INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CHILDREN'S DATA PROTECTION UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: ADEQUACY AND CHALLENGES

AUTHORED BY - DEVIKA SUNIL

Abstract

The Digital Personal Data Protection Act, 2023[1], marks an important milestone in India's ongoing effort to protect personal data, especially when it comes to children in our increasingly digital world. This Research paper takes a close look at whether the legal protections for children under this law are enough and what challenges they might face. It raises key questions about whether the current laws strike the right balance between keeping children safe, respecting their independence, encouraging innovation, and ensuring rules are practical to enforce. which is really important in the current world, here we are going to discuss a "child," the need for verified parental consent[2], and restrictions on tracking also the behavioural monitoring and targeted ads[3] aimed at kids. While these rules are designed to keep children safer online, there's concern they might have some unintended effects like overly depending on parents to control their kids' digital activity or creating difficulties for tech companies trying to follow the rules. This Research paper also considers practical challenges in putting these protections into action, such as verifying a child's age, limitations of current technology, and the lack of a detailed, risk-based approaches. It briefly compares India's law with international standards like the GDPR and COPPA, pointing out gaps and areas where Indian rules could be improved. Overall, this paper suggests that while the law is a positive step forward in protecting children's data, it needs some tweaks to work better in practice. It recommends adopting more flexible consent processes, clearer guidelines for regulators, and stronger institutions to better handle new digital risks facing children.

Keywords: Children's Data Privacy; DPDP Act 2023; Parental Consent; Age Verification; GDPR; COPPA; Data Protection Law.

[1] Digital Personal Data Protection Act, 2023
[2] Digital Personal Data Protection Act, 2023, s 9
[3] Digital Personal Data Protection Act, 2023, s 9 (3)

ISSN: 2582-6433

CHAPTER 1: INTRODUCTION

The rapid growth of digital technologies has fundamentally changed how personal data is created, gathered, and used in today's society. In India, this shift is clear in various areas such as education, entertainment, social interaction, and governance. Children are becoming active users in this digital environment, often using online platforms from a young age. While this digital involvement offers new chances for learning and connection, it also raises serious concerns about privacy, data misuse, and long-term psychological effects. On one hand, children today seem to be more tech-savvy than those in the past. Many can easily navigate digital platforms, create content, and engage with online communities. However, a closer look reveals that this familiarity with technology does not mean they understand how their personal data is collected or used. This gap between usage and understanding is especially important when we consider the commercial and algorithm-driven nature of modern digital platforms. The recognition of privacy as a basic right under Article 21[4] of the Constitution, as upheld in Justice K.S. Puttaswamy v. Union of India[5], marked a significant change in India's legal stance on data protection. The ruling established informational privacy as a key constitutional principle and highlighted the need for a strong data protection system. This is particularly crucial when the individuals affected are children, who may not have the ability to make informed decisions about their personal information. In response to these changes, the Digital Personal Data Protection Act, 2023 was enacted to regulate personal data processing and ensure accountability among data handlers. The Act includes specific rules aimed at protecting children, such as requiring verifiable parental consent and limiting tracking and behavioural monitoring[6]. At first glance, these measures seem to offer solid protection. However, this prompts an important question: does stronger protection really mean effective protection? This question becomes more critical in the context of India's socio-economic situation. There are significant gaps in digital access and literacy. Urban children may have access to advanced digital tools and parental guidance, while many others live in environments with little supervision and low awareness of data privacy. Practically, this creates challenges in applying uniform legal standards across such a diverse population. Another important factor is the increasing influence of digital platforms on children's behaviour and preferences. Content driven by algorithms, targeted ads, and data profiling can shape not just consumption patterns

[4] Constitution of India, art 21
[5] Justice K.S. Puttaswamy v. union of India (22017) 10 SCC 1
[6] Digital Personal Data Protection Act, 2023, s 9(3)

ISSN: 2582-6433

but also thought processes. This raises concerns about autonomy, manipulation, and long-term developmental impacts. We must consider whether current legal frameworks are able to manage these complex and changing risks. It can also be argued that the law's approach focuses more on control than on empowerment. By placing most of the responsibility on parents through consent requirements[7], the law assumes that parents are both willing and able to oversee their children's digital activities. However, this assumption does not hold true for everyone. Many parents may not have the digital skills needed to grasp the implications of data sharing and consent. Ultimately, this study hopes to go beyond just describing the situation. It aims to address whether the current framework strikes a reasonable balance between protection, independence, and practical implementation. This is increasingly important as digital technologies evolve and shape the experiences of younger generations.

