PROTECTION OF PERSONAL DATA OF CHILDREN IN INDIA: CHALLENGES, GLOBAL LESSONS, AND THE WAY FORWARD

Deepika Nandagudi Srinivasa[*]
Jupi Gogoi[**]

I. INTRODUCTION

Children are susceptible to several dangers that loom in the digital sphere. In addition to apparent risks like "sexual abuse, insomnia, obesity, low self-esteem, or addiction, minors are subject to other hidden threats, such as privacy invasions and data breaches."[1] This occurs primarily because children using the internet are treated as 'data-subjects'. Data subjects, in most global data protection regimes, are individuals whose information is shared, gathered, and processed, usually without their knowledge or any awareness of the potential repercussions.[2]

In a welcome move, the Indian position on privacy centred the proposed legal framework around the data subject and laid emphasis on a "free and fair digital economy".[3] Resultantly, the Indian data protection regime made a deliberate attempt at rewording the "data subject" terminology to "*Data Principal*". This change in terminology reflected the mindset shift that is required to acknowledge that all individuals, including children, become the focal actor in the digital economy.[4]

In view of the foregoing, the complexities with data collection, privacy violations and the vulnerabilities that children face in digital spaces will be discussed through the course of this paper. Building on the insights that are gathered from the literature survey, the researchers will explore the legal and regulatory regimes present in global jurisdictions such as the United Kingdom ('UK') and the European Union ('EU'). The exploratory exercise will continue in the penultimate section of the paper, where the researchers will highlight relevant provisions of India's Digital Personal Data Protection Act, 2023 ('DPDPA') and its impact on the processing of children's data.

Lastly, the intent behind this paper is two-pronged. First, to provide academic insights into a child rights-based understanding of data protection and data autonomy. Second, to identify the gaps in the current legal regimes protecting children's data and to unfurl alternate routes to safeguard this vulnerable segment of Data Principals.

---

[*] Policy and Privacy Associate at the Data Security Council of India.
[**]Assistant Professor, Faculty of Law, University of Delhi, Delhi, India.

[1] Cansu Caglar, "Children's Right to Privacy and Data Protection" 12(2) *EJLT* (2021), *available at*: https://www.ejlt.org/index.php/ejlt/article/view/828/1025 (last visited on May 27, 2022).
[2] *Ibid.*
[3] "A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians": Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *available at:* https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (last visited on May 27, 2022).
[4] *Ibid.*

II. UNDERSTANDING DATA COLLECTION AND ALLIED CONCERNS VIS-À-VIS CHILDREN

Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation (2016) state that three general categories can be used to classify personal data with high social, economic, and political value.[5] The first category is "data given". This refers to the "information that has been voluntarily submitted by people, such as survey responses (for example when users fill in their name, age or address on forms or surveys)." The second classification is "data observed" which refers to the "information that is typically unintentionally captured on utilising tracking tools or sensors such as cookies, facial recognition, and location tracking application."[6] The last classification is known as "data derived or inferred". This category of data is "generated from the examination of observed data. It might be connected to different sets of data. Usually, sophisticated algorithms and profiling procedures produce the result."[7]

In light of the above, literature also reveals that the third classification is especially troubling. This is due to the "fact that choosing not to have a certain type of data collected does not stop businesses from utilising data aggregation and data linkage techniques, as mentioned above, to attempt and fill in the gaps."[8] Another concern *vis-a-vis* inferred data, as pointed out by van der Hof (2018), is the "fact that inferred data is frequently unavailable to data subjects since it is based on correlations."[9] Given the sheer volume of data sets being examined and the intricacy of the procedure, it is practically impossible to predict the potential conclusion. Hence, this category of data has a high possibility of being erroneous.

