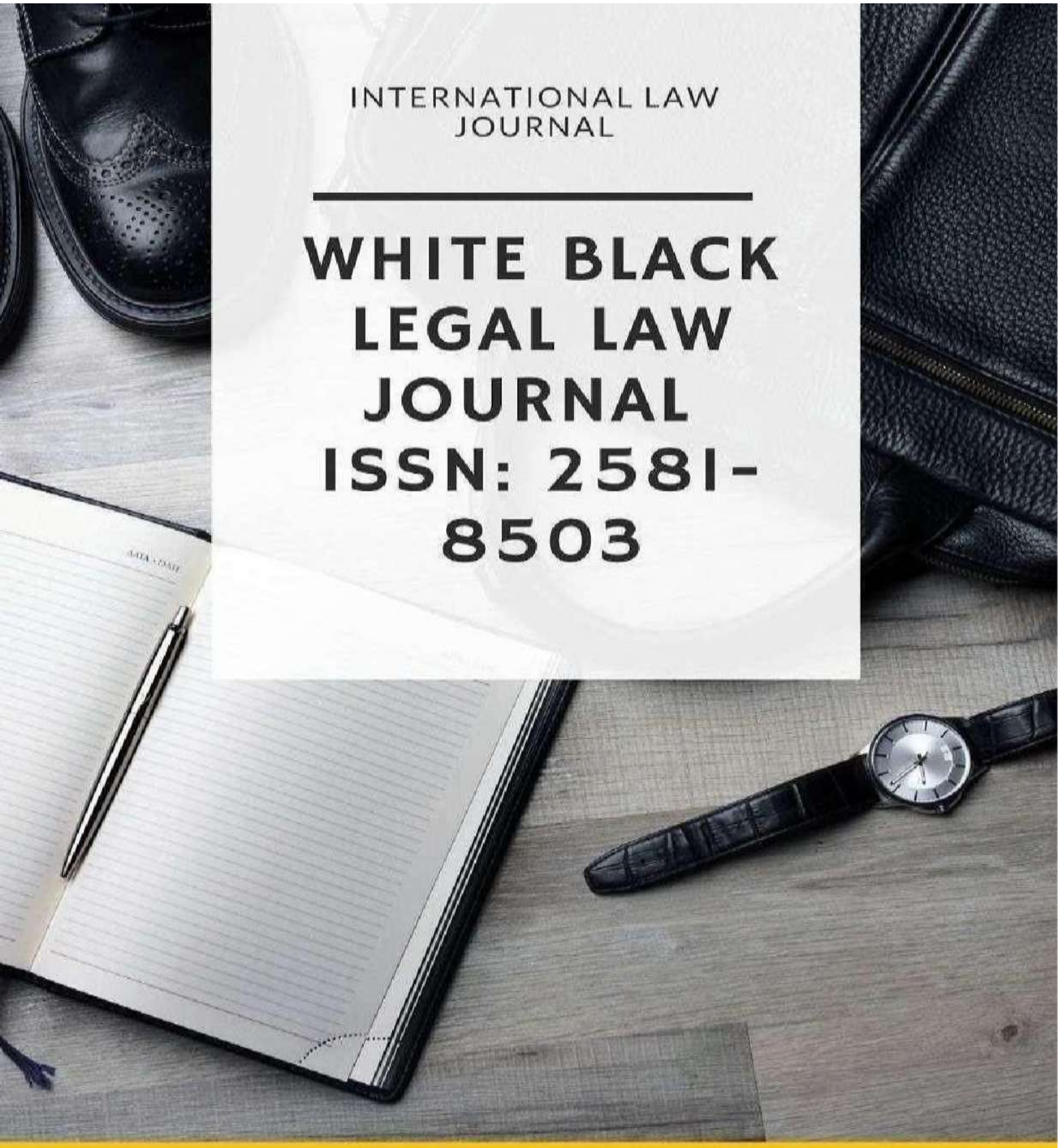

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

DATA PRIVACY AND USER CONSENT: ANALYSIS OF LEGAL FRAMEWORKS AND CHALLENGES IN INDIA

AUTHORED BY - JOHAN BIJU VARGHESE

ABSTRACT

In the digital era, data privacy and user consent have emerged as vital concerns for individuals, businesses, and governments worldwide. India's data privacy framework has been significantly shaped by the Supreme Court's judgment in *K.S. Puttaswamy v. Union of India*, which affirmed the right to privacy as a fundamental right under the Constitution.[1] This laid the foundation for the enactment of the Digital Personal Data Protection Act, 2023, marking a critical step towards personal data processing and safeguarding individual privacy. This paper critically examines the legal framework governing data privacy and user consent in India, exploring key legislations, including the Information Technology Act, 2000, and the DPDP Act, 2023.[2] It analyzes judicial precedents and compares India's regime with global standards like the European Union's GDPR. The paper also identifies the challenges in implementing data privacy laws in India, such as ensuring meaningful consent, lack of public awareness, and issues with enforcement, offering recommendations for strengthening the framework.