CHAPTER 2: LITERATURE REVIEW

The issue of protecting children's data has gained increasing attention from academics and policymakers, especially as digital platforms that depend heavily on personal information continue to grow. Many studies have highlighted how children are vulnerable online, pointing to concerns like data profiling, behavioural manipulation[8], and targeted advertising[9]. However, a deeper look at this research shows that while risks are widely recognised, there is less agreement on the best way to regulate these issues. Some scholars advocate for a protection-focused approach, arguing that children aren't fully capable of understanding what they share online. They emphasise the need for strict rules, such as parental consent and limits on data use. This makes sense given the commercial interests behind data collection, but it also raises fears that overly protective rules could limit children's access to digital opportunities. This debate is especially relevant when looking at international laws like the General Data Protection Regulation (GDPR). Often seen as a balanced model, the GDPR recognises children as a special group and allows countries to set different ages for consent. Some experts see this flexibility as a recognition of children's developing understanding, but others question whether this model effectively handles the challenges of digital environments, particularly in enforcement. In the U.S., the Children's Online Privacy Protection Act (COPPA)[10] is widely discussed, mainly because of its focus on parental consent. It mainly targets younger children

[7] Digital Personal Data Protection Act, 2023, s 9(1)
[8] Sonia Livingstone and Alicia Blum-Ross, Parenting for a digital future (oxford university press 2020).
[9] OECD, Children in the digital Environment (2021)
[10] Children's online Privacy Protection Act 15 USC ss 6501-6506

ISSN: 2582-6433

and tries to avoid over-regulation by keeping its scope narrow. Still, concerns remain about how well protections extend to older minors who are active online but outside the law's strict coverage.

In India, the conversation around children's data privacy is still evolving. Earlier studies mostly focused on the right to privacy following a landmark court ruling, Justice K.S. Puttaswamy v. Union of India. That decision laid down the constitutional basis for data privacy but didn't specifically consider children's data as a separate issue. As a result, research on child-specific concerns was limited for some time. Recently, the Digital Personal Data Protection Act, 2023, has prompted scholars to explore its potential impact. Some welcome its tough stance against tracking and targeted ads, seeing it as a vital step to shield children from exploitation. Others criticize the law for its rigid rules, especially the fixed age limit and dependence on parental approval. An important gap in the existing research is the practical application of these laws, especially in countries like India. While there's plenty of talk about strict versus flexible protection, little attention has been paid to how these rules work on the ground. Issues like digital literacy[11], economic inequality, and technological capacity are often mentioned but not examined in detail, raising doubts about how well the laws can be enforced practically. Another area worth exploring is how children's data privacy ties into broader societal issues, such as surveillance and government oversight. It's clear that children's privacy cannot be viewed in isolation from bigger debates about state access to data, but this connection isn't always fully explored in existing studies. From a critical point of view, much of the literature seems to focus either on heavy protection or complete liberalization, without finding a proper balance. A more nuanced view is needed one that considers not only legal principles but also social realities and technological changes. With these points in mind, this paper aims to add a balanced and context-aware perspective to the discussion. Instead of merely asking whether laws are strict or lenient, it seeks to evaluate whether they are workable in practice, socially relevant, and legally solid within the Indian co**ntext.**

CHAPTER 3: CONCEPTUAL FRAMEWORK AND KEY LEGAL PROVISIONS

The Digital Personal Data Protection Act, 2023, sets out the main legal guidelines for handling personal data in India. It pays special attention to children, recognizing their need for extra protection. At first glance, the Act seems thorough. But a closer look reveals questions about

[11] UNESCO, Digital Literacy Framework, (2021)

ISSN: 2582-6433

some of its underlying ideas. The Act defines a "child" as anyone under 18[12] years old. This simple, uniform definition might seem helpful for regulation. Yet, it doesn't account for the different levels of maturity among minors. In India, teenagers are increasingly engaging in digital spaces like social media and online learning. Treating all children the same may overlook these differences. The requirement that data handlers must get parental consent before processing a child's data is another key point. While this aims to protect children, it also raises practical concerns. It assumes parents are always aware and capable of making informed decisions. But in many parts of India, this isn't always the case.

In theory, parental consent is a safeguard against misuse. In practice, it might become just a box to tick, not a true protection, especially when children access platforms without supervision or parents don't fully understand data risks. The Act also bans tracking, behavioural monitoring, and targeted ads aimed at children. This reflects a cautious approach intended to reduce exposure to harmful data practices. While necessary given the rise of algorithms influencing behaviour, a complete ban could be problematic. Many Indian platforms use personalized content to operate effectively. Completely banning such practices for children might cause operational issues, especially for smaller companies and start-ups with limited resources. While well-meaning, this could have unintended economic and technological effects.