According to Calgar, "the majority of individuals are still ignorant of how much data is currently being gathered, processed, and analysed."[10] Since "dealing with banks, potential employers, and authorities appears far away and irrelevant to children, their sense of privacy is less focused on personal information than that of adults."[11] It might be "challenging for people, and especially children, to comprehend the dangers that come with data collection and profiling. As a consequence, they are less concerned about hazards linked to data mining, profiling, or identity theft."[12]

Van der Hof, have also pointed out that "profiling and automated decision-making can be used to blacklist children or to provide or deny them access to certain goods and services and thereby, have long-lasting, detrimental impacts on children."[13] As a "result of this particular set of

---

[5] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)
[6] *Ibid.*
[7] *Supra* note 1.
[8] Yilun Wang and Michal Kosinski, "Deep Neural Networks are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images" 114(2) *Innovations in Social Psychology* 246 (2018).
[9] Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* 6-7 (Wolters Kluwer, 2018).
[10] *Supra* note 1.
[11] W.M.P. Steijn, A.P. Schouten, *et.al.*, "Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook" 10(1) *Cyberpsychology-Journal of Psychosocial Research on Cyberspace* (2016).
[12] Eva Lievens and Valerie Verdoodt, "Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation" 34(2) *Computer Law and Security Review* 269 (2018).
[13] Simone van der Hof, Eva Lievens, *et.al.*, "The Child's Right to Protection Against Economic Exploitation in the Digital World" 28(4) *The International Journal of Children's Rights* 833, 835 (2020).

circumstances, children may experience unfair and discriminating outcomes."[14] In addition, children's data is increasingly being "monetised, dataveillanced, dataficated, misused, or hacked, raising serious privacy concerns in public policy circles."[15] Therefore, the primary concern remains how the collected personal data, especially of minors, is being used.

III DIMENSIONS OF PRIVACY IN THE CONTEXT OF CHILDREN

From a statutory perspective, the United Nations Convention of the Rights of the Child (UNCRC),[16] the Universal Declaration of Human Rights,[17] the European Convention on Human Rights,[18] the International Covenant on Civil and Political Rights,[19] and other national laws and constitutions recognise privacy as a fundamental human right. In India, "the right to privacy is not expressly protected by the Indian Constitution. However, a number of rulings by the Supreme Court of India (SC) over the years have construed other rights in the Constitution to be giving rise to a limited right to privacy, most notably through Article 21."[20] Notably, the SC in its landmark judgement in *K.S. Puttaswamy v. Union of India*,[21] laid stress on the importance of protecting children's right to privacy, especially in light of the fact that minors are not legally able to consent.[22]

Researchers have discovered three distinct ways that young people comprehend the value of privacy.[23] These are contextual, relational, and dialectical. Contextual understandings address how privacy is governed by specific norms and values, which are frequently challenged by the conflicts about the dynamic nature of these norms. Relational understandings link establishing relationships, which are built on transparency, reciprocity, and trust, while maintaining privacy.[24] Lastly, a dialectical concept of privacy points to the overlap between the public and private domains that have collapsed online.[25]

In light of the above, the notion of agreeing to online privacy terms and conditions by a child does not entail reciprocity; instead, it creates a one-way connection that permits monitoring of the child, who has little choice but to comply or forego the advantage.[26] Moreover, Steeves and Reagan point out that "young people can desire both privacy and publicity online, which requires

---

[14] *Supra* note 9.
[15] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, "Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review" *London School of Economics and Political Science* 16 (2019).
[16] Convention on the Rights of the Child (adopted Nov. 20, 1989, entered into force Sep. 02, 1990) E/CN.4/RES/1990/74, art. 16.
[17] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR), art. 12.
[18] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), art. 8.
[19] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art. 17.
[20] *Justice K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1; *Maneka Gandhi* v. *Union of India*, AIR 1978 SC 597.
[21] (2019) 1 SCC 1.
[22] *Ibid*.
[23] Valerie Steeves and Priscilla Regan, "Young People Online and the Social Value of Privacy" 12(4) *Journal of Information Communication and Ethics in Society* 298-313 (2014).
[24] *Ibid*.
[25] *Ibid*.
[26] *Supra* note 23.

ongoing negotiation of privacy and consent that cannot be irrevocably handed up."[27] Likewise, "physical, communicational, informational, and decisional privacy are among the privacy dimensions influenced by digital technology", according to research on children's online privacy and freedom of expression undertaken by the United Nations International Children's Emergency Fund ('UNICEF').[28]

