UDC 342.738-053.2/.6:004.738.5]:341.24
342.738-053.2/.6:004.738.5(540)

DOI: https://doi.org/10.46763/BSSR242323235g

SECURING THE DIGITAL FOOTPRINTS OF MINORS: PRIVACY IMPLICATIONS OF AI

HitanshI GOEL

Ph.D. Researcher, School of Law, Bennett University, India
E-mail: hitanshi3006@gmail.com

Gyandeep CHAUDHARY

Assistant Professor, School of Law, Bennett University, India
E-mail: gyan.2889@gmail.com

Abstract

The unprecedented growth of 'Artificial Intelligence' (*hereinafter* referred to as AI) has brought immense benefits but at the same time has posed complex challenges that has impacted users' lives, including privacy and data security, particularly, children who are vulnerable to these problems. This paper examines privacy of children in the era of AI and the legal framework's adequacy in protecting children's privacy, focusing on India, the world's most populous nation in 2024,[1] with over 833.7 million[2] internet users, accounting for more than half of its population. With the advent of AI, unprecedented accumulation, processing, and analysis of massive datasets has become possible by algorithms applying predictive analytics on discrete datasets. Nevertheless, AI's pattern recognition ability has blurred privacy boundaries which has enabled it to feed on sensitive information such as that concerning health, emotions, interests, and behaviours. Due to innate curiosity and digital immersion, children are more susceptible to privacy violations in this 'AI-driven' digital era. Since children possess a limited understanding of privacy risks, they are more likely to share information online. Consequently, there is an urgent need to address the issue concerning the

[1] *Population by country (2024) - Worldometer*. (2023, July 16). Worldometer - real time world statistics. https://www.worldometers.info/world-population/population-by-country/.
[2] *Internet users by country 2024*. World Population by Country 2024 (Live). https://worldpopulationreview.com/country-rankings/internet-users-by-country.

increased digital footprint of children and the associated conflict between the 'age of consent' and the 'age of contractual capacity' for the purpose of fixing the 'digital age' of the child. Such a requirement can be potentially addressed through legislative intervention by enacting a comprehensive piece of legislation to regulate the ubiquitous collection of data. Facial recognition, predictive analytics, autonomous systems, and other AI applications, could be the reason for the apprehensions that systemic discrimination could occur and governance is also at stake that points out the need for transparency and accountability. While AI brings with itself exponential growth, there is also a need to underscore the importance of protecting children's right to privacy, given their vulnerability. A comprehensive legislative framework, responsible corporate policies, and increased awareness can help strike a balance, allowing children to harness AI's benefits while safeguarding their fundamental rights.

Keywords: *Artificial Intelligence, Vulnerable groups, Data protection, Digital age, Data privacy.*

1. Introduction

In the early days of the Internet's development, Internet governance primarily focused on the technical aspects of connectivity, regardless of the impact of information flow on users and society. Over time, governance shifted towards regulating content dissemination, including determining what is suitable for different groups, especially vulnerable populations like children. However, children's rights were acknowledged late in Internet governance conversations. The 2003 World Summit on the Information Society (WSIS) first acknowledged children's rights. (*Declaration of principles building the information society: A global challenge in the new millennium*, 2003) However, the 2005 Tunis Agenda and subsequent creation of the Internet Governance Forum (IGF) resulted in losing the empowering vision for children online. (World Summit on the Information Society, 2005) This occurred because children's rights were not integrated into Internet governance frameworks and mechanisms early on.

