LEGISLATIVE AND REGULATORY FRAMEWORK OF DATA PROTECTION IN INDIA

Anbarasi. M, B.SC, M.SC, LL.M, VISTAS, Pallavarm, Chennai.

Dr. S. Jenifer Stella, Assistant Professor & HOD, School of Law, VISTAS, Pallavarm, Chennai.

ABSTRACT

This article discusses the laws and rules related to data protection in India in today's digital world. With the growing use of the internet, mobile apps, and online services, personal data is being collected and used on a large scale. This makes the protection of personal information very important. The main aim of this study is to understand the existing legal system for data protection in India and examine how effective it is. The study is based on available laws, case decisions, and other reliable sources. It finds that although India has made progress in developing data protection laws, there are still some issues such as lack of clarity, weak enforcement, and low public awareness. Problems like misuse of data and difficulties in regulating data across borders also continue. The article suggests that stronger laws and better implementation are needed to protect people's privacy while allowing digital growth. The article concludes that there is a need for a more comprehensive, transparent, and effective framework to ensure the protection of individual privacy while supporting technological growth and innovation.

Keywords: Data Protection, Privacy, Digital Law, Personal Data, India, Regulation

INTRODUCTION

"The protection of personal data and digital privacy has become a central concern in contemporary legal systems, particularly in light of rapid technological advancements and the increasing reliance on digital platforms. As individuals engage in various online activities, vast amounts of personal data are generated, collected, and processed by both governmental and private entities. This has necessitated the development of a robust legal framework to regulate such activities and ensure the protection of individual privacy." "In India, the legislative and regulatory framework governing data protection has evolved gradually in response to emerging technological challenges and the growing recognition of privacy as a fundamental right. Unlike certain jurisdictions that have historically adopted comprehensive data protection regimes, India initially relied on fragmented legal provisions to address issues related to data security and privacy. Early efforts were primarily focused on facilitating electronic transactions and regulating cyber activities, rather than establishing a comprehensive framework for the protection of personal data." "The enactment of the Information Technology Act, 2000 marked the first significant legislative attempt to address issues arising from the use of digital technologies. While the primary objective of the Act was to provide legal recognition to electronic transactions and promote e-commerce, it also introduced certain provisions relating to data protection. However, these provisions were limited in scope and did not provide a comprehensive mechanism for safeguarding personal data. Over time, the limitations of this framework became increasingly apparent, particularly in the context of rapid digitalization and the growing importance of data in economic and governance activities." In addition to statutory laws, the regulatory framework governing data protection in India also includes subordinate legislation and guidelines issued by various authorities. the rapid evolution of technology presents new challenges that require continuous adaptation of legal frameworks. The chapter also identifies the challenges and gaps in the existing framework, providing a critical foundation for the analysis and recommendations presented in the subsequent chapter.

2. CONSTITUTIONAL PROVISIONS RELATED TO PRIVACY

"The Constitution of India does not explicitly recognize the right to privacy as a fundamental right. However, through progressive judicial interpretation, privacy has been firmly established as an intrinsic part of the constitutional guarantee of life and personal liberty. The development of privacy jurisprudence in India reflects a gradual evolution from a restrictive interpretation

of fundamental rights to a more expansive and rights-oriented approach, particularly in response to changing societal needs and technological advancements." "The primary constitutional foundation for privacy is found in Article 21 of the Constitution, which guarantees that no person shall be deprived of their life or personal liberty except according to procedure established by law.

Over time, the Supreme Court has interpreted Article 21 in a broad and dynamic manner, extending its scope beyond mere physical existence to include the right to live with dignity.29 Privacy, as an essential aspect of dignity and autonomy, has therefore been read into Article 21 as a necessary condition for the meaningful exercise of personal liberty."