When tracking, monitoring, or live streaming technology is used to reveal a child's picture, activities, or whereabouts, a child's physical privacy is invaded.[29] The act of collecting, storing, and processing of children's personal data may violate their informational privacy, particularly if done without their knowledge or consent.[30] This dimension of privacy is especially important for this particular academic inquiry. Lastly, access to relevant information is restricted, which might hinder the child's ability to make independent decisions or develop to their full potential, resulting in a violation of the child's decisional privacy.[31]

Livingstone *et.al.* (2019) have also highlighted the typology of privacy. They classify privacy under three broad groups, namely, "interpersonal privacy, institutional privacy and commercial privacy."[32] Out of them, the last category of privacy, according to Livingstone (2019), is related to 'commercial privacy' is the biggest concern. The invasion of commercial privacy is said to pose a greater threat, as compared to institutional privacy, as commercial corporations are accumulating more data on minors than even governments do or can collect.[33] It is also to be noted that the mechanisms for processing children's data are developing and increasing quickly. As a consequence, marketers use a variety of, frequently intrusive, techniques to turn child-friendly activities into a commodity.[34]

Moreover, privacy settings of the child's friends, the frequency with which one uses social media, one's gender, the kinds of contacts on the child's social media profiles, the desire to control personal information, previously unpleasant experiences sharing personal information, or parental intervention are all factors that can influence privacy decisions.[35] However, the compromises in security and privacy that children are making may go unnoticed by parents, who may also be ignorant of all the potential effects of data processing, data linkage, and data aggregation that could damage their children's rights and freedoms.[36]

IV. VULNERABILITIES *VIS-A-VIS* CHILDREN IN DIGITAL SPACES

Calgar points out that "risks of privacy invasions and data protection violations significantly increase as more children use the internet and divulge information at an increasing

[27] *Ibid.*
[28] Children's online privacy and freedom of expression: Industry toolkit, UNICEF (2018).
[29] *Ibid*.
[30] *Supra* note 15.
[31] *Supra* note 28.
[32] *Supra* note 23.
[33] *Supra* note 28.
[34] Kathryn C Montgomery and others, "Children's Privacy in the Big Data Era: Research Opportunities" 140 *Pediatrics* (2017).
[35] Gustavo Mesch, "Cultural Values and Facebook Use among Palestinian Youth in Israel" *Computers in Human Behavior* (2015).
[36] *Supra* note 1.

rate."[37] From an Indian context, "risks of privacy invasions and data protection violations also significantly increase as the number of internet users who are minors is growing each day."[38] Likewise, a study conducted by Macenaite and Kosta revealed "children share a significant amount of personal data while utilising new technology, even while they enjoy learning, self-expression, socialising, playing, and creating with these tools."[39]

From a child's perspective, the issue of 'consent' is quite critical. Using consent as a sole or dominant control mechanism for children's interactions with the digital environment presents a difficulty because of children's low resistance to the advertisement technology industry's sophisticated persuasive methods.[40] UNICEF has also emphasised that children deserve special protection because of their particular characteristics, thus, they have specialised rights that only apply to them, even though human rights are universal and apply to both adults and children equally.[41] These particular characteristics could mean that minors simultaneously need special protection because they are biologically dependent on the care rendered by parents or guardians. Furthermore, since they lack cognitive capacity at this stage of life, they are unable to make informed judgments for themselves.[42]

The age of Big Data further exacerbates the situation, as children are at danger from these privacy-invading digital risks with the growing commercialisation of information society services.[43] With the use of artificial intelligence and machine learning, information that has gone unrecorded over a long period of time is increasingly being recorded, analysed, and linked using Big Data and algorithms.[44] Through this complex web of algorithms, children today are profiled and offered personalised marketing communications and content *via* self-learning mechanisms supplied by their own personal data.[45] Data is, hence, monetised and given a financial value in this way.

In addition, children are becoming more financially independent, having the power to direct how their parents spend their money, and will eventually become consumers.[46] In light of this, personal data from children is especially valued by commercial enterprises as businesses can offer clients more specialised goods and services, the more information they have about their

---

[37] *Supra* note 1.

