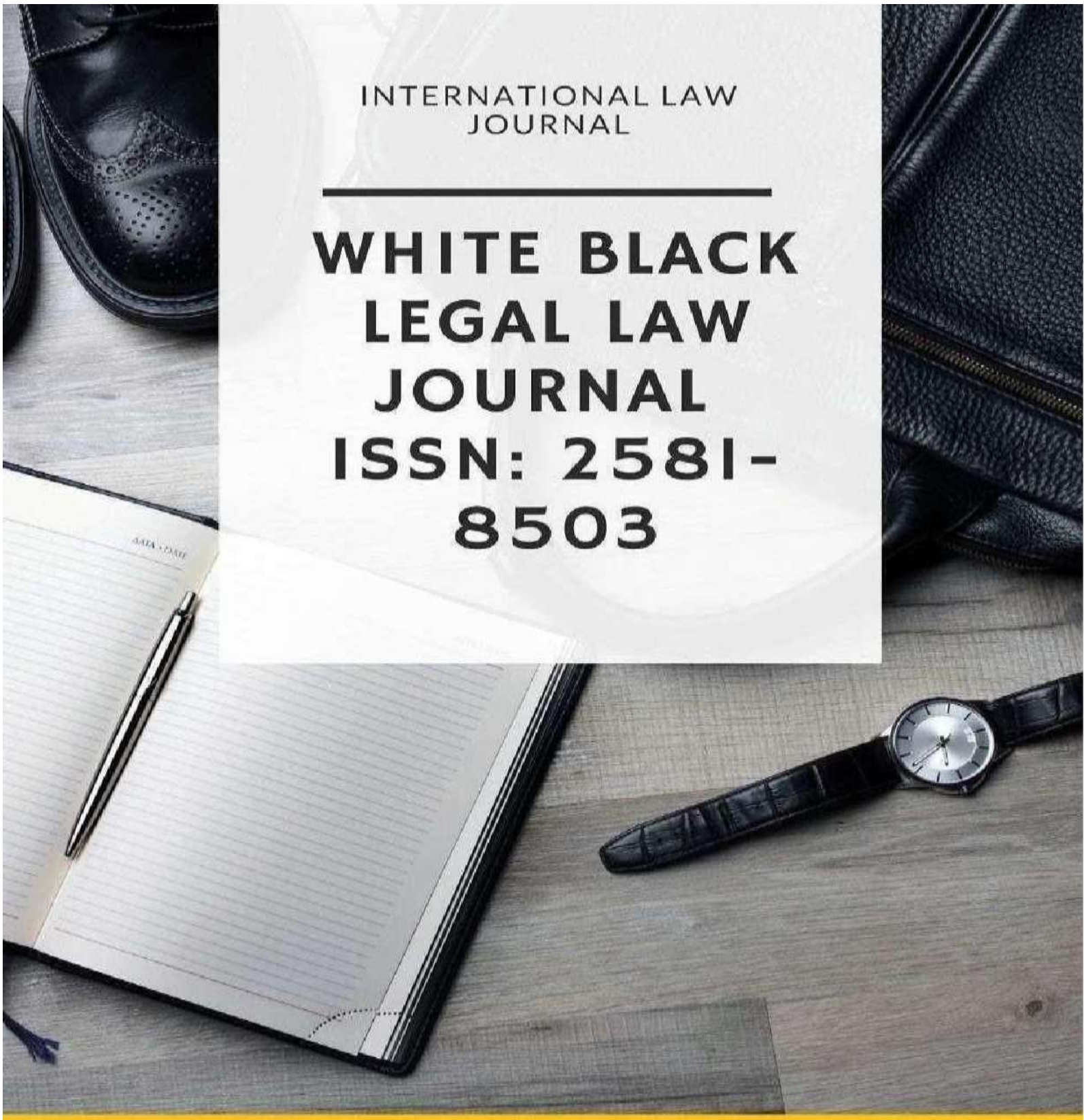

INTERNATIONAL LAW JOURNAL

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

CHILDREN DATA AND PARENTAL CONSENT VIS A VIS DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - DR. HARPREET KAUR & ASMI SHARMA

Abstract

As digital technology becomes increasingly integrated into our lives, protecting the personal data of children has emerged as a critical concern. India's Digital Personal Data Protection Act (DPDPA), 2023 represents a major step forward in addressing this issue. This paper provides a thorough analysis of how the DPDPA seeks to protect children's data, its impact, examining its main provisions, objectives, the challenges it faces and offers insights for the better implementation and strengthening of the protection of the digital personal data of the individuals, especially the children.

