



EXAMINING THE PRACTICAL CHALLENGES OF AGE VERIFICATION UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Aditya Raj Choudhary*

ABSTRACT

This paper examines the feasibility gaps between the written word in legislation and the real challenges in ensuring children's safety in the digital world in light of the Digital Personal Data Protection Act, 2023 (DPDP). It specifically focused on elaborating Section 9 of the DPDP Act, 2023, and Rule 10 of the DPDP Rules, 2025, which impose obligations on data fiduciaries to obtain verifiable parental consent before processing children's data and impose strict restrictions on data fiduciaries from tracking and monitoring children's behaviour and showing targeted advertisements to children, respectively. This paper addressed real problems in society regarding age verification and the reliability of current technology for ensuring children's safety online. It discusses basic age gating and advanced age verification. This paper provides findings on loopholes or gaps between written legislation and realities in societies; it specifically addresses fake age declarations, using VPNs to bypass jurisdiction of laws, fooling available AI age-estimation tools, using parents' devices and identities by their children, etc. It also provides a comparative overview of international legal frameworks in the UK's Online Safety Act, the USA's Children's Online Privacy Protection Act and the European Union's Digital Services Act and General Data Protection Regulation, and how these laws ensure children's safety on online platforms and provide rules and regulations to ensure children's age verification by platform. This paper concludes by providing sociological and technically based recommendations to avoid practical challenges in society, such as mandatory awareness campaigns by educational institutions to narrow the digital generational gap between children and parent, government must increase expenditure on research and development in age

*BA LLB, FOURTH YEAR, UNIVERSITY OF ALLAHABAD, CMP DEGREE COLLEGE (CONSTITUENT COLLEGE OF UNIVERSITY OF ALLAHABAD).

verification mechanisms to detect various available bypass mechanisms, using multi-layer age verification mechanisms by platforms.

Keywords: Digital Personal Data Protection Act 2023, Children Online Safety, Age Verification Mechanism, Verifiable Parental Consent, Age Gating and Age Verification.

INTRODUCTION

India's Digital Personal Data Protection Act 2023 mainly focuses on regulating personal data and safeguarding children's personal data in the race of digitalisation worldwide. The law specifies a child in section 2(f)¹ of the said Act and imposes strict regulations regarding their data in comparison to adults. Under this law, companies are strictly required to obtain verifiable permission from a parent or guardian before collecting and processing a child's personal data. This ensures the safety of children's data and information and ensures it is not shared without proper authorisation of a parent or guardian.

Furthermore, this act prohibits companies from monitoring or tracking children's behaviours or displaying personalised ads to them because they can easily influence them. So, the entities that are designated to handle such data, i.e. data fiduciaries,² are mandated to implement robust security to mitigate the risk of data leaks or misuse. This is the uniform legislation that seeks to provide a safer environment in the digital world for users in India. It strengthens parental authorisations for young users who are below 18 years. It enforces strict compliance on companies to comply with this law, with heavy penalty provisions.

LITERATURE REVIEW

This paper reviews how the existing Indian laws on children's data protection are underdeveloped because the DPDP Act 2023 is a new, emerging law in India, and the DPDP Rules 2025 are secondary legislation to ensure compliance with the primary law, which is the DPDP Act. In this paper, existing legal practice sources are used as Secondary sources, such as Economic Law Practice and MediaNama, etc., to review the practical challenges in age verification. This paper also uses some non-legal sources to look into the technical methods used to bypass age verification mechanisms, like VPN. It also draws a comparative analysis among development nation with relevant laws for children's protection online, that is, the

¹ Digital Personal Data Protection Act 2023, s 2(f)

² Digital Personal Data Protection Act 2023, s 2(i)

Digital Services Act and General Data Protection Regulation in European nations, the Children's Online Privacy Protection Act in the USA, and the Online Safety Act in the UK.

RESEARCH METHODOLOGY

This paper uses doctrinal and comparative legal research methodology. It uses existing codified laws in India, i.e., Section 9 of DPDP Act 2023 and Rule 10 of DPDP Rules and International laws i.e. Article 28 of Digital Service Act and Article 8 of General Data Protection Regulation of European Union, Children Online Privacy Protection Act in USA, and Online Safety Act in UK to show existing laws in concern of children protection online as a legal and comparative part. It also uses some other blogs, reports, and resources as secondary sources, such as Economic Law Practice and MediaNama, to put evidentiary value in finding the feasibility gap in practical realities and implemented legislation.