[38] As per reports, children in school, who are 15 years old or younger, account for 38% of all Internet users in India. Kantar and IAMAI, 'ICUBE 2020' (Internet Adoption in India 2020), *available at*: https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf (last visited on June 01, 2022).

[39] Milda Macenaite and Eleni Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" 26(2) *Information and Communications Technology Law* 146 (2017).

[40] Lisa Archbold, Damian Clifford, *et.al.*, "Adtech and Children's Data Rights" 44 *UNSW Law Journal* 857 (2021).

[41] UNICEF, "The Rights of Every Child" *available at*: https://www.unicef.org.uk/child-rights-partners/wpcontent/uploads/sites/3/2016/08/CRC_summary_leaflet_Child_Rights_Partners_web_final.pdf (last visited on May 24, 2022).

[42] Beauvais MJS and Knoppers BM, "Coming Out to Play: Privacy, Data Protection, Children's Health, and COVID-19 Research" 12 *Front Genet* (2021).

[43] *Supra* note 1.

[44] Mariya Stoilva, Rishita Nandagiri and Sonia Livingstone, "Children's Understanding of Personal Data and Privacy Online – A systematic Evidence Mapping" *Information, Communication & Society* (2019).

[45] *Supra* note 13.

[46] Simone van der Hof, "I Agree or Do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World" 34(2) *Wisconsin International Law Journal* 101,107 (2017).

customers. Prior to the digital revolution, it was difficult to employ traditional media to target children with personalised marketing, and children were unlikely to accidentally reveal sensitive information when left unsupervised by adults.[47] Hence, children are specifically targeted as they tend to share an alarming amount of personal data.

V. GLOBAL PERSPECTIVES ON CHILDREN'S PRIVACY

Child data subjects raise unique challenges for which there are few standards, whether the questions include affording adequate respect to the child's data retention, child and parental autonomy, or minors' best interests. In fact, evaluating the wide range of rights protected by the General Data Protection Regulation ('GDPR') regimes necessitates a balancing exercise in any situation. Hence, the UK and EU's existing normative systems for protecting children's data, as overseen by the Information Commissioner's Office ('ICO') and European Data Protection Supervisor ('EDPS') respectively, are surveyed in this section of the paper. It is concerned with determining whether India has chosen the optimal course of action *vis-a-vis* minors, or if there are other legal frameworks for the protection of children's data that provide measures that are, in theory, more advantageous.

A. European Union

European law governing the rights of children is primarily based on the UNCRC. The UNCRC has become the cornerstone of children's rights and has played a significant role in the development of European law on children's rights.[48] Taking a leaf from the provisions of the UNCRC, the European Council requires that all choices impacting a child's health and development are made on giving due regard to the child's best interests.[49] On the same lines, children's right to protection and care is acknowledged in article 24 of the Charter of Fundamental Rights of the European Union ('CFREU'), which also states that public and private authorities must consider the child's best interests in all decisions involving them.[50]

To address concerns about the processing of children's data, the European Union also adopted a specific provision in the GDPR on May 25, 2018.[51] The GDPR defines "the rights, data processing responsibilities, and appropriate tools to be applied to personal data processing."[52] Although the GDPR now provides effective safeguards for children's privacy and data protection, it still needs to be improved to increase transparency and give children more control over their

[47] Ingrid Lambrecht, Valerie Verdoodt and Jasper Bellon, "Platforms and Commercial Communications Aimed at Children: A Playground Under Legislative Reform?" 32(1) *International Review of Law, Computers & Technology* 58,59 (2018).
[48] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Law Relating to the Rights of the Child (June 2015) 26 *available at:* https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf (last visited on May 16, 2022).
[49] *Vavřička* v. *The Czech Republic*, App no 47621/13 (ECHR, Apr. 08, 2021).
[50] Ingrida Milkaite and Eva Lievens "The Internet of Toys: Playing Games with Children's Data?" in Giovanna Mascheroni and Donell Holloway (eds.), *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play* 287-288 (Springer 2019).
[51] Regulation (EU) 2016/679 of the European Parliament and 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, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5. 2016.
[52] *Supra* note 1.

personal information. This presents an opportunity to reevaluate the current principles and how they are being implemented.[53]A minor can provide their consent for the processing of their personal data to commercial online services starting at the age of 16, according to Article 8 of the GDPR, which governs the age of digital consent.[54] Under 16 years old, parental permission is necessary.