Discussions on children's rights in Internet governance tend to overly focus on issues like child abuse material and sexual exploitation. While critical, this narrow view depicts children solely as victims, disregarding their autonomy and rights to access information, privacy, and participation. Consequently, overly restrictive policies are often proposed, compromising children's online freedoms. The Internet has immense potential to empower and benefit children. As former UN Special Rapporteur La Rue stated, "It can enable children to

exercise rights to expression, education, association, and full social, cultural and political participation - essential for an open, democratic society." (Rue, 2011, p. 4)

In recent years, several UN agencies and affiliated organizations have emphasized the significance of the Internet concerning children's rights. For instance, the United Nations Convention on the Rights of the Child (UNCRC) held a special discussion day in September 2014 to explore the link between children's rights and digital media. (Committee on the Rights of the Child, 2014) The aim was to develop plans prioritizing children's rights, enhancing their online experience, and safeguarding them from potential harm without compromising benefits. As a signatory to the UNCRC, India is obligated to integrate its legal principles into domestic regulatory frameworks governing children's digital rights and privacy. (Committee on the Rights of the Child, 2014) This highlights the urgent need to formulate appropriate laws and policies safeguarding children's rights in the online sphere.

The UNCRC defines a child under Article 1 (*Convention on the rights of the child*, 1989) as any individual under 18 years old, except when an earlier majority is reached under applicable law. This aligns with the age limit of 18 years to define a child which was recommended in the B.N. Srikrishna Committee Report on Privacy and Data Protection. (*Joint committee on the personal data protection bill, 2019*, 2021) This was subsequently adopted in the Personal Data Protection Bill (PDPB) 2019 draft. Although the Joint Committee on PDPB discussed the umbrella age, the latest 2022 Digital Personal Data Protection Bill retains the under 18-year limit. This demonstrates the legislature's commitment to maintain alignment with the UNCRC's child definition. However, other domestic legislation employs a graded approach in defining a child, with different age thresholds across laws. This fragmented regulatory landscape regarding children's privacy necessitates consolidation for coherence. The U.K. was first out of the blocks in addressing this challenge with the statutory Age-Appropriate Design Code. The U.K.'s breakthrough was followed by California adopting the California Age-Appropriate Design Code Act in 2022. Today, other countries are taking inspiration from the UK's model and engaging in the global conversation about how to best protect children's digital privacy, so perhaps India's legal experts can also gain from UK's first-hand experience in developing and implementing the code and come up with a uniform age-based definition aligned with global standards that would strengthen the protection framework governing children's rights in India's digital ecosystem.

2. Literature Review

The rapid advancement of digital technologies, particularly AI, has opened up new opportunities and risks for children in the digital environment. Recognizing this, various international organizations have taken proactive measures to address the potential impact of AI on children's rights and well-being (Charisi et al., 2022).

The United Nations (UN) adopted the Comment 25 (*General comment No. 25 (2021) on children's rights in relation to the digital environment*, 2021) on the rights of the child in the digital environment, which considers children's interactions with various digital technologies, including AI, and calls on governments to mitigate risks and ensure equal access to the benefits. Organizations like UNICEF (*The state of the world's children 2017: Children in a digital world*, 2017), the OECD (*Recommendation of the council on children in the digital environment*, 2021), and UNESCO (Pedró et al., 2019) have also developed guidelines and recommendations to promote child-centered AI development, aiming to strike a balance between protection and opportunities, and foster responsible stewardship of trustworthy AI. UNESCO adopted the UN General Comment 25 on Children's Rights in Relation to the Digital Environment. Similar to OECD, UNESCO categorized AI-based applications for education into two broad categories that contribute to improved learning and equity for all children; firstly, AI for personalization and better learning outcomes, and secondly, Data analytics in Education Management Information Systems (EMIS) and the evolution to Learning Management Systems (LMS). (Pedró et al., 2019).

Within the European Union (EU), the Charter of Fundamental Rights guarantees the protection of children's rights, while the EU Agency for Fundamental Rights has emphasized the need to mainstream children's rights in AI policies (*Charter of fundamental rights of the European Union*, 2000, Art. 24, p. 13). The General Data Protection Regulation (GDPR) contains provisions aimed at securing the processing of children's personal data and ensuring their understanding and exercise of data protection rights (General Data Protection Regulation, 2016).