"In the early phase of constitutional interpretation, the Supreme Court adopted a narrow approach towards the recognition of privacy. In M.P. Sharma v. Satish Chandra, the Court dealt with the issue of search and seizure and held that the Constitution did not explicitly provide for a right to privacy.30 The Court refused to import the concept of privacy from other jurisdictions, particularly the United States, thereby limiting the scope of constitutional protection. This decision reflected a formalistic interpretation of fundamental rights, focusing strictly on the text of the Constitution." "A similar approach was adopted in Kharak Singh v. State of Uttar Pradesh, where the Court examined the validity of police surveillance measures.31 The majority held that the right to privacy was not a guaranteed fundamental right under the Constitution. However, the case is significant for the dissenting opinion of Justice Subba Rao, who recognized privacy as an essential component of personal liberty. His opinion emphasized that unauthorized intrusion into an individual's private life violates the dignity and freedom guaranteed under the Constitution. Although this view was not accepted at the time, it laid the foundation for future developments in privacy jurisprudence.

"The judicial approach began to shift with the decision in Gobind v. State of Madhya Pradesh, where the Supreme Court acknowledged that the right to privacy could be derived from Article 21 and other fundamental rights.32 The Court recognized that privacy is not an absolute right but may be subject to reasonable restrictions based on compelling state interests. This marked an important transition from outright denial to conditional recognition of privacy as a protected constitutional interest. Further expansion of privacy rights was observed in R. Rajagopal v. State of Tamil Nadu, where the Court addressed the issue of unauthorized publication of personal information.33 The Court held that individuals have a right to safeguard the privacy

of their personal life, and that the publication of such information without consent would constitute a violation of privacy. This case extended privacy protection to the domain of media and personal reputation, reinforcing the idea that privacy is essential for maintaining individual dignity." "In People's Union for Civil Liberties (PUCL) v. Union of India, the Supreme Court dealt with the issue of telephone tapping and recognized that the interception of communications constitutes a serious invasion of privacy.34 The Court emphasized that such actions must be carried out in accordance with established procedures and subject to safeguards to prevent misuse. This decision highlighted the importance of procedural safeguards in protecting privacy against arbitrary state action." "The most significant development in the constitutional recognition of privacy occurred in the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India.35 In this case, a nine judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution. The Court explicitly overruled the earlier decisions in M.P. Sharma and Kharak Singh to the extent that they denied the existence of a fundamental right to privacy.The Puttaswamy judgment represents a transformative moment in Indian constitutional law".

"The Court held that privacy is intrinsic to life and personal liberty under Article 21 and is also closely connected to other fundamental rights, including the freedoms guaranteed under Article 19. It emphasized that privacy is essential for the protection of individual autonomy, dignity, and freedom of choice.

The judgment recognized multiple dimensions of privacy, including bodily privacy, informational privacy, and decisional autonomy, thereby providing a comprehensive understanding of the concept." "Importantly, the Court in Puttaswamy laid down a threefold test to determine the validity of any infringement of privacy. It held that any restriction on privacy must satisfy the requirements of legality, necessity, and proportionality. This means that there must be a valid law authorizing the restriction, the restriction must serve a legitimate state purpose, and it must be proportionate to the objective sought to be achieved. This framework has become a cornerstone for evaluating state actions affecting privacy." In addition to Article 21, other constitutional provisions also contribute to the protection of privacy. Article 19, which guarantees freedoms such as speech and expression, movement, and association, is closely linked to privacy. The ability to exercise these freedoms meaningfully requires a private sphere free from unwarranted interference. Similarly, Article 14, which guarantees equality before the law, plays an important role in preventing arbitrary and discriminatory state actions

that may infringe upon privacy. "The recognition of privacy as a fundamental right has significant implications for the development of data protection law in India. It imposes a positive obligation on the state to enact laws that protect personal data and regulate its processing. The Supreme Court in Puttaswamy explicitly highlighted the need for a robust data protection framework to address the challenges posed by digital technologies. This observation has influenced legislative developments, including the enactment of the Digital Personal Data Protection Act, 2023." "Moreover, the constitutional recognition of privacy extends beyond protection against state intrusion to include safeguards against violations by private entities. In the digital age, private corporations play a significant role in collecting and processing personal data, often on a large scale. The constitutional framework thus requires the state to regulate such activities and ensure that individuals' privacy rights are adequately protected."