DPDP LAW ON CHILDREN'S DATA

If we look for statutory provisions governing children's data, then Section 9³ of the DPDP Act, 2023 provides rules for restrictions and obligations on data fiduciaries regarding managing children's data; it sets out three statutory pillars, which are as follows:

Section 9(1) deals with verifiable parental consent; it casts a strict obligation on data fiduciaries to obtain verifiable authorisation from a parent or legal guardian before processing any personal data relating to a child.

Section 9(2) explicitly prohibits data fiduciaries from using any data in such a way that causes or is likely to cause a detrimental effect on the well-being of a child.

Section 9(3) puts strict restrictions on data fiduciaries from tracking or behavioural monitoring of children and strictly bans personalised or targeted ads directed to children.

Furthermore, these laws are followed under DPDP Rules 2025. Rule 10⁴ provides for the verifiable consent of a parent or legal guardian for processing children's data. It provides that the data fiduciaries shall use the appropriate technology and organisational method to ensure that verifiable consent of a parent or legal guardian is obtained before managing any children's personal data and shall observe due diligence in checking that the person who identifies himself

³ Digital Personal Data Protection Act 2023, s 9

⁴ Digital Personal Data Protection Rules 2025, r 10

as the parent is an identifiable adult; it also seems like a dual verification method. It identifies the parent by reference to reliable details of identity and age, which already exist in the platform's existing database.

Rule 10 of the DPDP Rules 2025 provides for using a virtual token mechanism to identify the authenticity of an individual, which is issued by authorised agencies or government-backed agencies.

For instance, if a child wants to sign up for a new educational platform and that platforms ask for parent's permission then instead of uploading parent's sensitive documents like Pan cards or Aadhaar cards directly to the that unknown platforms this mechanism redirect to the secure government backed platforms such as DigiLocker and then he can sign up by entering OTP which is sent on parent's phone, through this mechanism it ensures safety of both children and parents.

UNDERSTANDING AGE GATING AND AGE VERIFICATION

Generally, online platforms use two methods for confirming the online user's age: age gating and age verification.

Age Gating: Age gating is a very basic process for managing access of age restrictive content available on online platforms. It's not a very effective method because it is very easy to bypass by entering false information by users. It is mostly based on self-reporting; in this method, children fill in the wrong age details intentionally to bypass the restrictions. It relies on users' honesty. For instance, A child wants to see a sensitive video on the internet. When he clicks on that video to play, the platforms on which the video is available show a pop-up notification stating 'I am 18 years old or older,' and ask to confirm their age only by clicking on that notification; then the child may just click on it and have access to that video. That's why this method is not effective or reliable.

Age Verification: Age verification technology is a step further than age gating. It takes more advance measure to confirm an online user's age. It uses valid ID proofs to confirm a visitor's age. It can request scanning government ID proofs like an Aadhaar card, using facial recognition to match the face with ID photos and cross-checking the authenticity of the ID in the government database.

Following mechanism are use commonly for age identification:⁵

- Document-based verification like Aadhaar verification;
- Facial age estimation tools;
- Third-party trust or identity providers;
- Authenticating the adult through OTP, KYC, or other Validation tools

Age identification mechanism under the DPDP Act for managing children's data is mainly based on the aforesaid age verification mechanism; Rule 10(1)(b)(ii)⁶ of the DPDP Rule 2025 explicitly mentions that 'through a virtual token mapped to such details, which is issued by an authorised entity'. Rule 10(2)(b)(ii)⁷ explicitly mentions a Digital Locker Service Provider. Rule 10(2)(c)⁸ provides that "Digital Locker service provider" shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);

PRACTICAL CHALLENGES IN AGE VERIFICATION FOR CHILDREN ONLINE

The mere implications of bare laws do not solve practical challenges in protecting children from unregulated content available on online platforms. There are many issues in case of restricting children through age verification from accessing age-appropriate content. Children of this generation are knowledgeable and smart; when the case is using the internet, they know many techniques very well to bypass the restrictions. A Report published by MediaNama in MediaNama's roundtable discussion on 'Age Verification and Restricting Social Media for Children,' held on 15 May in Bengaluru,⁹ presented that speaker raised a few common methods used by children to bypass age verification as follows:

⁵ Ravisekhar Nair, Abhay Joshi and Bhaavi Agrawal, 'Verifiable Consent for Processing Personal Data of Children under the DPDP Act' (*Economic Laws Practice*, April 2026) <<https://elplaw.in/wp-content/uploads/2026/04/Verifiable-consent-for-processing-personal-data-of-children-under-the-DPDP-Act.pdf>> accessed 9 august 2026.