The introduction sets the stage by tracing the evolution of data protection laws in India. It begins with the landmark Puttaswamy case of 2017, which established privacy as a fundamental right under the Indian Constitution. Prior to this legislation, India did not have specific Act dedicated to data protection, especially including the children, although various bills had been proposed over time. These earlier efforts set the foundation for the DPDPA, which aims to provide comprehensive protection for the digital personal data of the children.

The paper details the objectives of the DPDPA, especially its provisions related to children's data protection. A key feature of the Act is the requirement for parental consent before any data from individuals under 18 can be collected or processed. This ensures that parents or guardians must approve data handling practices. Additionally, the DPDPA restricts profiling and targeted advertising, aiming to prevent misuse of children's data for commercial purposes. The Act also enforces principles of data minimization and purpose limitation, mandating that only necessary data is collected and used for its intended purpose. The study helps in evaluating how this legislation provides for the complex modern data collection practices and their implications for the privacy of children.

A significant portion of the paper involves comparing the DPDPA with international frameworks like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA). This comparison highlights both similarities and differences. For example, while the GDPR allows for a variable age of consent between 13 and 16 years, and COPPA sets it at 13, the DPDPA sets a uniform age of 18. Additionally, the paper discusses how international standards can provide valuable insights for enhancing the DPDPA's provisions. Comparing the Act with the international frameworks will ensure the identification of the areas of strength and the opportunities for improvement the respective spheres.

Despite its comprehensive approach, the DPDPA encounters several challenges. These include issues with the effectiveness of parental controls, the varying levels of awareness among parents, and difficulties in enforcing restrictions on profiling and targeted advertising. The paper also highlights concerns about data protection in less affluent and rural areas, the ethical implications of biometric data, and potential infringements on privacy rights.

To address these challenges, this paper suggests several recommendations. These include improving the processes for verifying parental consent, boosting awareness efforts among parents and guardians, and addressing digital literacy disparities. Strengthening regulatory frameworks and ensuring compliance are also crucial for the effective implementation of the Act. By addressing these areas, India can better protect children's data in a rapidly changing digital environment.

Keywords: Digital Personal Data Protection Act, 2023, Data Privacy, Children's data protection, Parental consent, profiling, data minimization, targeted advertising, digital footprints.

1. Introduction

Children, as the future of our country, are becoming increasingly immersed in the digital world, relying heavily on technology for learning, socializing, and entertainment. The internet has transformed the way we connect, communicate, and access information, presenting great opportunities but also significant risks, especially when it comes to protecting the personal data of young users. As children's digital footprints expand, they become more susceptible to the

rising dangers in the digital space, including the misuse and exploitation of their data. In response to these concerns, India has enacted the Digital Personal Data Protection Act (DPDPA) of 2023, designed to regulate how personal data is collected, processed, and stored, offering a vital framework to safeguard children's digital privacy.

1.1 Historical Background

Right to privacy has been in existence in the international arena from the *Semayne*[1] case of 1604 to the article authored by Justice Louis Brandeis and Attorney Mr. Samuel Warren titled as "The Right to Privacy". In the period that followed, the statutory recognition to privacy was given by Article 12(4) of the Universal Declaration of Human Rights (UDHR) in 1984 and then by Organisation for Economic Cooperation and Development (OECD) in its Guidelines on Protection of Privacy and Transborder flow of Personal Data in 1980. The landmark turn in the sphere of the data protection was marked on May 25, 2018 with coming into the effect of General Data Protection Regulation (GDPR).

India's journey towards enacting robust data protection laws commenced when the right to privacy was formally acknowledged as a fundamental right. Under Article 21 of the Constitution, in a landmark decision of the Supreme Court of India ruled that the right to privacy is closely linked to the right to life and personal freedom.[2] This decision made clear how urgently we need a strong legal framework in the increasingly digital age to protect personal data.