To develop trustworthy AI for children, the European Commission has identified five primary requirements: strategic and systemic choices, child-friendly and non-discriminatory technology, facilitation of data control, integration of children's agency, and consideration of the full range of children's rights (Charisi et al., 2022, p. 3). Furthermore, recent initiatives like Stanford University's Human-Centered Artificial Intelligence have highlighted the importance of data governance measures to address privacy risks associated with unrestrained data collection (King & Meinhar, 2024).

Despite these efforts, the current scientific evidence about the impact of AI-based applications on children's development, and the opportunities and risks they bring, remains limited. Moreover, how the rights of the child, as defined in the UN Convention on the Rights of the Child and the General Comment 25, can be realized in the AI context is even less explored. To bridge this gap, a robust data collection process was undertaken to create a comprehensive corpus of AI policies, reports, guidelines, and ethical principles. This corpus encompasses documents prepared by organizations explicitly focused on safeguarding children's rights in an algorithmic-oriented society, expanding measures for preparing children to live in an AI world, and developing AI

literacy skills, as well as organizations actively addressing the privacy risks posed by digital technologies, especially AI.

The methodology involved leveraging an existing database of AI initiatives to analyze this diverse collection of documents from a diversity perspective. By examining this rich corpus, the study aims to provide insights into the potential impact of AI on children and how their rights can be realized in the AI context, given their heightened vulnerabilities and the numerous roles AI will play throughout the lifespan of individuals born in the 21st century. Through this comprehensive review and analysis, the study seeks to contribute to the growing body of knowledge on the intersection of AI and children's rights, informing the development of policies and practices that prioritize the best interests of children in an increasingly digital world.

3. Definition of "child" under various legislations

3.1 Domestic Legislations

The researcher has analyzed the terms "child" and "minor" jointly under different legislations as follows:

Serial No.	Legislation	Provision	Age of child
1	The Child Labour (Protection and Regulation) Act, 1986.	Section 2(ii)	14
2	The Plantations Labour Act, 1951.	Section 2(c)	15
3	The Motor Transport Workers Act, 1961.	Section 21	15
4	The Beedi ad Cigar Workers (Conditions of Employment) Act, 1966.	Section 2(b)	14
5	Prohibition of Child Marriage Act, 2006.	Section 2(a)	Male -21 Female - 18
6	Juvenile Justice (Care and Protection of Children) Act, 2 015	Section 2(12)	18
7	The Protection of Children from Sexual Offences Act, 2012.	Section 2(d)	18
8	India Apprentices Act, 1961	Section 3(a)	14

*Table 1[3]

[3] This table provides the analysis of the term "child" and "minor" under different legislations in India.

The Srikrishna Committee, (Committee of Experts under the Chairmanship of Justice B.N Srikrishna, 2018.) tasked with developing the Personal Data Protection Bill, 2019, selected the age of 18 years to designate minors in order to align with existing legislation. However, as elucidated previously, various statutes referring to children, including socially beneficial legislation specifically concerning children, define "child" differently. The Committee subsequently observed that the age threshold in the 2019 Bill may be set excessively high and warrant revision, accounting for children's developmental evolution and emerging capacity.
However, an umbrella categorization of children under 18 will not be able to demonstrate the steps to be taken to harbour the security needs. This is so because children of different age groups suffer from varied threats. A young child of less than 8 years old is very unlikely to have the same problems as a 14-year-old child. Therefore, we need to keep various factors in mind while designing the cyber security mechanism for children. Reducing this age bracket cannot come at the cost of protecting children. Hence, it is important that additional protections are provided to children, addressing their vulnerability against the processing of their data. This becomes even more important when such processing is being done against their interests.

Chapter 4 of the 2019 Bill intends to achieve two key objectives: first, implement age verification mechanisms; and second, prohibit tracking and behavioral monitoring of children, thereby precluding targeted advertising. However, these provisions engender issues. First, the notion of a "guardian data fiduciary," and second, the differential between the age of consent and the definition of "harm." Differing ages have been embraced by the National Commission for Protection of Child Rights, enunciated through guidelines on online protections specific to adolescents. Additionally problematic is the absence of discussion regarding sensitive personal data- while the term itself does not appear, related factors constitute liability criteria for data fiduciaries, creating legal uncertainty.