⁶ Digital Personal Data Protection Rules 2025, r 10(1)(b)(ii)

⁷ Digital Personal Data Protection Rules 2025, r 10(2)(b)(ii)

⁸ Digital Personal Data Protection Rules 2025, r 10(2)(c)

⁹ Prabhanu Kumar Das, 'Any Technical Measure Can Be Circumvented': Is It Feasible to Implement Age Verification at Scale?' (*MediaNama*, 22 May 2026) <<https://www.medianama.com/2026/05/223-age-verification-social-media-children-india/>> accessed 9 August 2026.

Fake Age Declaration: Most of the platforms rely only on a simple, unverifiable age declaration checkbox method, so children simply click on the checkbox and access the content.

Entering False Date of Birth: Most gaming apps and social media apps ask users to enter their date of birth, but the sign-up mechanism uses unverified means; children simply enter a wrong date of birth to appear as 18+ people and get access. For example, if a 12-year-old child downloads a video game that is suitable for 18+ youngsters and the gaming platform asks to enter a date of birth while creating an account for playing the game, then he may enter a wrong date of birth which is calculated as 18+, and he can easily play.

Using Parent or Guardian's Devices or Accounts: Generally, parents or guardians in the family share their own devices or social media accounts with their children, that is misused by children, and this gives the child access to restrictive content that is allowed for adults rather than children.

Using Parent Identifiers to Get Access: Children use parent-identifiable details in social media apps to log in through OTP or pass the ID verification process.

Using VPNs: Age verification laws are generally regulated by the local laws of a country. So Children are using Virtual Private Networks (VPN) to change their IP location out of jurisdiction to get access. Below are the main ways VPNs bypass age verification:

IP Masking: A VPN changes the user's real IP address to a different IP address from the VPN provider, which shows user appear in a different region. If the different region does not require age verification, the platform may skip it.¹⁰

Remote Servers and Location Obfuscation: Routing traffic through servers in other countries has the same effect. The platform sees the server's location instead of the user's own, so the age gate may not appear in places where the rules are lighter.¹¹

Residential Proxies: Some VPN and proxy services route traffic through residential IP addresses that resemble ordinary home networks. These IPs make masked traffic harder to

¹⁰ Lauren Hendrickson, 'Why VPNs Make Age Verification Harder for Websites' (*Identity.org*, 25 November 2025) <<https://www.identity.org/why-vpns-make-age-verification-harder-for-websites/>> accessed 9 august 2026

¹¹ *Ibid*

identify, allowing users to pass through systems that look for suspicious or unusual network patterns.¹²

Shifting to Unregulated Platforms: When mainstream platforms impose age restrictions on their content, children can visit unregulated platforms or third-party apps to gain access to content without any age restriction.

Fooling facial AI age estimation tools: Some platforms use AI-based facial age estimation tools, but since these AI tools are not perfect, they can be bypassed by using other means, such as using any adult images for scanning or generating their own images as an adult using other AI tools.

OTHER COUNTRIES LAWS ON CHILDREN ONLINE SAFETY

European Union: Article 28 of the Digital Services Act¹³ provides for the safeguards of children in the digital world. Article 28(1) mandates online service providers that the content which is accessible to children shall take appropriate and proportionate measures to ensure the safety and security of minors.

Article 28(2): This provision puts a strict prohibition on such providers from displaying targeted advertisements based on their profiling when they have reasonable certainty that the user is a minor.

Article 28(3) provides that compliance with this article shall not allow online service providers to collect extra personal data only to identify whether the user is a minor.

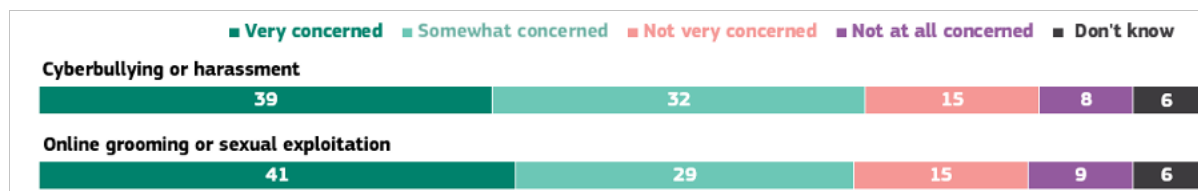
Article 28(4) provides that the European Commission may, after consulting with the Board, issue guidelines to assist the providers in the effective implications of these measures.