Another point is that processing children's data should not harm their well-being. While this is a positive standard, the lack of a clear definition of "detrimental effect"[13] creates uncertainty about how it will be applied or enforced. Overall, the Act seems to focus heavily on restricting data use for protection. Although justified to some extent, this overlooks children as active digital participants. Instead of solely controlling data flows, empowering children with awareness and choices could be more effective.

In the Indian context, issues like digital inequality, literacy levels, and socio-economic diversity make uniform rules challenging to implement. What works in one group might not fit another while the 2023 Data Protection Act provides a structured framework aimed at protection, its underlying assumptions and practical impacts deserve careful examination. The provisions are clear in intent but raise questions about flexibility, enforcement, and relevance within India.

[12] Digital Personal Data Protection Act, 2023, s 2(3)
[13] Justice B N Srikishna Committee, A Free and Fair Digital Economic (2018)

ISSN: 2582-6433

CHAPTER 4: CRITICAL ANALYSIS OF THE ADEQUACY OF THE LEGAL FRAMEWORK

The child-specific provisions in the Digital Personal Data Protection Act, 2023, initially appear to establish a robust protective framework. The emphasis on parental consent, along with restrictions on tracking and targeted advertising, suggests a clear legislative intent to shield children from the dangers of data misuse. However, a deeper analysis indicates that assessing the adequacy of such protections requires more than just examining the intent. The critical question is whether the framework is balanced, adaptable, and practically effective within India's diverse context.

A key concern is the law's uniform classification of all individuals under eighteen as children. While this simplifies regulation, it ignores the concept of evolving capacity. Today's adolescents are not just passive users; they actively engage with digital platforms for education, communication, and even income-generating activities like content creation. This raises questions about whether uniform restrictions might unintentionally hinder their meaningful participation in the digital space.

This issue becomes even more pertinent when compared to international standards. For instance, the General Data Protection Regulation (GDPR)[14] allows for variations in the age of consent, whereas Indian law enforces a strict threshold. From a critical standpoint, such rigidity may not suit India, where social and technological exposure varies widely across regions and communities. A one-size-fits-all approach may fail to address this diversity. And the reliance on parental consent as the main safeguard. While well-intentioned, this mechanism raises practical and conceptual issues. Parental consent is not always an effective barrier; often, parents may agree without fully understanding the implications, reducing the process to a formality rather than genuine protection[15].

Furthermore, India's socio-economic landscape complicates matters. Many sections of the population still face low digital literacy levels[16], raising doubts about whether parents are positioned to make informed decisions regarding their children's data. When knowledge gaps exist, the burden of protection shifts to individuals who may lack the resources or awareness, weakening the framework's effectiveness. Restrictions on behavioral monitoring and targeted advertising also spark debate. While intended to prevent manipulation and exploitation, these

[14] Regulation (EU) 2016/678 (General Data Protection Regulation)
[15] Information Commissioner's office, Age-Appropriate Design Code (2020)
[16] NITI Aayog, Digital India Report (2023)

ISSN: 2582-6433

measures may face enforcement challenges in India due to limited resources and the sheer scale of digital activity. Many platforms operate across jurisdictions, making compliance difficult. Additionally, ambiguity in certain provisions particularly around the phrase "detrimental effect on well-being" creates uncertainty. This vague standard can lead to inconsistent interpretations and uneven enforcement, potentially undermining the law's overall impact. The broader issue of data governance also looms large. Though primarily regulating private entities, ongoing debates about government access and surveillance influence privacy discussions in India. Children's data protection cannot be fully realized without addressing these larger structural concerns related to accountability and transparency. From a critical perspective, the current framework seems to favor control over empowerment. It focuses mainly on restricting data flows rather than providing children and parents with tools to make informed choices. A more balanced approach combining legal safeguards with awareness initiatives and education—would likely be more effective over time. Considering the rapid evolution of technology, laws that are too rigid risk becoming outdated quickly. The framework's success depends not just on its current provisions but also on its capacity to adapt to new digital risks and data processing methods. In conclusion, while the Digital Personal Data Protection Act, 2023, demonstrates a strong commitment to safeguarding children's data, doubts about its adequacy remain. Its rigidity, practical implementation challenges, and lack of context-sensitive provisions suggest that a more flexible, nuanced approach is needed to balance protection with participation and innovation