In September 2019, the EDPS, in its attempt to prescribe measures to operationalise the GDPR, released checklists and flowcharts on data protection.[55] When deliberating on transparency, the EDPS made a reference to children as the targeted audience to be the recipients of information on processing activities undertaken by Data Controllers. In such cases, the EDPS guidance highlighted that children would require "tailored information" to ensure that Data Controllers follow the transparency principle in letter and spirit.

B. United Kingdom

The UK ICO plays an active role in providing child-specific guidance vis-a-vis processing activities. For instance, the ICO has a dedicated section on its website to guide organisations processing children's personal data.[56] Similar to the EU's stance on children's data, the UK ICO places importance on the transparency and accountability principles when processing children's data. As a result, the ICO recommends using 'plain clear language' when addressing children, in a manner that can be easily comprehensible.[57]

The recommended approach for children's data processing is underscored by the "data protection by design and default" and "child-friendly" principles.[58] Organisations coming within the ambit of the UK GDPR are thereby mandated to integrate the principles into their processing activities, from the design stage right through the lifecycle. The ICO, in this regard, envisions the integration being achieved by placing appropriate technical and organisational measures.

The UK ICO also goes a step further to balance the protection considerations with the child's freedom to learn, develop and explore.[59] If a given organisation's processing activities pose a high risk to the freedoms or protection considerations of a child, the ICO recommends conducting a Data Protection Impact Assessment ('DPIA'). In instances where organisations are unsure whether the data subject is a child, the ICO recommends a cautious and risk-based approach. To illustrate this suggestion, examples such as up-front implementation to verify the age of the data

---

[53] *Ibid*.
[54] *Supra* note 51, art 8.
[55] European Data Protection Supervisor, "Checklists and flowcharts on data protection" (Sep. 2019), *available at*: https://www.edps.europa.eu/data-protection/our-work/publications/factsheets/checklists-and-flowcharts-data-protection_en (last visited on May 16, 2022).
[56]Information Commissioner's Office, "Children and the UK GDPR", *available at:* https://ico.org.uk/for-organisations/ uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/ (last visited on June 16, 2025).
[57] *Ibid*.
[58]Information Commissioner's Office, "What should our general approach to processing children's personal data be?" *available at:* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/ (last visited on June 16, 2025).
[59] *Ibid*.

subject or designing processing activities in a manner that provides sufficient protection for children have been highlighted.

The interesting aspect of the UK GDPR emerges with the age of consent to data processing activities. It is to be noted that England, Wales and Northern Ireland have no set age of consent for a child to be deemed competent to provide their own consent to data processing. In Scotland, on the other hand, the age is defined as 12 or over.[60]

Aligning with India's DPDPA, which will be discussed in the next section, the UK ICO's approach to consenting to processing children's data is rooted in parental consent in some instances. An important implementation challenge identified by the ICO is how Data Controllers would inform child data subjects that they have the right to withdraw consent once they reach the age of being competent to consent to processing activities. This leaves some food for thought from the Indian perspective as well.

The UK guidance stands out as an excellent example of accounting for a child's evolving capabilities in a digital context. In particular, the UK's emphasis on presenting privacy notices in a child-appropriate manner is a unique regulatory approach. Quoting the ICO guidance, organisations must "consider using diagrams, cartoons, graphics and videos that will attract and interest them".[61]

VI. Data Protection Mechanisms for Minors: An Indian Perspective

A. Legal Framework Prior to the DPDPA

Before the DPDPA, there were no legal measures in place to specifically safeguard children from data breaches and dangers online. However, the framework for data protection in India was then determined by the Information Technology Act, 2000, ('IT Act') and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('SPDI Rules'). Data protection under the IT Act, 2000, primarily involved section 43A, which "mandated reasonable security practices for handling sensitive personal data (SPDI) and holds bodies corporate liable for compensation in cases of negligence and data breaches." Further, section 72A of the IT Act stated that "a person is subject to punishment if they divulge information, they have access to due to a legal contract. This could be done without the person's permission or if they do so in violation of the terms of the contract." The SDPI rules under rule 3 provided definition of 'Sensitive Personal information'.[62] According

[60] Information Commissioner's Office, "What do we need to consider when choosing a basis for processing children's personal data?", *available at*: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children -and-the-uk-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/> (last visited on June 16, 2025).