India had no specific data protection legislation that existed before this decision. Only sectoral regulations provided minimal protection against misuse of personal data, especially that of children, due to the lack of comprehensive legislation. The government realized how urgently it required to create a legal framework to handle the mounting concerns about data privacy in reaction to the Supreme Court's decision.

1.2 Origin of the Digital Personal Data Protection Act, 2023

The government started drafting a comprehensive data protection law after the Puttaswamy ruling. The first major move was the formation of the Committee of Experts on Data

[1] Peter Semayne v. Richard Gresham [1604] All ER Rep 62.
[2] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., (2017) 10 SCC 1 (India).

Protection, which Justice B.N. Srikrishna chaired. The committee aimed to provide a legislative framework for data protection in India and published a draft of the Personal Data Protection Bill (PDPB) in 2018. It was considered important for the data protection legal framework, strengthening the existing regulatory framework and influencing future legislation.[3] Over the following few years, nevertheless, the draft underwent a number of alterations and iterations.

The Personal Data Protection Bill that was introduced in 2019 faced criticism for certain provisions, and after extensive deliberations, it was referred to a Joint Parliamentary Committee (JPC) for further deliberations and examination.[4] The JPC filed its report in 2021 and made a number of recommendations, one of which was to rename the bill to the Data Protection Bill. However, this bill was similarly criticized and subsequently dropped in 2022, with the government declaring that a revised and more simplified version of the law will be presented.

The Digital Personal Data Protection Act (DPDPA) was finally passed in 2023, which was a major turning point in India's data protection history. The DPDPA is in line with international best practices for data protection and represents the progress of the legislative process by taking into account input from multiple stakeholders.

1.3 Objectives and Overview of the Digital Personal Data Protection Act, 2023

The principal aim of the DPDPA is to institute a thorough legal structure for safeguarding personal data in India. The legislation aims to strike an equilibrium between the demands of innovation, growth, and governance in the digital economy and the right to privacy. It presents important ideas including purpose limitation, data minimization, and the need for consent-particularly when handling children's data.

In accord with the DPDPA, processing children's personal data of the children, which are the individuals under the age of 18, requires parental consent. This clause is essential for protecting

[3] M. DevaPrasad et al. "The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law." *International Journal of Law and Information Technology*, 28 (2020): 1-19. https://doi.org/10.1093/ijlit/eaaa003.

[4] Dvara Research et al. "Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019." *Consumer Law eJournal* (2020). https://doi.org/10.2139/ssrn.3569465.

children's rights and interests digitally by guaranteeing that their parents or legal guardians have given their informed consent before any data about them is collected or processed. Apart from safeguarding children's data, the DPDPA also creates duties for data fiduciaries, imposes penalties for defiance and establishes a legal structure for enforcing data protection standards. In India's efforts to provide a safe and secure digital environment for all residents, especially the younger generation, the act is a major step forward.

In essence, years of discussion and legislative progress in India's data protection domain have resulted in the DPDPA of 2023. Parental consent is essential to this protective framework, which tackles the pressing need to protect children's personal data in an increasingly evolving world. The DPDPA seeks to guarantee that people's rights to privacy, especially those of children, are protected and maintained as the digital landscape develops.

2. Legal Framework Regarding the Protection of Children under The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 marks a noteworthy step in safeguarding children's data in the digital age.[5] Recognizing children's unique vulnerabilities, the act creates special measures to protect their data online. The Act seeks to protect children from the unique risks associated with the digital age by classifying anybody under the age of 18 as a child, requiring parental consent for data processing, and imposing stringent regulations on profiling and targeted advertising. This section explores these fundamental safeguards and their broader implications.

2.1 Important definitions under the Act

2.1.1 Child as defined in Section 2(f)

"(f) "child" means an individual who has not completed the age of eighteen years;" [6]

The legal bar for what qualifies as a minor is set by this definition, which makes it clear who is eligible for special protection under the Act. The statute recognizes that children may not completely comprehend the potential consequences of revealing their personal data online, thus by putting the age restriction at 18, it assures that they are provided a higher level of data protection.