CHAPTER 5: CHALLENGES IN IMPLEMENTATION

Even a well-drafted statute does not automatically translate into effective protection. The real test lies in how its provisions operate in everyday situations. In the case of the Digital Personal Data Protection Act, 2023, the gap between legal intention and practical enforcement becomes quite visible when examined closely. One of the most immediate issues is age verification. The law assumes that platforms can accurately identify whether a user is a child. In reality, most online systems still rely on basic self-declaration[17], which can be easily bypassed. This creates a situation where compliance may exist formally, but not substantively. A critical examination suggests that without reliable verification mechanisms, many of the child-specific protections remain difficult to enforce.This becomes even more relevant when viewed in the Indian context, where internet access has expanded rapidly, often without corresponding regulatory

[17] European Commission, Age Verification Study (2022)

ISSN: 2582-6433

infrastructure. Children frequently access digital platforms independently, using personal or shared devices. At this point, it is important to consider whether the law overestimates the ability of platforms to monitor users effectively, especially in a country with such a vast and diverse user base. Another challenge lies in the requirement of verifiable parental consent. While the provision appears strong on paper, its practical functioning raises several concerns. In many households, particularly outside urban areas, parents may not possess the digital literacy required to understand consent requests or privacy implications. As a result, consent may become a routine click rather than an informed decision. This weakens the very safeguard the law seeks to establish. From a critical standpoint, the assumption that parents can act as effective gatekeepers does not fully align with social realities in India. In some cases, children may be more digitally aware than their parents. In others, access to devices may not be actively supervised. This creates a disconnect between the legal model and actual behaviour patterns. The issue of digital divide[18] further complicates implementation. India's digital landscape is highly uneven, with significant differences in access, literacy, and awareness across regions. A uniform legal standard may function differently depending on these factors. This raises concerns about whether the law, in its current form, can achieve consistent results across such varied conditions. At the same time, enforcement mechanisms themselves face structural limitations. Regulatory authorities are expected to oversee compliance across a large number of digital platforms, many of which operate across borders. Monitoring such a wide ecosystem is not only resource-intensive but also technologically complex. It is submitted that without clear operational guidelines and adequate institutional capacity, enforcement may remain selective or inconsistent. The dimension that deserves attention is the economic impact on digital platforms[19], particularly smaller entities. Compliance with requirements such as consent verification and restrictions on data processing may involve significant costs. Larger companies may be able to absorb these costs, but smaller platforms and startups could struggle. This may unintentionally create an uneven playing field, affecting innovation and competition in the digital sector. This issue also intersects with broader debates around data governance and surveillance. While the Act focuses on regulating private actors, concerns about state access to data continue to be part of the larger conversation in India. The effectiveness of children's data protection cannot be fully separated from these concerns. If trust in the overall data protection framework is weak, its impact on specific groups, including children, may also be limited.

[18] International Telecommunication Union, measuring digital development (2023)
[19] World Bank, Digital Economy Report (2022).

ISSN: 2582-6433

Further, the absence of detailed regulatory clarity adds another layer of difficulty. Terms such as "detrimental effect on well-being[20]" remain open-ended. In practice, this could lead to varying interpretations by different stakeholders. From a practical perspective, such ambiguity may either result in over-compliance, where platforms act excessively cautiously, or under-compliance, where provisions are loosely applied. This becomes even more relevant when considering how quickly digital technologies evolve. New forms of data collection and interaction continue to emerge, often faster than regulatory responses. A framework that is too rigid may struggle to adapt, while one that lacks clarity may fail to guide behaviour effectively. Overall, the challenges in implementation highlight a deeper issue. The law, while comprehensive in structure, appears to rely on assumptions that may not fully align with India's social and technological realities. It is submitted that addressing these challenges requires not only legal refinement but also investment in awareness, infrastructure, and institutional capacity. Without such support, the gap between law and practice is likely to persist.