"In conclusion, the constitutional provisions related to privacy in India demonstrate a dynamic and evolving jurisprudence that has adapted to changing societal and technological conditions. From an initial reluctance to recognize privacy as a fundamental right, the judiciary has progressively expanded the scope of constitutional protection to include privacy as an essential component of life and personal liberty. The landmark Puttaswamy judgment has firmly established privacy as a fundamental right, providing a strong foundation for the development of data protection laws and policies. As India continues to navigate the challenges of the digital age, the constitutional framework will play a crucial role in ensuring the effective protection of privacy and personal data."

'INFORMATION TECHNOLOGY ACT, 2000 AND DATA PROTECTION'

"The Information Technology Act, 2000 represents India's first comprehensive legislation addressing issues arising from the use of digital technologies. Enacted primarily to provide legal recognition to electronic transactions and facilitate e-commerce, the Act also contains certain provisions relating to data protection and privacy.

However, these provisions were introduced in a limited and fragmented manner, reflecting the early stage of digital regulation in India at the time of its enactment." Initially, the Information Technology Act, 2000 did not contain explicit provisions dealing with data protection.

"To operationalize Section 43A, the government introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)

Rules, 2011 (commonly referred to as the SPDI Rules).38 These rules represent a significant step in defining the scope of data protection under the Information Technology Act. They specify the types of information that qualify as "sensitive personal data," including passwords, financial information, health conditions, sexual orientation, and biometric information." "The SPDI Rules impose several obligations on body corporates handling sensitive personal data. These include the requirement to obtain consent before collecting data, the obligation to inform individuals about the purpose of data collection, and the duty to ensure that data is used only for lawful purposes.39 The rules also mandate the implementation of reasonable security practices, such as adherence to internationally recognized standards like ISO/IEC 27001. These provisions aim to enhance data protection by establishing minimum standards for data handling and security. the data protection framework under the Information Technology Act has been subject to significant criticism. One of the major limitations is its narrow scope, as the provisions primarily apply to "body corporates" and do not adequately cover government entities. This creates a gap in the protection of personal data, particularly in cases involving state surveillance and data collection." "The enforcement mechanism under the Information Technology Act is also relatively weak. While the Act provides for adjudicating officers and appellate tribunals, the lack of specialized regulatory bodies and limited enforcement capacity has hindered effective implementation. Additionally, the penalties imposed under the Act are often considered insufficient to deter large-scale data breaches and violations."

PERSONAL DATA PROTECTION INITIATIVES IN INDIA

"The development of a comprehensive data protection framework in India has been a gradual and evolving process, shaped by judicial recognition of privacy as a fundamental right and the increasing need to regulate the processing of personal data in a digital economy. Prior to the enactment of a dedicated data protection statute, India relied primarily on the Information Technology Act, 2000 and the rules framed thereunder, which provided limited and fragmented protection. The inadequacies of this framework, coupled with the growing importance of data in governance and commerce, led to the initiation of comprehensive legislative efforts to address data protection concerns." Based on the recommendations of the Srikrishna Committee, the Personal Data Protection Bill, 2018 was introduced as India's first comprehensive attempt to establish a data protection regime.

"The Bill was later revised and introduced as the Personal Data Protection Bill, 2019 in the

Parliament.42 The 2019 Bill incorporated several changes, including provisions relating to data localization, classification of data into personal, sensitive personal, and critical personal data, and the establishment of a Data Protection Authority. The Bill also imposed obligations on data fiduciaries to ensure transparency, accountability, and security in data processing.