[5] Anil Kumar et al. "AN ANALYSIS OF THE LAWS CONCERNING DIGITAL PRIVACY." *Russian Law Journal* (2023). https://doi.org/10.52783/rlj.v11i4s.834.
[6] Digital Personal Data Protection Act, 2023, § 2(f).

2.1.2 Data as defined in Section 2(h)

"(h) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;"[7]

The Act defines "data" as any material information or a fact that, whether directly or indirectly, can be used to identify a specific person. This includes less evident information like IP addresses or internet activities in addition to more obvious ones like names and phone numbers. By covering both physical and digital forms of information, the definition ensures that any piece of data capable of revealing someone's identity is protected under the Act. This broad scope is essential for addressing the diverse and evolving ways in which personal data is collected and used in the digital age.

2.1.3 Digital Personal Data as defined in Section 2(n)

"(n) "digital personal data" means personal data in digital form;"[8]

"Digital personal data" is defined as any personal information that is either collected, stored, or processed in a digital format. Essentially, it covers any data related to an identifiable individual that has been gathered electronically or converted into a digital form. In the current digital setting, this term is especially crucial since it makes it clear that the Act's primary goal is safeguarding personally identifiable information that is handled digitally and making sure that this data is subject to the Act's security and privacy regulations.

2.1.4 Digital Personal Data as defined in Section 2(t)

"(t) "personal data" means any data about an individual who is identifiable by or in relation to such data;"[9]

Any information that directly or indirectly relates to a specific individual who can be identified is considered personal data. This includes various types of information, such as names, contact details, and even online identifiers like IP addresses. If the data can be linked back to a person, it qualifies as personal data under the Act.

2.2 Provisions as per Section 9 of the Act

2.2.1 Consent of the parent

According to the Act, before processing a child's personal information, entities in charge of maintaining and processing personal data which are known as data fiduciaries must get

[7] Digital Personal Data Protection Act, 2023, § 2(h).
[8] Digital Personal Data Protection Act, 2023, § 2(n).
[9] Digital Personal Data Protection Act, 2023, § 2(t).

verifiable parental consent.[10] This implies that the collection and subsequent utilization of a child's data need the express consent of the child's parents or a lawful guardian in case of person with disability. It is mandatory for organizations to put in place mechanisms to confirm that the consent is genuinely from a parent or legal guardian, ensuring that the consent is legitimate and informed.

2.2.2 Restrictions on profiling and targeted advertising

The data fiduciaries are prohibited from using their data to profile children, evaluate, or forecast their behaviour.[11] This is crucial because profiling may result in the detrimental practice of using children for commercial gain or other illicit purposes. Additionally, the DPDPA forbids the use of child-specific data for advertisement targeting.[12] This guarantees that children will not be exposed to tailored advertisements that might, frequently without their knowledge, affect their actions or choices.

2.2.3 Data Minimization and Purpose Limitation Principles

As per this principle, children should only have their data collected if it is required for a particular purpose. For instance, an app should not ask for extra information like the residence of a child or school information if it just needs their name to work. The intended use of the acquired data should be limited to that purpose only. Without the child's express consent, data acquired for educational purposes shouldn't be used for other objectives, such as marketing.

2.2.4 Transparency and Accountability of Data Fiduciaries

Data fiduciaries need to be transparent about the kind of information they collect from children, why they seek it, how they plan to use it, and with whom they plan to share it. Children and their parents need to be able to understand this information when it is conveyed. Organizations' management and safeguarding of children's data is subject to accountability. They have to put in place sufficient security measures and be able to prove that they are abiding by the DPDPA's rules.

3. International Frameworks and Children's Data

As the digital world rapidly advances, protecting children's personal data has emerged as a critical issue worldwide. Various nations have implemented legal frameworks to address these challenges. India's Digital Personal Data Protection Act (DPDPA), 2023 is a pivotal step in this direction. To weigh its effectiveness, it is helpful to compare it with well-established

[10] Digital Personal Data Protection Act, 2023, § 9(1).
[11] Digital Personal Data Protection Act, 2023, § 9(2).
[12] Digital Personal Data Protection Act, 2023, § 9(3).

regulations like the General Data Protection Regulation (GDPR) of the European Union (EU) and the Children's Online Privacy Protection Act (COPPA) in the United States of America. These frameworks, recognized for their strong safeguards for children's data, provide key insights into how India's data protection laws can be strengthened. By examining differences in consent mechanisms, transparency, and protections against profiling, we can better understand the DPDPA's capacity to protect children's privacy and highlight areas for enhancement.