CHAPTER 6: COMPARATIVE ANALYSIS OF CHILDREN'S DATA PROTECTION FRAMEWORKS

Understanding India's approach requires looking beyond its borders. Comparing different legal systems not only highlights differences but also reveals the assumptions behind each. When examining the Digital Personal Data Protection Act, 2023 alongside international models, clear contrasts emerge. The European Union's General Data Protection Regulation (GDPR) is viewed as one of the most comprehensive data protection laws. Notably, it treats children's consent flexibly by allowing member states to set the age between thirteen and sixteen, acknowledging that children's capacity to consent changes over time. In contrast, India sets a strict age limit of eighteen years, with no variation. This difference may seem minor but reflects a deeper regulatory philosophy. The GDPR seeks to balance protection with autonomy, while Indian law tends to be more cautious. However, given India's diverse digital landscape, this blanket approach may fall short, as adolescents often engage with digital platforms in ways similar to adults. Treating all minors as equally incapable can lead to practical issues. Looking at the United States, the Children's Online Privacy Protection Act (COPPA)[21] targets children under thirteen and emphasises parental control and transparency. Unlike India's broader restrictions, COPPA takes a more focused approach, regulating specific data practices. This

[20] Digital Personal Data Protection Act, 2023, s 9(4)
[21] Children's Online Privacy Protection Act

ISSN: 2582-6433

targeted strategy has advantages and drawbacks. It prevents over-regulation, allowing older minors more freedom online, but also raises concerns about inadequate protection for teenagers who remain vulnerable. Neither total freedom nor strict controls offer a perfect answer. Each legal framework mirrors its own social and technological setting. The GDPR functions in a context of high digital literacy and strong regulatory infrastructure, while COPPA operates within specific legal and economic conditions. Therefore, adapting these models to India's unique environment is crucial rather than simply comparing them. Enforcement and awareness present additional challenges. European systems benefit from robust institutional support, whereas India continues to work on strengthening its regulatory capacity and digital literacy. A model suited for one region may not be directly transferrable.

Regulatory clarity also varies. The GDPR offers detailed guidelines that reduce ambiguity. Meanwhile, some provisions in Indian law remain open to interpretation, raising compliance concerns. This comparison prompts a broader question: should children's data be protected mainly through restrictions, or through a mix of protection and empowerment? India seems to favour restriction, while international models strive to incorporate both aspects. A purely restrictive approach may not be sustainable long-term in a fast-changing digital landscape. As we know international frameworks are not perfect. The GDPR, for example, faces criticisms over enforcement and complexity. The key isn't merely adopting a "better" model but developing one suited to local conditions. Overall, the comparison suggests India's approach is well-intentioned but could benefit from greater flexibility and context-sensitive adjustments. The challenge is balancing child protection with enabling meaningful digital engagement.

CHAPTER 7: IMPACT ON STAKEHOLDERS

The Digital Personal Data Protection Act, 2023, impacts more than just legal rules; it touches the lives of many people involved in the digital world. These include children, parents, online platforms, and authorities who oversee regulation. Looking at each group separately helps us see whether the law works in real life or just on paper. For children, the law aims to create a safer online environment by reducing risks like profiling and targeted ads. This is especially important as concerns[22] grow about online manipulation and influence. But the reality is more complex. Children today use digital platforms not just for fun but also for learning, talking to others, and expressing themselves. With online schooling and content creation becoming more popular among Indian teens, restrictions could unintentionally limit their access and

[22] NASSCOM, India tech industry report (2023)

ISSN: 2582-6433

participation. Protecting children is vital, but it needs to be balanced so it doesn't end up excluding them from opportunities tied to digital access. Parents also play a key role here. The law makes them responsible for giving consent when their children's data is used. In theory, this encourages more parental involvement, but in practice, many parents may not fully understand digital privacy risks or how to handle consent. This issue is even more pronounced in many parts of India where digital literacy is limited. Some parents might treat giving consent as a routine step rather than an informed choice. Digital platforms are directly affected as well. They must have systems to verify age, manage consent, and restrict certain data practices. Larger companies might find it easier to meet these requirements thanks to their resources. Smaller platforms and startups could struggle, which might create an uneven playing field. This raises questions about whether the law might unintentionally hinder innovation, especially in India's rapidly growing digital economy. Regulators also have a tough job. Ensuring compliance across countless platforms isn't easy, especially with a fast-expanding user base. They need clear rules, technical know-how, and strong institutions to monitor and enforce compliance. Cross-border services add another layer of complexity—platforms outside India may still use Indian user data, making enforcement a bigger challenge. The law's success will depend not just on what it says but on how well it functions within this global digital space. Beyond the legal aspect, the law influences how people relate to technology. If it builds trust, more people might feel comfortable using digital services. But if regulations seem confusing or overly strict, it could create uncertainty for users and service providers alike.

Overall, the impact of the Act varies among different groups. While it aims to protect everyone, how it actually affects individuals depends on access, awareness, and capacity. Its true effectiveness will depend not just on the law's design but also on how well it fits into India's social and technological landscape.