However, it attracted significant criticism from various stakeholders, including concerns regarding excessive government powers, data localization requirements, and compliance burdens on businesses." "One of the key criticisms of the 2019 Bill was the broad exemptions granted to the government, particularly in the interest of national security and public order. These exemptions raised concerns regarding potential misuse of personal data and lack of adequate safeguards against state surveillance. Additionally, the requirement for data localization, which mandated that certain categories of data be stored within India, was debated extensively due to its potential impact on global data flows and business operations'. The government introduced the Digital Personal Data Protection Bill, 2022, which was later revised and enacted as the Digital Personal Data Protection Act, 2023. This new framework reflects a departure from the earlier approach, focusing on simplicity, ease of compliance, and adaptability to technological changes. It eliminates certain controversial provisions such as strict data localization requirements and adopts a more pragmatic approach to regulating data processing." 50 10 23 38 The evolution of data protection initiatives in India highlights the challenges of balancing competing interests, including individual privacy, economic growth, and national security. While the earlier drafts emphasized a comprehensive and rights-based framework similar to the European Union's GDPR, the final legislation adopts a more flexible and business-friendly approach. This shift reflects the need to create a regulatory environment that promotes innovation while ensuring adequate protection of personal data. "In conclusion, the personal data protection initiatives in India reflect a dynamic and iterative process of legal development. From the recommendations of the Srikrishna Committee to the enactment of the Digital Personal Data Protection Act, 2023, India has made substantial progress in establishing a structured framework for data protection. However, the effectiveness of this framework will depend on its implementation, enforcement, and ability to adapt to technological advancements. These developments set the stage for a detailed examination of the Digital Personal Data Protection Act, 2023, which forms the core of India's contemporary data protection regime."

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

"The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in the evolution of data protection law in India. It represents the first comprehensive legislative framework specifically designed to regulate the processing of digital personal data and safeguard the right to privacy in the digital age. The Act seeks to balance the protection of individual privacy with the need for economic development and technological innovation, thereby reflecting a pragmatic and adaptable approach to data governance." "At its core, the DPDP Act governs the processing of digital personal data, which includes data collected in digital form or digitized from non-digital sources.

The Act applies to the processing of personal data within India as well as outside India where such processing is related to offering goods or services to individuals within India. This extraterritorial application reflects the global nature of digital data flows and aligns India's framework with international standards."

"One of the key features of the Act is the introduction of the concepts of "data principal" and "data fiduciary." A data principal refers to the individual to whom the personal data relates, while a data fiduciary is the entity that determines the purpose and means of processing such data. This terminology emphasizes the fiduciary responsibility of entities handling personal data and highlights the trust-based relationship between individuals and organizations". "The Act also introduces the concept of "deemed consent" in certain situations, such as for state functions, compliance with legal obligations, and employment purposes. While deemed consent facilitates ease of data processing, it has raised concerns regarding potential dilution of individual control." "The DPDP Act provides several rights to data principals, thereby empowering individuals in relation to their personal data. These include the right to access information about the processing of their data, the right to correction and erasure of personal data, and the right to grievance redressal. The Act also provides for the right to nominate another person to exercise these rights in the event of death or incapacity. These rights aim to enhance transparency and accountability in data processing activities." In addition to rights, the Act imposes certain duties on data principals, such as the obligation to provide accurate information and not to file false or frivolous complaints. This reflects a balanced approach, recognizing that individuals also have responsibilities in the data ecosystem. "The obligations of data fiduciaries under the Act are extensive and aimed at ensuring responsible data

processing. Data fiduciaries are required to process personal data only for lawful purposes and in accordance with the consent provided by the data principal. They must implement appropriate technical and organizational measures to ensure data security and prevent breaches. In the event of a data breach, the fiduciary is required to notify both the Data Protection Board and the affected individuals.45 These provisions are intended to enhance accountability and minimize risks associated with data processing. The Act also introduces the concept of "Significant Data Fiduciaries," which are entities identified based on factors such as the volume and sensitivity of data processed, risk to individuals, and impact on national interests. Such entities are subject to additional obligations, including the appointment of a Data Protection Officer and the conduct of data protection impact assessments. This classification ensures that entities with higher risk profiles are subject to stricter regulatory scrutiny." "Another important aspect of the DPDP Act is the establishment of the Data Protection Board of India, which is responsible for enforcing the provisions of the Act. The Board has the power to inquire into data breaches, impose penalties, and issue directions for compliance. The introduction of a dedicated enforcement authority represents a significant step towards strengthening the regulatory framework for data protection in India. The Act also provides for significant penalties in cases of non-compliance. Depending on the nature and severity of the violation, penalties can extend to substantial monetary fines. This serves as a deterrent against non-compliance and encourages organizations to adopt robust data protection practices."

However, despite its comprehensive nature, the DPDP Act has been subject to criticism on several grounds. One of the major concerns is the broad exemptions granted to the government, particularly in the interest of national security, public order, and sovereignty.