Article 8 of General Data Protection Regulation sets the threshold of age, if a child is above age of 16 years then he can give consent for lawful processing of children's personal data in relation to information society service, but if child is below the age of 16 then such consent is lawful for such processing if the consent is given by the adult who hold parental responsibility over the child, although the members states may lower this threshold by law to 13 years for

¹² *Ibid*

¹³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)[2022]OJ L277/1, art 28.

those purpose, further this provision mandates the data controller to make reasonable efforts to ensure that consent is obtained by person who is authorised by the holder of parental responsibility.¹⁴



Although the EU has this strong legislation, the European are faced sever failure in children's online safety; a survey shows that most children facing cyberbullying, harassment, sexual exploitation or online grooming are the biggest concern of European.¹⁵

United Kingdom: The Online Safety Act was introduced in the UK to protect minors from harmful online content relating to pornography, self-harm, suicide, and eating disorder content. To protect minors from this content, platforms are required to use age verification methods like facial scans, photo ID and credit card checks to verify the age of their users. This also ensures that strangers have no way of directly messaging children. Further, this legislation provides that, in the process of age verification, the platforms should take appropriate measures to ensure the privacy of users; they must confirm the age without collecting or storing personal data, unless it is necessary. It is explicitly provided that platforms must use safe, proportionate and secure methods, and if any platforms misuse users' personal data or do not protect users' privacy, then such platforms could face heavy penalties.¹⁶

UK also faced harmful effects on children, although they have effective legislation. The Youth Justice Board for England and Wales published a comprehensive new Evidence and Insights Pack on Online Harms Affecting Children¹⁷. Key evidence presented in this press release is that children face digital harms, cyberbullying, sexual abuse, radicalisation and exploitation;

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 8

¹⁵ European Commission, 'EU Challenges and Priorities' (*Eurobarometer*, July 2026) <<https://europa.eu/eurobarometer/surveys/detail/3677>> accessed 10 August 2026.

¹⁶ Department for Science, Innovation and Technology, 'Keeping Children Safe Online: Changes to the Online Safety Act Explained' (*GOV.UK*, 1 August 2025) <<https://www.gov.uk/government/news/keeping-children-safe-online-changes-to-the-online-safety-act-explained>> accessed 10 August 2026.

¹⁷ Youth Justice Board for England and Wales, 'New Evidence on Online Harms Affecting Children' (*GOV.UK*, 25 June 2026) <<https://www.gov.uk/government/news/new-evidence-on-online-harms-affecting-children>> accessed 10 August 2026.

sharing of intimate images is normalised among children, which cause increasing in the sexual exploitation of girls digitally.

United States of America: The Children's Online Privacy Protection Act (COPPA) 1998 governs children's online safety in the USA. It was enacted in 1998 and came into force on 21 April 2000; it is managed by the Federal Trade Commission (FTC). It aims to protect children under the age of 13. Specifically, it applies to platforms of commercial websites, online services, mobile apps, plug-ins and IoT devices that collect personal information from children.¹⁸ Some examples of the information that COPPA protects are as follows:

- Full name
- Home address
- Email address
- Phone Numbers
- Social Security numbers
- IP address
- Geolocation data
- Behavioural data

Key provisions of COPPA¹⁹ are as follows:

Privacy Policy and Direct Notice: Platforms shall have a clear, comprehensive and easily accessible privacy policy about their information processing of children's data; they must deliver a direct notice to the parents before collecting data.

Verifiable Parental Consent: Platforms must ensure that parental consent is obtained before processing any data relating to the child under the age of 13.

Data Minimisation: Platforms are not allowed to collect unreasonable and unnecessary information from children in that activity.

¹⁸ The Ultimate Guide to the Children's Online Privacy Protection Act (COPPA)' (*Kiteworks*)
<<https://www.kiteworks.com/risk-compliance-glossary/coppa-childrens-online-privacy-protection-act/>>
accessed 10 august 2026

¹⁹ *Ibid*

Confidentiality and Security: Platforms are directed to ensure the safety and security of collected personal information of children and take all appropriate measures to protect the confidentiality of data.

Data Retention Limits: Platforms are only authorised to retain personal information collected from children as long as it is necessary to fulfil the purpose for which it is collected, and after the accomplishment of the purpose, they must delete the information with proper care.

Parental Rights: Upon parents' request, platforms must provide the collected personal information of the child, with the ability to review, delete and refuse any further collection of data of their children.