CHAPTER 8: TOWARDS A RISK-BASED AND RIGHTS-ORIENTED APPROACH

The framework laid out under the Digital Personal Data Protection Act, 2023, clearly emphasizes safeguarding personal data, especially through restrictions and parental controls. While these measures address certain risks, they also raise questions about whether protection alone is enough in today's fast-changing digital landscape. A more balanced approach might involve moving beyond strict safeguards toward a system that considers both risks and individual rights. Understanding this requires looking at how data processing actually works. Not all digital activities carry the same level of danger. For example, simple interactions on

ISSN: 2582-6433

educational websites may not be as risky as behavioural tracking or algorithmic profiling. This distinction becomes even more important when considering children, whose digital engagement varies widely depending on age and context. It's worth asking whether a one-size-fits-all regulation can really address this diversity. Treating all types of data processing the same way might lead to over-regulation in some areas and insufficient oversight in others. A risk-based approach could allow for tighter controls where the risks are higher, while offering more flexibility in lower-risk situations. This also ties into the idea of recognizing children as individuals with rights, rather than just subjects needing protection. In India, more adolescents are engaging with digital platforms for learning, communication, and even economic activities. Completely restricting their access might not truly reflect their role in society today. From a broader view, the current framework seems to focus more on control than on building capacity. Safeguards are important, but they shouldn't work alone. Raising awareness, promoting education, and improving digital literacy are equally important for meaningful protection especially since understanding of digital safety varies widely across India. Introducing a layered or graded consent process could be part of a more adaptable system. Instead of just focusing on 18 as a cut-off age, different levels of autonomy could be considered based on age and context. This doesn't mean removing safeguards but tailoring them to how children actually use digital tools. Looking at international examples like the GDPR, flexibility is built into the system. But simply copying such models without considering India's unique social and technological context might not work. The challenge is to adapt these ideas to fit India's particular environment. Another crucial factor is raising awareness and providing institutional support. Laws alone won't achieve their goals unless backed by initiatives like digital literacy programs, clear guidelines, and easy-to-access grievance mechanisms. Without these, even the best-designed frameworks may fall short. Ultimately, shifting toward a risk-based, rights-focused approach aims to strike a better balance between protecting children and enabling their participation. Children should be shielded from harm, but also given the freedom to explore and engage meaningfully online. All in all, the current framework, while strong in its protective intent, would benefit from more flexibility and sensitivity to context. Recognising both the risks and the capacities of children offers a more sustainable way forward.

CHAPTER 9: ROLE OF TECHNOLOGY AND AGE VERIFICATION MECHANISMS

The effectiveness of child data protection under the Digital Personal Data Protection Act, 2023 is closely tied to the technological systems that support its implementation. Legal provisions,

ISSN: 2582-6433

no matter how detailed, depend heavily on whether they can be translated into workable technical processes. This becomes particularly important in the context of age verification, which forms the foundation for applying child-specific safeguards under the Act. At a basic level, the law assumes that digital platforms are capable of identifying whether a user is a child. In practice, however, most platforms continue to rely on self-declared age information. This creates a situation where users can easily misrepresent their age, intentionally or otherwise. As a result, the distinction between child and adult users becomes blurred, making it difficult to enforce the intended protections. This issue becomes even more relevant in India, where access to smartphones and internet services has expanded rapidly across age groups. Children often use shared devices or create accounts without supervision. In such scenarios, the effectiveness of age-based regulation depends on systems that may not be reliable or widely implemented. More advanced technological solutions have been proposed, including biometric verification[23], artificial intelligence-based age estimation[24], and integration with identity databases such as Aadhaar. While these methods may improve accuracy, they introduce a new set of concerns. Collecting additional personal or biometric data for verification purposes may increase privacy risks, particularly when dealing with children. From a critical standpoint, this creates a tension between accuracy and intrusiveness. Stricter verification mechanisms may enhance compliance but could also lead to excessive data collection, which goes against the principle of data minimisation. This raises concerns about whether the solution to one problem may inadvertently create another. Another aspect that deserves attention is feasibility. Implementing advanced verification technologies requires financial resources, technical expertise, and infrastructure. Larger platforms may be able to adopt such systems, but smaller entities may find it difficult to do so. This becomes particularly relevant in India's digital economy, where startups and emerging platforms play a significant role.