Moreover, Proposal 5 by the Joint Committee on the 2019 Bill suggests renewed consent upon attaining a majority as defined under the Majority Act at 18 years. (*Joint committee on the personal data protection bill, 2019*, 2021, p. 22) Here, the Committee subtly distinguishes between the age of majority and the age of consent which will be scrutinized in the paper. Furthermore, Proposal 47 requires that guardian data fiduciaries managing children's data register with the Data Protection Authority (DPA). Finally, under Proposal 37, the Committee denotes the concept of a "Data Fiduciary Guardian" as redundant as superfluous.

3.2 International Legislations

In contrast to the age limits described in international laws and agreements, the US Children's Online Privacy Protection Act,1998 (COPPA) sets the age of consent at 13 years old. COPPA requires 'verifiable parental consent' only

when children are younger than 13 years old. The European Union's General Data Protection Regulation (GDPR) (General Data Protection Regulation, 2016) delineates an age bracket ranging from 13 to 16 years old. With regards to online privacy rights for children, the statutory age minimum for consent comprises 13 years old in the US, 16 years old in China, and 18 years old in the UK.

The table below delineates the varying age thresholds defining a 'child' with regard to online privacy and data protection across different international legislative frameworks:

S. No.	Country	Legislation	Age of child for personal data processing
1	Argentina	Personal Data Protection Act, 2000	18
2	Australia	Privacy Act, 1988	15
3	Austria	Data Protection Act, 1999 (under GDPR)	14
4	Belgium	Protection of Natural Persons with Regard to the Processing of Personal Data, 2018 under GDPR	13
5	Brazil	Lei Geral de Proteção de Dados (LGPD) or General Data Protection Law, 2018 (in English)	12
6	European Union (EU)	General Data Protection Regulation, 2016 (GDPR)	13-16 (left to the specific countries to provide the same in their domestic legislation)
7	Canada	Municipal Freedom of Information and Protection of Privacy Act, 1990 (MFIPPA)	13
8	China	Regulations on the Protection of Minors in Cyberspace, 2024; and Personal Information Protection Law, 2021	16
9	Denmark	Databeskyttelsesloven or The Data Protection Act (in English)	13
10	Finland	Finnish Data Protection Act, 2018	13
11	Frace	French Data Protection Act, 1978 (under GDPR)	15

12	Germany	Federal Data Protection Act, 2017 (under GDPR)	16
13	Greece	Personal Data Protection Authority, 2019 under GDPR.	15
14	India	Information Technology Act, 2000	18
15	Japan	Act on the Protection of Personal Information, 2003 (APPI)	15
16	Portugal	Portuguese Data Protection Law, 2019 (under GDPR)	13
17	Singapore	The Personal Data Protection Act, 2012	13
eighteen	South Africa	Protection of Personal Information Act, 2013	18
19	South Korea	Personal Information Protection Act, 2011	14
20	Spain	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales or the Organic Law 3/2018 on Protection of Personal Data and Guarantee of Digital Rights (under GDPR)	14
21	Sweden	Swedish Data Protection Act, 1973	13
22	UK	Data Protection Act, 2018 which is an implementation of General Data Protection Regulation (GDPR).	18
23	USA	Children's Online Privacy Protection Act, 1998	13

*Table 2[4]

4. Concept of 'child vulnerability'

In our hyper-connected world, some believe privacy is mythical - rendering protections futile. They argue privacy, if existent, acts as currency exchanged for digital services benefitting both adults and children. Some claim privacy concerns stem from media hysteria surrounding children's Internet of Things (IoT) usage. (Cavoukian & Popa, 2016, p. 5) However, even privacy skeptics admit vulnerable groups like children necessitate strengthened protections in

[4] This table provides for the age of the child for personal data processing across various legislations or policy framework globally.

the digital era. Children perpetually inhabit internet-suffused environments - immersed across public and private domains, ingrained in daily life.