These exemptions may potentially undermine the protection of privacy by allowing extensive data processing without adequate safeguards. "Another area of concern is the limited scope of rights provided to individuals compared to international frameworks such as the GDPR. For instance, the Act does not explicitly provide for rights such as data portability or the right to object to automated decision-making. This has raised questions regarding the adequacy of the Act in ensuring comprehensive protection of personal data." Additionally, the reliance on consent as the primary basis for data processing has been criticized for being ineffective in practice. In many cases, individuals may not fully understand the implications of giving consent, leading to concerns about the meaningfulness of such consent. The concept of deemed consent further complicates this issue by allowing data processing without explicit consent in

certain situations. The enforcement mechanism under the Act also raises certain concerns. While the establishment of the Data Protection Board is a positive step, questions remain regarding its independence, capacity, and effectiveness in handling complex data protection issues. Ensuring the proper functioning of the Board will be crucial for the success of the Act.

In conclusion, the Digital Personal Data Protection Act, 2023 represents a significant advancement in India's data protection framework. It introduces a structured and comprehensive approach to regulating the processing of personal data, emphasizing consent, accountability, and individual rights. However, certain limitations, including government exemptions, limited scope of rights, and enforcement challenges, highlight the need for continuous evaluation and improvement. As India continues to develop its digital economy, the effectiveness of the DPDP Act will depend on its implementation and its ability to adapt to evolving technological and societal needs.

ROLE OF REGULATORY AUTHORITIES AND REGULATORY FRAMEWORK

"The effectiveness of any data protection regime depends not only on legislative provisions but also on the strength and efficiency of its regulatory framework. In India, the regulation of data protection is characterized by a combination of statutory authorities, sector-specific regulators, and technical agencies that collectively contribute to the enforcement and implementation of data protection norms. The introduction of the Digital Personal Data Protection Act, 2023 has further strengthened this framework by establishing a dedicated regulatory body, while existing authorities continue to play complementary roles." A central feature of the current regulatory framework is the establishment of the Data Protection Board of India under the Digital Personal Data Protection Act, 2023.[1] The Board is entrusted with the responsibility of enforcing the provisions of the Act, including monitoring compliance, addressing grievances, and imposing penalties for violations. It has the power to conduct inquiries into data breaches, issue directions to data fiduciaries, and ensure that organizations adhere to the obligations prescribed under the Act.46 The creation of a specialized regulatory authority represents a significant advancement in India's data protection regime, as it provides a focused mechanism for addressing privacy-related issues.

However, the effectiveness of the Data Protection Board will depend on its independence, capacity, and operational efficiency. Concerns have been raised regarding the extent of government control over the Board, which may impact its ability to function as an independent

regulator.

Additionally, given the increasing volume and complexity of data processing activities, the Board will require adequate technical expertise and resources to effectively carry out its functions. In addition to the Data Protection Board, the regulatory framework includes the Indian Computer Emergency Response Team (CERT-In), which plays a crucial role in ensuring cybersecurity and responding to data breaches. CERT-In operates under the Ministry of Electronics and Information Technology and is responsible for collecting, analysing, and disseminating information related to cyber incidents.47 It also issues guidelines and directions for incident reporting and cybersecurity practices, thereby contributing to the protection of digital infrastructure and personal data. CERT-In's role is particularly significant in the context of data breaches, as organizations are required to report certain cyber incidents within specified timeframes. This facilitates timely response and mitigation of risks associated with data breaches. However, the focus of CERT In is primarily on cybersecurity rather than broader aspects of data protection, which highlights the need for coordination between different regulatory bodies. Sector-specific regulators also play an important role in the data protection framework. For instance, the Reserve Bank of India (RBI) regulates data protection practices in the banking and financial sector. The RBI has issued guidelines on data localization, cybersecurity, and storage of payment data, requiring financial institutions to adopt stringent security measures.48 These guidelines aim to protect sensitive financial information and ensure the stability of the financial system. Similarly, the Securities and Exchange Board of India (SEBI) regulates data protection in the securities market by mandating cybersecurity and data protection standards for market intermediaries. The Insurance Regulatory and Development Authority of India (IRDAI) also issues guidelines to ensure the protection of policyholders' data in the insurance sector. These sectoral regulators contribute to a layered regulatory framework by addressing industry specific risks and requirements. Another important component of the regulatory framework is the role of adjudicating officers and appellate mechanisms under the Information Technology Act, 2000. These authorities are empowered to adjudicate disputes relating to data breaches and impose penalties for violations of the Act.49 However, the effectiveness of this mechanism has been limited due to procedural delays and lack of specialization in handling complex data protection issues. "The regulatory framework in India is therefore characterized by a multi-layered structure, where different authorities perform complementary functions. While the Data Protection Board focuses on enforcing the provisions of the DPDP Act, other regulators address sector-specific concerns and technical