At this point, it is important to consider whether uniform technological requirements are realistic in such a diverse ecosystem. A system that works effectively for large corporations may not be suitable for smaller players. This may result in uneven compliance, where some entities adhere strictly to the law while others struggle to meet basic requirements. The question of reliability also remains unresolved. Even advanced technologies are not entirely fool proof. AI-based age estimation, for example, can be affected by biases and inaccuracies. Biometric systems raise concerns about data security and misuse. This suggests that technological

[23] UIDAI, Aadhaar verification
[24] European Commission, AI and Age Verification report (2022)

ISSN: 2582-6433

solutions, while necessary, cannot be treated as complete or infallible answers. This discussion also connects to broader debates around digital identity and surveillance in India. The use of large-scale identity systems for verification purposes has been subject to ongoing scrutiny. Extending such systems to regulate children's data may intensify these concerns, particularly in relation to consent and oversight.

From a practical perspective, the success of technological implementation depends on striking a balance between effectiveness, privacy, and accessibility. Overly complex systems may discourage compliance, while overly simple ones may fail to achieve their purpose. It is submitted that technology should be viewed as a supporting tool rather than the sole solution. Legal clarity, awareness, and institutional capacity must complement technological measures. Without this combination, the gap between legal provisions and actual outcomes is likely to persist.

CHAPTER 10: JUDICIAL AND POLICY DEVELOPMENTS IN INDIA

Any conversation about data protection in India, especially when it comes to children, is deeply rooted in the country's constitutional principles. The landmark case of Justice K.S. Puttaswamy v. Union of India marked a turning point by recognizing privacy as a fundamental right. The Supreme Court's decision confirmed that individuals should have control over their personal information under Article 21, even though children were not explicitly the focus. Still, the ruling's principles apply across all age groups, including minors. This is particularly important when considering how the court views personal autonomy and dignity. Children, while needing safeguarding, are also individuals who develop their capacities over time. It's worth examining whether laws enacted afterward have struck the right balance between protecting children and respecting their growing autonomy. After the Puttaswamy case, the Justice B.N. Srikrishna Committee laid the foundation for a comprehensive data protection law. They stressed protecting personal data while supporting the digital economy's growth. The committee also recognized children as a vulnerable group that needs special protections. However, their recommendations suggested a nuanced approach, not a one-size-fits-all standard. Later legislative drafts and debates reflected these ongoing discussions about how tightly to regulate data. Over time, the focus shifted toward strengthening control measures, culminating in the Digital Personal Data Protection Act of 2023, which takes a tougher stance on children's data. From a critical perspective, this shift raises questions. While stricter protections might seem better, it's not always clear if imposing more restrictions actually leads to better outcomes. The

ISSN: 2582-6433

law still lacks detailed judicial interpretation on key issues, leaving many provisions untested and open to different interpretations in future cases. Enforcement and oversight are especially significant here. Courts will likely have to step in to clarify ambiguous parts like how consent should be managed, what constitutes well-being, and what is proportional. Until then, the real-world impact of these laws remains uncertain. Another layer to consider is India's broader policy environment, which ties data protection to governance, infrastructure, and government access to information. Discussions around surveillance and state control influence how the public perceives privacy laws. In this context, protecting children's data cannot be viewed in isolation.

While progress has been made in recognizing the importance of data rights, there's still a lot of work needed to create clear, consistent rules. Laws should reflect constitutional values but also offer straightforward guidance for those implementing them. This is especially true as technology evolves rapidly. Judicial and policy responses must keep pace with new digital realities. If they don't, the law risks falling behind the actual practices of data use India has built a solid base for data protection through legal and judicial efforts. Still, the system is in a transition phase, heavily reliant on future interpretations, regulatory decisions, and practical adaptations.

CHAPTER 11: FUTURE DIRECTIONS AND REFORM MEASURES

The current framework under the Digital Personal Data Protection Act, 2023, lays a foundation for safeguarding children's data but also raises several unresolved questions. Addressing these gaps requires looking beyond the law's text and considering how it can develop in response to practical and societal realities. One important aspect to reconsider is the uniform age threshold of eighteen years. While this provides clarity, it may not fully capture how children actually interact with digital platforms. Today's adolescents engage in online education, social interactions, and even content creation in ways that often mirror adult users. A more adaptable framework, possibly through a graded or tiered approach, could better accommodate these differences without compromising safeguards. This issue becomes even more significant when linked to consent. The current model relies heavily on parental approval, but its effectiveness depends on awareness and understanding. Often, consent is given without a clear grasp of its implications. Strengthening this process might require not just legal changes but also better communication and user-friendly design of consent systems, making them easier to understand and more meaningful in practice. Another critical area is regulatory clarity. Some concepts