3.1 Age of Consent for Data Processing

DPDPA (India)

India's Digital Personal Data Protection Act (DPDPA), 2023 considers anyone under the age of 18 as a child and mandates parental consent before processing any personal data related to minors. This is a rigid rule applying to all children under 18, offering no flexibility for older teens.

GDPR (EU)

Under the GDPR, children are considered to be under 16, but EU member countries can lower this threshold to 13 for digital services, allowing more autonomy for teenagers, depending on the country. Parental consent is still required for minors below the national age of consent.

COPPA (US)

The Children's Online Privacy Protection Act (COPPA) applies to children under 13 and requires verifiable parental consent for collecting, using, or sharing children's personal data. It focuses specifically on online services directed at or knowingly collecting data from children.

Comparison: The DPDPA has a stricter consent rule, with an age threshold of 18, compared to GDPR and COPPA, which focus on younger children (16 and 13, respectively). This means India's law offers stronger protections but may limit the autonomy of older teenagers in a way that GDPR does not.

3.2 Parental Consent Mechanisms

DPDPA (India)

While the DPDPA requires parental consent, it lacks clarity on how this consent is verified, leaving room for potential gaps in enforcement.

GDPR (EU)

The GDPR mandates that consent must be verifiable, ensuring that the parent or guardian is genuinely the one giving consent, rather than the child.

COPPA (US)

COPPA has strict rules for verifiable parental consent, requiring steps such as using government-issued IDs, credit cards, or signed consent forms to confirm that the consent is truly from a parent.

Comparison: While COPPA and GDPR have strong mechanisms to verify parental consent, DPDPA is less specific, which could be a potential weakness. Adopting more rigorous verification methods, like those in COPPA, could enhance India's protection measures.

3.3 Transparency, Communication, Profiling and Targeted Advertising

DPDPA (India)

The DPDPA focuses on parental consent without specific provisions for communicating data practices in a way children can understand. It also prohibits profiling, tracking, and targeted advertising aimed at children, safeguarding them from data exploitation for commercial purposes.

GDPR (EU)

The GDPR emphasizes age-appropriate communication, requiring companies to make sure children can understand how their data is being used. Profiling and automated decision-making based on children's data are highly regulated, requiring explicit consent and ensuring that such activities are in the child's best interest.

COPPA (US)

COPPA requires privacy policies to be clear and understandable but focuses more on ensuring that parents are informed rather than directly engaging children. It strictly forbids collecting personal data from children under 13 for targeted advertising or behavioural tracking, unless there is verifiable parental consent.

Comparison: The GDPR excels in ensuring transparency and clear communication with children, while DPDPA and COPPA primarily focus on parents. DPDPA could benefit from incorporating child-friendly communication standards similar to those in the GDPR. All three frameworks offer strong protections against profiling and targeted advertising for children. DPDPA aligns closely with GDPR and COPPA but could consider adopting GDPR's more extensive restrictions on automated decision-making.[13]

[13] A. - et al. "The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis." *International Journal For Multidisciplinary Research* (2023). https://doi.org/10.36948/ijfmr.2023.v05i02.2534.

4. Challenges

Several obstacles still need to be tackled even though the Digital Personal Data Protection Act, 2023 aims to provide a strong foundation for shielding children's data through the numerous measures listed in Section 9 of the Act.[14] It is challenging to ensure that parental consent procedures are effective, particularly when it comes to confirming the authenticity of the consent given. Furthermore, there is an apparent absence of parental knowledge and comprehension of their obligations under the Act, which could prevent their kids from managing their data properly. Although necessary, the ban on profiling and targeted advertising is difficult to enforce since advertisers and internet platforms frequently use intricate algorithms that are difficult to keep an eye on. Furthermore, it might be difficult for organizations to put data minimization and purpose limitation into practice, especially those that deal with a lot of children data, such as schools and educational institutions. These organizations also have trouble complying with the act's obligations, particularly in areas with lower levels of digital literacy. Children living in low-income and rural locations may also be more susceptible to data privacy violations because of differences in their access to technology and legal knowledge. Lastly, more focus is required within the DPDPA framework to address the significant ethical and legal concerns brought up by the collection and safeguarding of biometric data, especially in relation to long-term storage and potential misuse.