aspects of data protection. This approach allows for flexibility and specialization but also creates challenges related to coordination and consistency." "One of the key challenges in this framework is the lack of a unified regulatory approach. The presence of multiple authorities with overlapping jurisdictions can lead to confusion and inconsistency in enforcement. For example, a data breach involving financial data may fall under the jurisdiction of both the Data Protection Board and the RBI, raising questions regarding coordination and accountability." Another challenge is the issue of enforcement capacity.

Effective regulation requires not only strong legal provisions but also adequate institutional capacity to monitor compliance and address violations. The rapid growth of digital technologies and the increasing volume of data processing activities place significant demands on regulatory authorities, necessitating continuous capacity building and technological advancement.

Transparency and accountability are also critical factors in the effectiveness of regulatory authorities. Regulatory bodies must operate in a transparent manner, providing clear guidelines and ensuring that their decisions are subject to oversight. This is particularly important in the context of data protection, where regulatory actions can have significant implications for individual rights and business operations. Despite these challenges, the establishment of the Data Protection Board and the involvement of sectoral regulators represent important steps towards strengthening the regulatory framework for data protection in India. The integration of technical expertise through agencies such as CERT-In further enhances the ability of the system to respond to emerging threats.

CHALLENGES IN THE EXISTING LEGISLATIVE AND REGULATORY FRAMEWORK

"Despite significant advancements in the field of data protection, particularly with the enactment of the Digital Personal Data Protection Act, 2023, the existing legislative and regulatory framework in India continues to face several challenges. These challenges arise from structural limitations, enforcement issues, technological complexities, and the need to balance competing interests such as privacy, economic development, and national security."One of the primary challenges lies in the fragmented evolution of the data protection framework in India. Prior to the enactment of the DPDP Act, data protection was governed by the Information Technology Act, 2000 and the rules framed thereunder, which provided limited and sector-

specific protection. Even after the introduction of the DPDP Act, certain aspects of data protection continue to be regulated by different authorities and sectoral guidelines. This multi-layered structure creates issues of overlap, inconsistency, and lack of coordination among regulatory bodies, thereby affecting the overall effectiveness of the framework." Another significant challenge is related to the enforcement of data protection laws. The effectiveness of any legal framework depends on the capacity of regulatory authorities to monitor compliance and address violations. While the DPDP Act establishes the Data Protection Board of India as the primary enforcement body, concerns remain regarding its independence, resources, and technical expertise. The increasing volume and complexity of data processing activities require a highly specialized and well-equipped regulatory authority, which may be difficult to achieve in practice. "The issue of broad government exemptions under the DPDP Act also presents a major challenge. The Act allows the government to exempt certain entities from its provisions in the interest of national security, public order, and sovereignty.50 While such exemptions may be necessary in certain circumstances, their broad scope raises concerns regarding potential misuse and lack of accountability.

Excessive reliance on such exemptions may undermine the fundamental right to privacy recognized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India.51" The reliance on consent as the primary basis for data processing is another area of concern. Although the Act requires consent to be free, informed, and specific, in practice, individuals often lack the necessary understanding to make informed decisions. Privacy policies are frequently complex and lengthy, leading to "consent fatigue," where individuals agree to terms without fully comprehending them. This undermines the effectiveness of consent as a meaningful safeguard for privacy. Technological advancements further complicate the implementation of data protection laws.