Keywords: Data privacy, user consent, India, Digital Personal Data Protection Act, right to privacy, GDPR, information technology law, enforcement challenges.

INTRODUCTION

Data is now considered to be one of the most important resources of the twenty-first century due to the digital revolution of economies and societies. Personal data, in particular, has emerged as a crucial asset for both businesses and governments, taken advantage of to deliver personalized services, affect customer behavior, and improve governance. But this growing reliance on personal data has also given rise to serious worries about protecting sensitive data and maintaining privacy.

[1] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India)
[2] Digital Personal Data Protection Act, No. 30 of 2023, INDIA CODE.

Over the past ten years, India's regulatory environment pertaining to data privacy has experienced a significant change. This shift was spurred by the Supreme Court's verdict in K.S. Puttaswamy v. Union of India (2017), where a nine-judge bench recognised the right to privacy as an integral component of the right to life and personal liberty under Article 21 of the Constitution. This historic ruling acknowledged that electronic privacy is just as much a part of privacy as physical areas. Following this court's approval, India draughted its first comprehensive data protection law, which resulted in the Digital Personal Data Protection Act, 2023 (DPDP Act) being passed.

Although the DPDP Act is a major step forward, there are still a lot of unanswered questions about how it will be implemented, particularly with regard to user permission. A key component of data protection regimes is consent, which gives people control over their personal data.

Securing meaningful permission, however, is made more difficult by the digital environment.

The basic goal of getting user consent might be compromised by elements such as consent fatigue, convoluted privacy regulations, and forceful methods used by data processors. Furthermore, a comparison with global best practices is necessary to comprehend the Indian data protection framework. The General Data Protection Regulation (GDPR) stipulates a stringent framework for obtaining and handling user consent, requiring it to be freely provided, informed, explicit, and unambiguous.[3] The true issue lies in adapting these international norms to India's socio-economic and technological context, which includes widespread digital illiteracy and little public awareness of data privacy rights[4], even though the country's DPDP Act heavily borrows from the GDPR.

This paper aims to explore the current landscape of data privacy laws in India, concentrating on the legal criteria for user consent, the hurdles in ensuring compliance, and the wider implications for both individuals and businesses. The analysis will be bolstered by pertinent case law and legislative updates, providing insights into how India's data protection framework can be enhanced to better protect privacy in the digital era.

[3] General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
[4] European Data Protection Board (EDPB), Guidelines on Consent under Regulation 2016/679, at 6 (2020).

I. Evolution of Data Privacy and User Consent in India

A. The Right to Privacy: A Constitutional Mandate

In the landmark decision of K.S. Puttaswamy v. Union of India (2017), the Supreme Court laid the foundation for data privacy in India. In this decision, the Supreme Court—which was composed of a nine-judge bench—clearly upheld the Indian Constitution's Article 21 right to privacy as a basic freedom. This landmark ruling declared that an individual's informational privacy is just as important as their physical integrity. The Court stressed how important it is to protect personal information in order to maintain an individual's autonomy and dignity. This acknowledgement is very important, particularly now that technology makes it possible for personal data to be collected and analysed on a large scale.The Puttaswamy ruling highlighted that any infringement on the right to privacy must satisfy the criteria of legality, necessity, and proportionality. This judicial endorsement underscored the urgent need for a legal framework to regulate data collection, storage, and processing. Following the Supreme Court's guidance, the Indian government began drafting the Personal Data Protection Bill, which led to the introduction of the DPDP Act in 2023. This Act is designed to empower individuals with greater control over their personal data while ensuring that organizations handling such data comply with strict regulatory standards.

A minimum standard mandating the state to ensure adequate protection for personal data has been set by the constitutional mandate that recognises the right to privacy. Additionally, this has spurred initiatives to strengthen privacy protections, leading to increased public scrutiny of data practices by both public and commercial entities. As a result, this legal development has impacted legislative actions and sparked a growing public discourse on data privacy issues, highlighting the significance of accountability and transparency in data processing.

B. Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 marks India's first thorough legislative effort to tackle data protection in the digital age. [5]This Act aims to oversee the handling of personal data while balancing the privacy rights of individuals with the needs of businesses and the government. It establishes key principles for processing personal data, including purpose limitation, data minimization, and the necessity of user consent[6].

[5] Digital Personal Data Protection Act, No. 30 of 2023, § 3 (India).
[6] Digital Personal Data Protection Act, 2023, § 3 (India).

1. **Purpose Limitation**: Companies are required by the DPDP Act to only gather personal data for certain, legitimate purposes that are made explicit at the time of collection. By prohibiting companies from using personal information for unknown reasons, this principle fosters openness and confidence.
2. **Data Minimization**: According to the Act, organisations must only gather the bare minimum of personal data required to fulfil the stated purpose. This idea is essential for minimising the possibility of data breaches and misuse involving personal information.
3. **User Consent**: Consent is a mandatory requirement before processing personal data. The Act specifies that consent must be free, informed, specific, and clear. This means that organizations must provide users with comprehensive information about the data processing activities and obtain explicit consent before proceeding.

   Consent is a mandatory requirement before processing personal data. The Act specifies that consent must be free, informed, specific, and clear. This means that organizations must provide users with comprehensive information about the data processing activities and obtain explicit consent before proceeding.

A Data Protection Board is also established by the DPDP Act, and its duties include monitoring compliance and imposing sanctions for legal infractions and data breachesIn order to preserve the integrity of the data protection framework and guarantee that people's rights are upheld, the Board is essential. India's approach to data privacy has undergone a substantial change with the enactment of the DPDP Act, bringing it more in line with global norms, particularly those specified by the GDPR.[7] The DPDP Act's efficacy, however, will depend on how well it is put into practice and whether a robust regulatory structure is established to support it.

C. Information Technology Act, 2000

The Information Technology Act, 2000, is still a key component of India's digital regulatory system in addition to the DPDP Act. The IT Act was initially designed to combat cybercrime and advance electronic commerce, but it has now expanded to include various aspects of digital data protection. Important safeguards for sensitive personal data were established with the adoption of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[7] General Data Protection Regulation, Regulation (EU) 2016/679, art. 83, 2016 O.J. (L 119) 1.

These Rules require organizations that gather personal data to adopt reasonable security measures to safeguard sensitive information from unauthorized access, disclosure, and misuse. Additionally, organizations must obtain user consent prior to processing sensitive personal data, which encompasses financial information, health records, and biometric data. The IT Act's focus on reasonable security practices has set a foundational standard for data protection that works alongside the more detailed provisions found in the DPDP Act.

The IT Act has come under fire for its limited scope and incapacity to provide comprehensive personal data protections. Stronger legal measures are becoming more and more necessary to protect people's rights in the digital sphere as data processing grows more complex and pervasive. By addressing the loopholes in the current legislative framework, the DPDP Act and the IT Act will be integrated to provide a more cohesive framework for data protection.

II. Key Judicial Precedents on Data Privacy and User Consent

A. K.S. Puttaswamy v. Union of India (2017)

The *Puttaswamy* case laid the essential groundwork for recognizing the right to privacy, including informational privacy, as a fundamental right in India. The Supreme Court's decision marked a pivotal moment in Indian jurisprudence, highlighting the importance of individual autonomy and dignity in the context of digital data.[8] The Court emphasized that the right to privacy encompasses the protection of personal information and the right to control the dissemination of one's data[9].

The ruling established a number of fundamental ideas that have greatly influenced the development of India's data protection legislation. Crucially, the Court found that any violation of an individual's right to privacy must satisfy the requirements of necessity, proportionality, and legality. The significance of a robust legal framework in protecting the personal information of individuals was underscored by this judicial support, which also established a clear expectation that all data processing operations must adhere to constitutional norms.

The Puttaswamy verdict has had far-reaching effects on legislative modifications as well as the general public discourse in India around privacy rights. It has given people the confidence to

[8] Anupam Chander, *India's Privacy Law: A Work in Progress*, 98 TEX. L. REV. 967, 980 (2020).
[9] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

stand out for their rights and prompted more government and corporate sector scrutiny of data practices.

b. Shreya Singhal v. Union of India (2015)

In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, which criminalized the sending of offensive messages through communication services, including social media.[10] While the case primarily addressed free speech concerns, it had significant implications for privacy rights, particularly regarding the use of social media platforms and the processing of personal data by private entities[11].