4.1 Effectiveness of parental control

Before processing a child's data, the DPDPA mandates that parental consent is to be acquired. However, it can be difficult to make sure that this consent is authentic and correctly checked.[15] The efficaciousness of current mechanisms in preventing fraud or misuse, as well as how well organizations can authenticate consent as being received from a parent or guardian is still a matter of concern. The working of the verification methods in its actuality and their reliability in various demographics especially where the digital literacy is low is largely questionable.

4.2 Awareness and Understanding Among Parents and Guardians

The awareness amongst the parents and guardians regarding giving consent for sharing and managing the digital personal data of their children is substantially low. Many parents fail to

[14] Digital Personal Data Protection Act, 2023, § 9.
[15] I. Coyne et al. "Research with Children and Young People: The Issue of Parental (Proxy) Consent." *Children & Society*, 24 (2009): 227-237. https://doi.org/10.1111/J.1099-0860.2009.00216.X.

understand the potential privacy breaches,[16] the implications behind the sharing of their children's data online data footprints and thereby consent for the sharing of the data considering the stated matter as a trivial affair. They even do not consider taking any amending measures after the digital data of their children have been shared and abused in the online sphere. This makes the security of the digital personal data of the children a matter of utmost concern and a grey area in the effective implementation of the legislation.

4.3 Impact of Prohibition on Profiling and Targeted Advertising and challenges in its enforcement

In spite of the prohibition on profiling and targeted advertising by the Act, there still exists a hovering concern of its implementation. The plan of implementation is lacks practicality, especially when sophisticated algorithms have been used by the data fiduciaries to target users. The targeted advertisements have been heavily relied upon, as a primary source of revenue, by many platforms that offers free services to the users. Its prohibition by the Act will amount to the heavy loss of revenue being incurred by such platforms.

4.4 Implementation of Data Minimization and Purpose Limitation

The purpose for which the data is collected and for which the it is used by the data fiduciaries is limited by this Act. The involvement of multiple stakeholders of the data like educational institutions, third-party service providers and other governmental agencies, makes the process of data minimization quite complex and difficult to structure. The risk of the data being over-shared or repurposed increases with the increase in the number of the stakeholders involved. In addition to this, the personalization of the data as per the user also makes the implementation of the limitation of the purpose of collection of the data difficult.

4.5 Protection in low-income and rural areas

The children of low-income groups and rural areas are prone to the violation of their data privacy due to the lack of digital literacy. They have limited access to technology and almost negligible knowledge of the data protection laws. In such cases, both the parents and children fail to comprehend the rationale behind the need of parental control in context of the data privacy of the children. Certain socio-economic factors also pose a major challenge as

[16] Renee Barnes et al. "Sharenting and parents' digital literacy: an agenda for future research." *Communication Research and Practice*, 7 (2020): 6 - 20. https://doi.org/10.1080/22041451.2020.1847819.

economic pressure also compel the families to choose access to digital services over the concern for the privacy of digital data. This exposes the children to the wide open digital web where there is no protection of their personal data shared online which is widely susceptible to misuse.

4.6 Legal and ethical issues in biometric data

The sharing of the biometric data of the children includes sharing of the fingerprints of the children or the facial recognition. As the biometric data is tied to the individuality of the person, it is considered extremely sensitive in nature and is prone to hacking and identity theft. The collection, storage or processing of the biometric data of the children remains a major area of privacy concern of the children.[17] Even the parents are, sometimes, not fully aware of the long term risks involved before giving their consent. Additionally, the use of biometric data also leads to increased surveillance of the children which is a matter of ethical concern about the potential abuse and misuse of the data thus shared.

4.7 Probable infringement of Right to Privacy

The collection of data in a widespread fashion often results in the potential threat to right to privacy of the individuals, especially the children. The data collected from the children forms a part of their digital footprint which will be a part of their digital identity in their adulthood as well. This data may be used for profiling and for targeted advertisements. It may also be used for the purposed that the parents could not have comprehended and foreseen at the time of giving consent for the sharing of the digital data of their children. If this data is shared with a third party, it further attacks the privacy of the children and affects their growth and personal development, thereby making them vulnerable to exploitation and identity theft.