FTC Oversight: The Children's Online Privacy Protection Act is managed by the Federal Trade Commission, and this commission has authority to issue rules and bring enforcement action against non-compliant platforms.

RECOMMENDATIONS FOR AVOIDING CHALLENGES

Platforms should not rely on simple self-declaration checkboxes for age verification. They can use multi-layer verification to ensure that the user is not a minor.

Platforms must ensure that the information for verification is authenticated. When the information or documents are uploaded by the user, the platform must cross verify person version by using audio, video electronic means. For instance, if a platform provides high-risk adult content such as online betting apps for cricket available in India, e.g. My11circle, Dream11, etc. It is mandatory that if a user wants to make accounts in these such kind of platforms, then the platform must have mechanisms for verification of the user through personal audio or video calls by operators, require government-approved ID proof, and do cross-verification through government databases and facial verification that user is the same person and is not a minor.

Platforms must develop one-time data-reading mechanisms for age verification rather than storing data collected for age verification for a longer duration. If a person provides his or her crucial personal information for age verification, then after completion of the process, the data should be erased automatically. It helps in reducing the risk of data misuse by operators and

also protects users' personal information from hackers, which might be possible if data is stored for a long period.

Parents and adults in the family should avoid sharing their personal phones with their child, whether for educational purposes or otherwise; they must ensure that the child uses the device only for that purpose. Parents must monitor their child when they use phones, laptops or any other device so they do not misuse it.

The government can take steps for an awareness scheme to increase digital literacy among older-generation parents; it helps in reducing digital generational gaps between children and parents, which helps parents identify what type of platform is used by their children. The government can mandate that every educational institution run awareness campaigns led by technology experts, with a combined campaign for both students and their parents; this helps increase psychological transparency between children and parents and helps them talk comfortably.

Parents must teach their children about how misrepresentation of their age on online platforms can badly impact their lifestyle or how it is harmful to their social life and mental health. The government should spend more expenditure in research and development for better age verification mechanisms and also make legislation to regulate the production or uploading of unethical content such as pornography, sexual or nudity content available on the internet, which can be easily accessible to children.

Technical experts must do scientific research on AI tools to improve AI-based age estimation more accurately and precisely, and also integrate AI detection tools so that children can't use AI to misrepresent their age.

Technical experts must develop software to detect VPN usage and unusual software tools that can be used to change the geographical location of users to skip the verification methods. Platforms can attach preventive mechanisms with available tools to identify VPN usage during the user age verification process.

The government can take coercive measures to regulate unregulated platforms or third-party websites, such as banning them or removing them from the internet, so children cannot get access through these unregulated platforms.

CONCLUSION

Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025 are uniform and significant legislation for children's data protection on online platforms in India. DPDP Act, 2023 provides a dedicated provision that deals with obtaining verifiable parental consent before managing and processing children's personal data by data fiduciaries, imposes restrictions on data fiduciaries from using data that causes a detrimental effect on the well-being of a child, and provides protection from targeted advertisements to children. The DPDP Rules, 2025 provide a dedicated provision for an age verification mechanism using a virtual token mechanism and a Digital Locker Service Provider and other provisions for compliance of act, 2023. Age gating is one of the mechanisms of age identification, but it is a very basic and not effective method; age verification is much better in comparison to age gating it use documents-based verification and authenticates adults through OTP and KYC mechanisms. After all these available age identification mechanism this is not enough to protect children from age restricted content available on online platforms, there are several factors responsible for failure of protection such as fake age declaration by children, parents share their own devices and identify to children in family, using software tools like VPN to change geographical location, available unregulated platforms on internet which is easily accessible without any age verification of users, imperfect facial AI age estimations tools which can be easily fooled using others adult images, etc. If we look into foreign law to ensure children online safety then the European Union has of Digital Service Act and of General Data Protection Act, UK has Online Safety Act and USA has Children's Online Privacy Protection Act, these comparative overview of foreign legislation shows the each countries have some feasibility gaps in practical realities which may not resolve by only legal reforms, It is necessary to took a combined social legal and technical approach to avoid these problems such as strengthening our technology to detect VPNs, use government database to crosscheck user's identity, stronger regulatory oversight on unregulated platforms, combined awareness campaign in educational institutions for both parent and children to reduce digital generation gap, government should spend more on research and development in age verification mechanism only through this approach we can protect intent of DPDP Act and we can ensure the enforceability of true legislation in society and we can provide a safer digital environment to our children.