulations effectively. This authority should oversee compliance, investigate breaches and impose penalties to ensure accountability.

Promote Public Awareness

Launch initiatives to educate citizens about their privacy rights, safe online practices and the implications of sharing personal information. Public awareness campaigns should aim to foster a culture of informed digital behavior and vigilance against cyber threats.

Encourage Collaboration:

Foster partnerships between governments, corporations, and civil society organizations to address global and cross-border data challenges. Collaborative efforts should focus on developing shared strategies for data governance, cybersecurity, and ethical data usages.

Balance Privacy and Security

Ensure that surveillance practices are transparent, proportionate and subject to judicial and legislative oversight. Striking a balance between individual privacy rights and national security needs is critical to maintaining trust in state institutions and safeguarding democratic freedoms.

6.3. Suggestions:

Several improvements are required to achieve a balance between privacy and security. First, precise legislative definitions of "national security" and "public order" must be established. Their existing vagueness allow s for arbitrary interpretation and manipulation, weakening constitutional rights under Article 19(1)(a) and Article 21.

Second, Judicial review of nominations and decision-making should be used to strengthen the Data Protection Board's independence and ensure impartial enforcement.

Third, enacting a "Right to Data Minimization" will limit data gathering to what is absolutely essential, supporting responsible data governance and lowering abuse risks.

Furthermore, public awareness and digital literacy campaigns must be expanded to inform citizens about their data rights and potential remedies. Citizens who are empowered play an important role in preserving privacy precautions are implemented from the start rather than as an afterthought.

Finally, regular judicial audits of surveillance systems should be required to promote transparency, proportionality, and accountability in state surveillance methods.

These reforms would create a rights-based, transparent and responsible data protection policy, ensuring that technological progress does not come at the expense of individual liberty.

Bibliography

Case laws:

1. Justice K.S. Puttaswamy vs Union of India , AIR 2017 10 SCC 1
2. M.P. Sharma vs Satish Chandra (1954)
3. Kharak Singh vs State of Uttar Pradesh (1964)
4. Karmanya Singh Sareen and Anr vs Union of India and Ors(2016)
5. ACLU vs Clearview AI (USA 2022)
6. Pegasus Spyware case
7. Shreya Singhal vs Union of India (2015)

Statutes:

1. The Constitution of India, 1950
2. Digital Personal Data Protection Act, 2023
3. Information Technology Act,2000
4. IT(Reasonable Security Practice and Procedures and Sensitive Personal Data or Information) Rules,2011
5. Aadhaar(Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act, 2016
6. Right to Information Act, 2005(RTI Act)
7. The Bharatiya Nyaya Sanhita,2023
8. The Consumer Protection Act, 2019
9. Telecom Regulatory Authority of India (TRAI) Regulations,{Telecom Commercial Communications Customer Preference Regulation, 2018}

Websites:

1. https://blog.ipleaders.in/digital-personal-data-protection-act-dpdpa-2023/#

Article and Journal

1. Ananta Kr. Adhikari; “Article 21 of the Constitution of India and the Right to Privacy in the Digital Era: An Analytical Review” ;International Journal of Creative Research Thoughts(IJCRT) .www.ijcrt.org
2. Jayeeta Mandal and Yoshita Manral ; “ Analysis on Digital Personal Data Protection Act 2023”;(academike articles on legal issues) ; www.lawctopus.com,
3. Ms. Adyasha Behera &Mr. Bhanu Pratap Singh.; (safeguarding privacy in the digital Era: Balancing Rights, Security, and Innovation); ; Chanakya National Law University (CLR); (Vol V, Issue 11July-Dec.,2024)
4. Dr. Tanveer Kaur ;“Right to privacy in digital age: a study with Indian Context”; (htt://eelet.org.uk)
5. Mr. Abhishek Tiwari , “ a step forward? unpacking the gaps and government overreach the DPDP Act 2023”; Indian Journal of Integrated Research in law
6. International Centre For Information Systems and Audit, 9th edition, e-journal Data Protection And Data Privacy