5. Recommendations

5.1 Strengthening parental consent mechanism

The fallacies in the process of obtaining the consent of the parents can be done away with by introduction of a number of regulatory and precautionary measures.

5.1.1 Simplified Consent Forms

It can include simplification of the consent forms by ensuring the transparency. It should

[17] S. Prabhakar et al. "Biometric Recognition: Security and Privacy Concerns." *IEEE Secur. Priv.*, 1 (2003): 33-42. https://doi.org/10.1109/MSECP.2003.1193209.

clearly state the motive and the goal for which the data will be used and the consequences of consenting to share the data. The language should not be ambiguous and clearly mention about the end that stores this information and has access to it.

5.1.2 Updates to the Parents

By apprising the parents of any change in the privacy policy, sending them notifications and updates about the usage of the digital data of their children would greatly impact the awareness and concern of the parents regarding the digital privacy of their children. They should also be given an option to remove the consent at any given point of time where they deem it unsuitable to continue with their privacy policy of the data fiduciaries.

5.1.3 Verification Mechanism

The verification of the authenticity of the consent given by the parents needs to be ensured. It encompasses the use of digital tools to verify the identity of the parents who is providing the consent. It would be beneficial in preventing any false consent without the actual knowledge of the parent.

5.2 Increasing awareness among the stakeholders

Sometimes the stakeholders, themselves, are not aware of the risks posed by the casual sharing of such sensitive data. The parents, guardians, educational institutions and even the children are oblivious of the hazards of sharing such private and sensitive information online. The awareness could be spread in a number of ways:

5.2.1 Workshops and Seminars

The involved parties must be educated of the need for data privacy and the serious implications that follows it in case of breach. This could be done in most effective manner by ways of seminars, informative sessions and workshops. These sessions should cover various facets that are included in the sphere of data protection of children such as the ways to ensure the data privacy online, potential threats of hacking and data breach, data phishing, among others.

5.2.2 Incorporation in the school curriculum

The young children should be taught in the school about the importance and confidentiality of their data and some simple techniques to protect their digital privacy. The knowledge about the data' protection laws at such a young age would further help in increasing the consciousness about the digital personal data protection in the future that follows.

5.3 Enhancing enforcement and compliance

The Digital Personal Data Protection Act, 2023 lays down a number of provisions for the

protection of the digital personal data of the children yet its enforcement mechanism remains questionable. The laws in India concerning the data protection need improvement to protect personal liberty[18] and privacy of the individuals, especially the children. For the purposes of ensuring compliance, certain measures need to be considered:

5.3.1 Audits and penalties for non-compliance

Fixing routine audits of the data fiduciaries would lead to stricter compliance with the provisions of the Act.[19] The collection, storing and use of the data, including the security measures that are necessitated by the Act would be seriously taken care of by the providing for special and regular audits of such companies and corporations. There should be a provision for strict penalties in the event of non-compliance with the provisions of the said statute. It may include fines, penalties, legal action and even the revoking of the right to collect the data from the children and other such entities. It would ensure greater compliance with the outlined rules.

5.3.2 Independent Monitoring Body

An independent statutory body needs to be constituted which will assume an important role in the enforcement of the objectives as envisaged by the Act. The body would play an important role in handling of the complaints regarding the breaches, investigation of the breaches and guidance to the organizations for practising data protection in its actual essence. The formulation of rules regarding data protection and ensuring its implementation would be ensured by such monitoring bodies at centre and state level.

5.4 Addressing socio-economic disparities

Children in low income or rural areas are often subjected to the threats of their data privacy that are connected with their poor economic condition and low social standing. They face various challenges that embodies low digital literacy rates, limited access to the technology and bleak knowledge of their rights like the right to privacy in context of their digital personal data. For the addressal of such challenges, some steps could be brought into implementation:

5.4.1 Ensuring Digital Literacy through various programmes

Government-backed instruction initiatives in digitally disconnected communities should be developed to educate children and parents regarding safe internet practices, with a special reference to privacy. In the practice scenario, programs could be offered in schools or community centres, even on sophisticated mobile units. The cost of ownership can be

[18] V. Agarwal et al. "Privacy and data protection laws in India." *International Journal of Liability and Scientific Enquiry*, 5 (2012): 205. https://doi.org/10.1504/IJLSE.2012.051949.
[19] Digital Personal Data Protection Act, 2023.

dramatically reduced by making secure digital devices and internet connections affordable or better yet subsidized in low income, rural areas. This could be a way to close the digital divide and guarantee that all children have access to what they need in order not to give away personal data.