The judgment emphasized the need for laws governing the digital landscape to be clear, specific, and proportionate. The Court's ruling highlighted the dangers of vague and overly broad regulations that can infringe upon individual rights. This decision reinforced the idea that privacy rights must be protected, especially in the context of digital communication, where personal data is frequently shared and disseminated.

The *Singhal* case serves as an important reminder of the interplay between privacy and free expression in the digital age. It underscores the necessity of crafting legislation that protects both privacy and free speech rights, ensuring that individuals can engage with digital platforms without fear of undue surveillance or censorship.

c. Google India Pvt. Ltd. v. Visakha Industries (2020)

In the case of *Google India Pvt. Ltd. v. Visakha Industries*, the Supreme Court addressed the responsibilities of online intermediaries regarding third-party content. The Court ruled that intermediaries, such as Google, have certain obligations to ensure that they do not host illegal or defamatory content. This ruling raised important questions about the liability of intermediaries in cases involving the misuse of personal data[12].

The ruling made clear how crucial it is to reach a compromise between protecting user privacy and making sure that middlemen are held accountable for their part in content distribution. This

[10] Apar Gupta, *Shreya Singhal v. Union of India: The Supreme Court's Free Speech Intervention*, 9 INDIAN J.L. & TECH. 128, 140 (2015).
[11] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[12] Google India Pvt. Ltd. v. Visakha Industries, (2020) 5 SCC 162 (India)

decision highlights the necessity for precise legislative norms that regulate intermediaries' operations and serves as a crucial resource for understanding what digital platforms must do to secure users' personal information. This case demonstrates the challenges the judge has in addressing the intricacies of data privacy in a rapidly changing digital environment. It highlights the pressing need for legislation that clearly outlines the obligations of internet platforms and the safeguards that users have while using them.

III. Challenges in Implementing Data Privacy and Consent Laws

A. Ensuring Meaningful Consent

One of the biggest problems with data privacy law in the digital age is getting meaningful permission. Frequently, users must consent to extensive and intricate privacy policies without fully comprehending the consequences.[13] Many times, people click "I agree" without reading or understanding the terms that are stated in these documents. When users are inundated with requests for consent from several platforms, they may accept agreements without carefully reviewing them, a problem known as "consent fatigue" arises.

To effectively tackle this issue, the DPDP Act requires that consent be clear, specific, and informed. Organizations must offer users straightforward and understandable information regarding their data processing activities, including why data is collected and the potential risks involved. However, even with these legal obligations, putting meaningful consent into practice is still a challenge. Many organizations use complicated language and legal terms in their privacy policies, which can make it hard for the average user to fully understand what they are consenting to.The permission process is made more complicated by the dynamic nature of data processing in the digital world. The context in which consent was originally given may change as a result of organisations' continuous data collection and analysis, raising questions regarding the consent's continued validity. Simplifying privacy notifications, designing consent forms that are easy to use, and utilising technology to assist users in better understanding their options are all critical to increasing the efficacy of consent processes.

B. Lack of Public Awareness

Another significant challenge is the lack of public awareness about data privacy rights. While laws such as the DPDP Act provide individuals with the right to control their personal data,

[13] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 36 (2011).

many users are unaware of these rights or how to exercise them. This knowledge gap is particularly pronounced in a diverse country like India, where varying levels of digital literacy exist among different population segments.[14]

Many consumers may not completely understand the hazards associated with data breaches or the exploitation of their data, nor the ramifications of providing personal information online.

People may unintentionally jeopardise their privacy as a result of this ignorance when they consent to data processing operations without considering the possible repercussions.

In order to tackle this problem, extensive public education initiatives that emphasise the value of informed consent and data privacy rights must be put into place. Collaboration between public and commercial sector entities is necessary to provide easily accessible materials and instructional initiatives that enable people to take control of their data.