The increasing use of artificial intelligence, big data analytics, and automated decision-making systems presents new challenges that are not fully addressed by the existing framework. These technologies often involve complex data processing activities that are difficult to regulate using traditional legal mechanisms. For example, algorithmic decision-making may affect individuals' rights without transparency or accountability, raising concerns about fairness and discrimination. Another important challenge is the issue of cross-border data flows. In a globalized digital economy, personal data is frequently transferred across national boundaries. While the DPDP Act allows such transfers subject to certain conditions, it also grants the

government the power to restrict data flows to specific countries. This creates uncertainty for businesses and may impact international trade and cooperation. Balancing data sovereignty with the need for global data exchange remains a complex challenge. The lack of awareness among individuals regarding their data protection rights is also a significant issue. Many individuals are not fully aware of how their data is collected, used, and shared, or of the rights available to them under the law. This limits their ability to exercise control over their personal data and reduces the effectiveness of the legal framework. Public awareness and education are therefore essential components of an effective data protection regime. Cybersecurity risks and data breaches further exacerbate the challenges in protecting personal data. The increasing frequency of cyberattacks and unauthorized access to data highlights vulnerabilities in digital systems. While the law imposes obligations on data fiduciaries to implement security measures, the dynamic nature of cyber threats requires continuous adaptation and improvement of security practices. Another challenge lies in the limited scope of rights provided under the DPDP Act. Compared to international frameworks such as the GDPR, the Act does not include certain rights such as data portability and the right to object to automated decision-making. This may limit the ability of individuals to exercise effective control over their data in a rapidly evolving digital environment. Additionally, the absence of a comprehensive framework for non-personal data creates a regulatory gap. While the DPDP Act focuses on personal data, non-personal data can also have significant implications for privacy, particularly when it is combined with other datasets. The lack of clear regulation in this area may lead to potential misuse and exploitation of data.

FINDINGS

1. The Information Technology Act, 2000 and SPDI Rules, 2011 provide only limited and fragmented protection, focusing mainly on data security rather than comprehensive data protection.

2. The enactment of the Digital Personal Data Protection Act, 2023 represents a major step towards establishing a structured data protection framework in India.

3. Despite its significance, the DPDP Act has several limitations, including: “

    i. Absence of data portability rights

ii. Broad government exemptions

iii. Lack of specific provisions for emerging technologies such as AI and big data

4. The current data protection framework in India, although evolving, remains incomplete and requires further strengthening to effectively address modern digital challenges.

SUGGESTION

Based on the findings of the study, it is suggested that the legislative and regulatory framework of data protection in India requires further strengthening to effectively address the challenges of the digital era. There is a need to develop clearer and more comprehensive legal provisions that define the scope of personal data, consent, and accountability of data handlers. The regulatory authorities should be empowered and function independently to ensure proper implementation and enforcement of data protection laws. Additionally, strict compliance mechanisms and penalties must be introduced to prevent misuse and unauthorized access to personal data. The framework should also include well-defined rules for cross-border data transfer and data localization to safeguard national interests. Furthermore, increasing public awareness and digital literacy is essential to enable individuals to understand and exercise their privacy rights. Regular updates to the legal framework are also necessary to keep pace with rapid technological advancements. Therefore, a balanced and effective approach is required to protect individual privacy while supporting technological growth and innovation.

CONCLUSION

The present study has examined the existing legal framework is not fully adequate to address the complexities of the modern digital environment. While the Digital Personal Data Protection Act, 2023 introduces important principles such as consent, accountability, and transparency, it remains limited in scope with respect to emerging technologies, enforcement mechanisms, and regulatory clarity. The study also highlights challenges relating to ineffective consent models, lack of public awareness, and the growing risks posed by technologies such as artificial intelligence and big data." The role of the judiciary has been instrumental in bridging gaps within the legal framework by developing key principles such as legality, necessity, and proportionality. Judicial interventions have ensured that privacy rights are protected against arbitrary state action and have contributed significantly to the development of digital privacy

jurisprudence. Nevertheless, the study recognizes that judicial intervention alone cannot ensure comprehensive protection, and must be supported by effective legislative and regulatory mechanisms.