[61] Information Commissioner's Office, "How does the right to be informed apply to children?" *available at*: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/how-does-the-right-to-be-informed-apply-to-children/> (last visited on June 16, 2025).

[62] SDP included (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; Shweta Mohandas and Deepika Nandagudi

to Rule 4, "corporations must make their privacy policies available to individuals who have submitted their information as part of a lawful contract." According to rules 5 and 7, "a person's consent, based on the principles of legality and necessity, is necessary to collect and/or disclose personal information or SPDI."

B. The Digital Personal Data Protection Act, 2023

The DPDPA is the first legislation in India that specifically discusses data protection of processing activities related to children. First, the Act defines a child as "an individual who has not completed the age of eighteen years".[63] The concept of "data principal" is also introduced by the Act to mean "the individual to whom the personal data relates". In instances where the Data Principal is a child, the definition includes the parents or lawful guardian of such a child.[64] Thus, this provision brings children's personal data also within the purview of the Act.

Section 9 of the Act deals with the data processing of children's personal data. These provisions impose specific obligations on the "Data Fiduciary" when they process children's data. Data Fiduciary is defined as, "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."[65]

Similar to the UK GDPR, when the legal basis for processing a child's data is via consent, the Data Fiduciary is obligated to obtain verifiable consent of the parent of such child.[66] The same has been reiterated by the proposed operational framework of the DPDPA under its Draft Rules. However, the Rules go a step further to place an additional obligation on Data Fiduciaries to take appropriate technical and organisational measures to ensure parental consent is obtained before commencing processing activities.[67]

A novel legal requirement introduced by the Indian framework also includes laying emphasis on obtaining "*verifiable*" parental consent. Thereby, Data Fiduciaries must "observe due diligence" to validate that the individual identifying as a parent is an adult by verifying their own reliable details or through government-verified systems.[68]Also, special obligations are placed on the Data Fiduciary so that they cannot process personal data that is likely to cause any detrimental effect on the well-being of a child; shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.[69]

Srinivasa, "The Boss Will See You Now - The Growth of Workplace Surveillance in India, is Data Protection Legislation the Answer?" (Centre for Internet and Society, 31 December 2020) < https://cis-india.org/internet-governance/blog/the-boss-will-see-you-now-the-growth-of-workplace-surveillance-in-india-is-data-protection-legislation-the-answer > (last visited on June 9, 2022).

[63] Digital Personal Data Protection Act, 2023, s. 2(f),

[64] *Id..,* s. 2(j).

[65] *Id.,* s. 2(i).

[66] *Id.,* s. 9(1).

[67] Draft DPDP Rules, 2025, rule 10(1).

[68] If an individual voluntarily provided details of identity and age or a virtual token mapped to the same which is issued by an entity entrusted by law or the Central Government or a State Government or a digital locker service provider

[69] *Supra* note 63, ss. 9(2) and 9(3).

Further, there are certain exceptions provided in cases of processing of personal data of children without consent and relating to tracking or behavioural monitoring of children.[70] These exceptions are applicable to certain kinds of organisations.[71] These organisations can use personal data under this provision for only certain limited purposes. Processing is restricted to the extent necessary for such exercise, performance or discharge.[72] The Central Government is empowered to issue these Draft Rules by the parent DPDP Act under section 40(2)(j).[73]

In light of the aforementioned legal provisions, three major dilemmas arise when brought into the context of children. First, since there is no overarching concept of consent[74] under Indian law, it becomes important to determine whether consent is independent of the capacity to enter into legally binding contracts.[75] Second, the DPDPA framework also implies that a minor cannot exercise the rights as Data Principals without the consent of their legal guardian, who must execute the same on their behalf. Lastly, these legal provisions are also critiqued for being insufficient for protecting children as they do not flesh out pertinent concepts such as verifiable parental permission" or "differentiated policies for various age groups.[76]

VII. CONCLUSION AND SUGGESTIONS

Through the course of this academic inquiry, the researchers have found that the use of children's data for commercial purposes is at the centre of the current minors' data protection debate.