ISSN: 2582-6433

within the framework, especially those related to harm or well-being, remain vague. While flexibility can be beneficial, too much ambiguity may create uncertainty for users and platforms alike. Clearer guidelines or interpretative frameworks could help reduce this uncertainty and promote consistent application. From a broader perspective, there's a need to boost institutional capacity. Effective enforcement depends not just on laws but also on technical expertise, resources, and coordination. In a country with a rapidly growing digital ecosystem, this becomes particularly crucial. Without adequate support, even well-meaning regulations may fall short of achieving meaningful results. This connects to the importance of awareness and digital literacy. Legal safeguards are only effective if people understand them. In India, where levels of digital literacy vary greatly, targeted awareness efforts can make a significant difference, including educating parents and children and ensuring platforms communicate data practices clearly and accessibly. Another aspect worth considering is how data protection ties into wider governance issues. Debates over data access, surveillance, and accountability continue to influence India's privacy landscape. Strengthening children's data protection may require addressing these larger structural challenges, as a fragmented approach could limit overall effectiveness. Recognizing that legal reform is an ongoing process is also essential. Technologies evolve rapidly, often unpredictably. A framework that is too rigid may struggle to adapt, while one that is too vague may fail to guide proper behaviour. The challenge is to find a balance between certainty and flexibility. From a practical standpoint, reform should focus on adaptability rather than purely theoretical models. Elements from international frameworks like the General Data Protection Regulation can be helpful, but they must be tailored to India's social and technological context. future reforms aim to build a system that is not only protective but also responsive to real-world conditions. This includes recognizing user differences, strengthening enforcement, and enhancing awareness alongside regulation. the way forward involves refining the current framework rather than replacing it entirely. With suitable adjustments, the existing law can develop into a more balanced and effective system for protecting children's data in India.

CHAPTER 12: CONCLUSION

The Digital Personal Data Protection Act of 2023 marks a significant step in India's ongoing efforts to protect personal data, especially emphasizing the need to shield children in our increasingly digital world. The law's framework shows genuine concern for vulnerabilities and seeks to address issues like data misuse, profiling, and targeted influence. On the surface, the

ISSN: 2582-6433

focus on parental consent and restrictions on certain data practices indicate a protective intent a closer look reveals that the situation is more complicated. The real question isn't just if protections are in place, but if they are suited to the real-world conditions they're meant to operate in. Treating all individuals under eighteen the same, along with a strict consent model, seems to lean heavily on control. While this might reduce some dangers, it also raises questions about whether such an approach truly considers the different abilities and experiences of children, especially teenagers. This issue is even more relevant in India, where digital access is growing fast but unevenly. Variations in literacy, awareness, and access mean that legal protections may work differently across communities. In such a diverse setting, relying mostly on parents to oversee and understand these safeguards assumes a level of knowledge and supervision that might not always be there. As a result, how well these rules work can vary a lot in practice.

Another important point is the challenge of enforcing these laws. India's vast digital landscape, along with technical limitations, makes consistent enforcement difficult. Tools like age verification[25] and consent management are critical in theory but face practical challenges when put into real-world use. This reveals a gap between what the law intends and what can actually be done. At the same time, it's important to recognize that the Act does set a meaningful foundation and brings attention to children's data rights within Indian law. This is especially significant given the constitutional recognition of privacy in the landmark Puttaswamy case, which highlights dignity, autonomy, and control over information. The Act is part of a broader shift in law and society. Still, the overall message suggests that protection alone isn't enough. A system that's too rigid may struggle to keep up with changing technology and social habits. Conversely, one that's too vague or inflexible may not provide clear guidance. The real challenge is finding the right balance protecting children without unnecessarily restricting their digital participation. Looking at the bigger picture, this issue ties into larger debates about how data is governed, the role of the state, and trust in digital systems. Children's data protection isn't standalone; it's part of a wider ecosystem where questions of access, control, and accountability keep evolving the Digital Personal Data Protection Act of 2023 should be viewed as a work in progress. Its success will depend on how it's understood, carried out, and refined over time. Building awareness, strengthening institutions, and updating legal provisions will all be key in shaping its future impact. In summary, while the Act makes important strides, it also underscores the complexities of regulating children's data in a diverse, fast-changing

[25] UNICEF, Policy guidance on AI for Children (2021)

ISSN: 2582-6433

society. Moving forward, the goal should not just be stronger protection but smarter, more context-aware regulation that reflects the real risks and realities of our digital age.