C. Enforcement Mechanisms

Effectively enforcing data privacy laws presents a significant challenge. Although the DPDP Act allows for the creation of a Data Protection Board, the law's success hinges on the board's independence, resources, and authority[15]. Insights from data protection authorities in other regions, like the European Union's General Data Protection Regulation (GDPR), underscore the necessity of strong enforcement mechanisms to ensure compliance and safeguard individual rights. Previous experiences with regulatory bodies in India, such as the Telecom Regulatory Authority of India (TRAI), have demonstrated that inadequate infrastructure, funding, and political commitment can hinder effective enforcement. To establish a robust enforcement framework, the Data Protection Board needs sufficient resources and personnel to fulfill its responsibilities effectively. Moreover, the Board should function independently from government influence to maintain impartiality and protect individuals' rights. Additionally, the penalties for failing to comply with data privacy laws should be substantial enough to deter violations and motivate organizations to prioritize data protection. By creating a clear and transparent enforcement mechanism, India can strengthen its data protection framework and build greater trust among individuals regarding the management of their personal data.

[14] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, 8(2) U.C. DAVIS J. INT'L L. & POL'Y 253, 260 (2012).
[15] Telecom Regulatory Authority of India (TRAI), Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (2018).

IV. Comparative Analysis: Global Standards vs. Indian Legal Framework

A. GDPR Influence

The GDPR is often seen as the benchmark for data protection worldwide, setting high standards for obtaining user consent. According to the GDPR, consent must be given freely, be informed, specific, and clear, and individuals have the right to withdraw their consent whenever they choose. Additionally, the GDPR stresses the importance of accountability, requiring organizations to prove their compliance with data protection principles.

The DPDP Act closely follows the principles laid out by the GDPR, especially regarding consent, data minimization, and purpose limitation[16]. However, India encounters distinct challenges in applying these global standards to its socio-economic context. The country's diverse population, varying degrees of digital literacy, and the commonality of informal data practices create a situation where enforcing strict data protection measures can be quite complicated.

To reconcile international standards with local realities, India needs to develop clear guidelines and best practices that are both enforceable and easy for businesses and individuals to understand. Working together with international organizations and participating in global discussions on data protection can also assist India in aligning its legal framework with global standards while taking local circumstances into account.

B. U.S. Sectoral Approach

The United States takes a sectoral approach to data protection, unlike the GDPR and India's DPDP Act, where various industries are subject to different regulations. For instance, the Health Insurance Portability and Accountability Act (HIPAA) specifically addresses healthcare data, while the Gramm-Leach-Bliley Act (GLBA) pertains to financial institutions. This fragmented system offers some flexibility but also results in gaps in comprehensive data protection.

Critics point out that the absence of a unified federal data protection law in the U.S. leads to inconsistencies in privacy protections, leaving individuals at risk of data misuse. In contrast, India's effort to establish a comprehensive framework through the DPDP Act represents a

[16] Ministry of Electronics and Information Technology (MeitY), Personal Data Protection Bill, 2019.

proactive stance on data privacy rights. However, the real challenge lies in ensuring that this framework is effectively implemented and enforced.

By analyzing the strengths and weaknesses of both the GDPR and the U.S. sectoral model, India can pinpoint areas for enhancement in its own data protection system. Creating a cohesive framework that covers all sectors while allowing for specific regulations tailored to unique contexts could be crucial for effectively safeguarding individuals' privacy rights in the digital era.

Conclusion

The issue of data privacy in India is currently at a crucial point, with the DPDP Act representing a significant step forward in the country's efforts toward comprehensive data protection. However, despite the progressive measures included in the Act, there are still considerable practical challenges in establishing a strong privacy framework. The issue of informed consent is particularly problematic in India, where digital literacy is still developing, and is further complicated by factors like consent fatigue and the use of intricate, opaque data policies by businesses.

The K.S. The Puttaswamy judgment set the foundation for a privacy-focused legal framework, but the Aadhaar case (Justice K.S. Puttaswamy v. Union of India, 2018) highlighted the difficulties in balancing state interests with individual privacy rights. While the Aadhaar scheme was upheld for specific purposes, the ruling stressed the need to protect sensitive personal data, especially regarding biometric identification. This case, along with others like Google India Pvt. Ltd. v. Visaka Industries and Shreya Singhal v. Union of India, illustrates the judiciary's changing role in interpreting privacy rights in our digital age.

In conclusion, while India's legal framework for data privacy is on the right path, it is clear that more work is needed to ensure that users can truly control their personal data in the digital age. The DPDP Act, inspired by global best practices, provides a strong foundation, but its success will depend on how effectively it is implemented and enforced. India must continue to evolve its legal and regulatory frameworks to meet the challenges of a rapidly changing digital world, ensuring that data privacy remains a fundamental right for all its citizens.[17]

[17] Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, 10(1) J.L. & INFO. SCI. 45, 50 (2018).