The architecture of the digital world's supporting regulatory bodies and commercial organisations does not sufficiently recognise or protect the unique requirements and rights of children.[77] As a result, children's privacy rights are often an afterthought. Owing to this, there is a greater fiduciary responsibility of care for children's data. This also necessitates a tailored approach that takes into account children's individual differences and varied developmental stages. In light of the foregoing, the researchers' recommendations fall under two primary thematic areas: Recommendations on the Legal Framework and Recommendations for Organisations Processing Children's Data.

---

[70] *Id.,* s. 9(4).

[71] Such as clinical establishment, mental health establishment or healthcare professional, educational institutions, creche or day care, gtransport facilitator to educational institutionas, creche or daycare

[72] Under the Draft DPDP Rules 2025, the reasons are in the interests of a child, under any law for the time being in force in India, for providing or the providing or issuing of any subsidy, benefit, service, certificate, licence or permit, by whatever name called, under law or policy or using public funds, in the interests of a child. Also, for creation of a user account for communicating by email; for ensuring that information likely to cause any detrimental effect on the well-being of a child is not accessible to her; for confirmation by the Data Fiduciary that the Data Principal is not a child and observance of due diligence.

[73] The Central Government is given rule-making power regarding those data fiduciaries who come within the exceptions under sub-section (4) of section 9.

[74] Here, the discourse on consent entails concepts such as parental consent and the age-gating thresholds to ascertain the capacity to provide consent to data processing activities.

[75] Trishee Goyal, "Working Paper on Safeguarding Children's Informational Privacy in India: An Assessment of the Framework under the PDP Bill, 2019" *Centre of Applied Law & Technology Research* (ALTR), Vidhi Centre for Legal Policy (2022).

[76] Amar Patnaik, "A black mirror for policy makers: Looking at data protection for minors" *Economic Times*, Mar. 04, 2021.

[77] Sonia Livingstone and Ellen Helsper, "Balancing Opportunities and Risks in Teenagers' Use of the Internet: The Role of Online Skills and Internet Self-Efficacy" 12(2) *New Media & Society* (2010).

A. Recommendations on the Legal Framework

The DPDPA empowers the Central Government to notify Data Fiduciaries as a "Significant Data Fiduciary" ('SDF') based on an assessment of factors such as volume and sensitivity of data processed, as well as national security considerations.[78] A key implication for being notified as an SDF includes appointing a Data Protection Officer ('DPO') and undertaking periodic data audits and DPIAs.[79] However, making an explicit call out under the DPDPA to classify those Data Fiduciaries who process children's data as SDFs is recommended.

This proactive measure would enable regulatory scrutiny and impose additional safeguards on Data Fiduciaries who undertake processing activities of vulnerable Data Principals. Therefore, having dedicated teams under the DPO and undertaking DPIAs and data audits would align with global practices as well as transparency and accountability principles.

Particularly when processing is likely to result in a high danger to the rights and freedoms of natural people", DPIAs are used to analyse the extent and effects of that processing.[80] DPIAs, when executed effectively, may be helpful in obtaining the child's informed consent for data processing. It may even be useful in informing the child and their legal guardians about the advantages and disadvantages of data processing as well as how the Data Fiduciary protects the security of their data.[81]

In global regimes such as the UK, it has been proposed that Data Controllers (Data Fiduciary equivalent under GDPR) ought to engage in continual, transparent communication with child data subjects in order to uphold the autonomy of children in digital spaces.[82] In line with this, DPIAs give controllers the chance to closely analyse the risks associated with data processing throughout its lifecycle and then put safety measures in place to lessen or eliminate those risks. Since DPIAs are well-suited for interacting with minors to help them understand the hazards that some scientific data processing tasks may pose to their interests, it has also been recommended to modify DPIAs according to a child's comprehension level.[83] Hence, to increase transparency, accountability, and confidence, the DPIAs should be made available to parents and child participants.[84] Ultimately, such practices would build a mutually trusting relationship.