5.4.2 Providing Financial assistance for privacy tools

Low-income families should receive financial assistance and subsidies to pay for privacy-enhancing tools, like secure browsers or parental control software. It is measures such as these that may be necessary to avoid the risk of economic consideration barring children from benefiting from the same level of data privacy protections as are being afforded by their peers.

5.5 Policy and legal recommendations

With the advancement in technology, the Digital Personal Data Protection Act, 2023 also needs to be adjust and change its provisions as per the need of the hour. Based on the gaps identified in the research, some policy and legal recommendations can be as mentioned hereunder:

5.5.1 Protection of the biometric data and stronger penalties for breach

Certain provisions for the safety of the biometric data of the children needs to be introduced. The biometric data includes fingerprints, facial recognition and so on. The provisions may embody making the requirement of consent stricter, more secure means to store the sensitive biometric data and implementation of the privacy-preserving biometric schemes,[20] popularly known as PPBS. Any breach in meeting the specified conditions should be dealt with penalties for the same

5.5.2 Right to Erasure

It is a legal right that empowers the individuals to ask for the deletion of their digital personal data from all databases, servers and software. By introducing a clause of Right to Erasure in the Act, the children should be allowed to demand for the deletion and removal of their digital personal data after they attain majority. This would enable them to correct and reverse any wrong information shared by them when they were children and when they were not able to comprehend its long-term consequences and impact.

[20] Iynkaran Natgunanathan et al. "Protection of Privacy in Biometric Data." *IEEE Access*, 4 (2016): 880-892. https://doi.org/10.1109/ACCESS.2016.2535120.

6. Conclusion

The Digital Personal Data Protection Act (DPDPA), 2023 represents a significant advancement in India's approach to protecting children's personal data. Building on the principles established by the Puttaswamy case, the DPDPA provides a comprehensive framework designed to safeguard children's digital privacy. Key provisions include mandatory parental consent, restrictions on profiling, and adherence to principles of data minimization.

The DPDPA's emphasis on parental consent is a crucial feature, requiring that parents or guardians give explicit permission before collecting or processing data from individuals under 18. This measure is intended to give parents greater control over their children's digital information and ensure it is used appropriately. Additionally, the Act's restrictions on profiling and targeted advertising aim to protect children from the commercial exploitation of their data, helping to create a safer online environment.

Despite its strengths, the DPDPA faces several significant challenges. One concern is the effectiveness of parental control mechanisms. Ensuring that parents fully understand and can manage their children's data privacy is challenging. Current provisions for verifying parental consent may not be robust enough, potentially leaving gaps. Furthermore, awareness of data protection issues among parents, particularly in rural or economically disadvantaged areas, needs improvement.

Enforcing restrictions on profiling and targeted advertising can also be difficult due to the rapid pace of technological change and the global nature of many tech companies. Although the DPDPA aligns with international frameworks such as the GDPR and COPPA, there are opportunities for enhancement. For instance, the GDPR's flexible age of consent and COPPA's stringent verification requirements offer useful lessons for refining the DPDPA.

To enhance the effectiveness of the DPDPA, several recommendations are proposed. These include refining parental consent mechanisms, increasing awareness campaigns, and addressing digital literacy gaps. Strengthening compliance measures and regulatory oversight will also be essential to ensure the Act's provisions are effectively enforced.

While the DPDPA marks a significant step forward in protecting children's digital data, its

success will depend on how well these challenges are addressed. By incorporating lessons from international best practices and adapting them to the Indian context, the DPDPA can become a more effective tool for guaranteeing the privacy and safety of information in relation to the children. The continued development and implementation of the Act will play a crucial role in safeguarding the next generation's digital rights.