---

[78] *Supra* note 63, s 10(1).
[79] *Ibid.*
[80] Van der Hof, S., and Lievens, E., "The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR" 23 *Communications Law - Journal of Computer, Media and Telecommunications Law* 33–43 (2018).
[81] Rahimzadeh andV., Schickhardt, *et al.*. "Key implications of data sharing in pediatric genomics" *JAMA Pediatrics* 476–481 (2018).
[82] M.J. Taylor, M. J., Dove, *et.al.*, "When can the child speak for herself? The limits of parental consent in data protection law for health research" *Medical Law Review* 26 (2017).
[83] Art. 29 Data Protection Working Party (2017). Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679. Article 29 Data Protection Working Party, *available at*: http://ec.europa.eu/newsroom/ document.cfm?doc_id=47711 (last visited on June 6, 2022); Lievens, E., and Verdoodt, V., "Looking for needles in a haystack: key issues affecting children's rights in the general data protection regulation" 34 *Comput. Law Secur. Rev*., 269–278 2018).
[84] *Supra* note 42.

Another key perspective is concerning the child's autonomy over their data and holistic development through decision-making. If the Indian data protection regime were to develop a child-appropriate DPIA to seek informed consent, we see an opportunity to revisit the age of consent to data processing activities. With such safeguards in place, the current age of consent vis-a-vis data sharing, as specified by the DPDPA, can potentially be reduced from 18 to the global standard, i.e., anywhere between 13 to 16.[85] Moreover, slating 18 as the age of consent would prove to be impractical and disadvantageous on many accounts. Firstly, setting a consent age that is out of line with reality would encourage minors to lie about their ages, commonly with their parents' approval. In such situations of circumventing the law, the protection of children's personal data is lessened. Secondly, it makes it challenging for internet service providers to give children the age-appropriate guidance they need for a safe browsing experience. Moreover, minors who are at greater risk, such as youth belonging to the LGBTQIA+ community, children with disabilities, and those living in abusive environments, will have fewer opportunities to obtain relevant information online.

B. Recommendations for Organisations Processing Children's Data

The DPDPA and its proposed operational framework to regulate processing activities are a promising first step in the right direction to safeguard children's experiences in digital spaces. It is hoped that organisations would view these measures as an opportunity to conduct intentional and proactive operational changes, rather than viewing this as a compliance burden.

With this mindset shift in place, we recommend organisations budget for privacy-related activities. This is especially considering the DPDP framework mandates implementing measures that cause impact on (i) an organisational level; and (ii) a technical level.[86] From an organisational standpoint, we anticipate changes such as appointing a DPO and a dedicated team for overseeing consent management activities. In the particular case of processing activities for children, the appointment of DPOs who are excellent communicators is essential. This is considering the DPO and/or the Grievance Officer, as the case may be, becomes the single point of contact for all the queries a Data Principal may have. In the event such queries are posed by Data Principals who are minors, the DPO must have the ability to explain the details of processing activities in plain and simple terms to the child.

The second privacy budget consideration is that of the implementation of technical measures to operationalise the DPDP framework concerning children. This includes onboarding external entities that offer age verification services, as well as validating the parent's identity to establish verifiable parental consent. In the event a Data Fiduciary wants to manage age and parent verification internally, the privacy budget must account for hiring technical personnel to build the digital workflows for the same, as well as invest in Privacy-Enhancing and Privacy-Enabling Technologies such as Zero Knowledge Proofs or Age Tokens.[87]

[85] Refer to the UK GDPR. As well as the US Children's Online Privacy Protection Rule (COPPA) and Singapore Personal Data Protection Act (PDPA).
[86] *Supra* note 67.
[87] *Supra* note 62.

Lastly, to remedy the vulnerabilities children face in the digital world, the 'Good Governance of Children's Data Project' by UNICEF suggests that digital providers ought to integrate a 'children's rights by design' standard in the goods and services targeted towards minors.[88] All in all, the protection of children's privacy rights and the promotion of their well-being depend heavily on the responsible use of their data.

[88] Kathryn C Montgomery and Jeff Chester, "Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework" 1(4) *European Data Protection Law Review* (2015).