Alarmingly, children's learning data - including thinking patterns, learning trajectories, engagement scores, response times, pages read, and videos viewed - face digitization and storage. While the online world presents children with opportunities, risks persist - like online sexual abuse and personal data collection for targeted advertising. Marketers can mislead children unable to differentiate ads from content or fiction from fact. (UC Berkeley Human Rights Center, 2019) Children are spending more time online, starting younger - a child goes online for the first time every half second globally. The internet holds creative, educational promise when accessible to all. However, risks exist.

Cyberbullying and online violence affect children via social media and messaging. Browsing exposes them to hate speech, and violent content encouraging self-harm and suicide. Tech companies compromise privacy via child-targeted marketing and excessive screen time hampering healthy development.

Most disturbing is the ease of online sexual exploitation and abuse - offenders easily contact and share imagery with potential victims. Children face risks like sexual abuse material production/distribution/consumption, grooming for exploitation, and offenders attempting in-person meetings or soliciting explicit content. (*Children rights in the digital age | Trends in 2024*, 2024). Anybody anywhere can create/store abusive material digitally. Offenders may livestream home-based abuse of distant children. Children may also self-generate explicit imagery intended for age-appropriate relationships then widely shared without consent. Trusted adults sometimes solicit such imagery, bringing social, mental, physical, and behavioral harm. These risks hamper childhood/adolescent self-development and severely damage mental, emotional, and physical well-being. (Shmueli & Prigat, 2011)

India's rich-poor gap exacerbates the issue - wealthy children enjoy the latest gadgets and tech-savvy parents while poorer families remain unaware of tech's harms. Internet expansion in education, especially post-pandemic, heightens this. Hence child digital vulnerability results from fluctuating societal/environmental factors interacting over time. Age shapes needs and risks. While global child Internet access rises, inequalities persist regarding connectivity, cost, necessity, and cultural/political settings - impacting exposure. Domestic and foreign legislations delineate varying child ages depending on legislative purpose, environment, and capacity - questioning the suitability of India's blanket 18-year age limit digitally. However, an umbrella categorization cannot address age-specific security needs - an 8-year-old faces different threats than a 14-year-old. Cybersecurity mechanisms must account for these factors.

5. Age of contractual capacity v. Age of consent

5.1 Age of Contractual Capacity

Minority status conferring legal incapacity remains entrenched across diverse jurisdictional and statutory frameworks. Certain jurisdictions confer limited contractual capacity on minors, while others deem all minor contracts void. Such provisions originated in pre-digital eras. However, today's digitally immersed minors undertake exponentially more heterogeneous transactions relative to previous generations - spanning online retail purchases, social media account creation, and conventional employment contracts.

This paper argues that the current understanding of contracts for necessities and contracts benefiting minors does not adequately address the gap between the law and reality. The law views being a minor as almost the same as being unable to enter into contracts. But in reality, minors today are entering into more and more contracts - like creating social media accounts, shopping online, or taking a part-time job.

The Indian position is that minor contracts are unenforceable unless they are 'contracts for necessaries or contracts for the benefit of the minor. Section 2(h) of the Indian Contract Act of 1872 defines a contract as an agreement holding legal validity between two or more parties. Per Section 10, contractual competence necessitates both parties possess the capacity to enter into it.

Section 11 outlines competence stipulations, stating:

"Every person is competent to contract who is of the age of majority according to the law to which he is subject, and who is of sound mind, and is not disqualified from contracting by any law to which he is subject."

Two interpretations are possible; the minor is incompetent to contract and thus their agreement is void, or he/she is not bound by the contract, while the other major contracting party is, which results in a voidable contract. In 1903, the Privy Council sought to bring this controversy to rest by making a final determination on the validity of minors' contracts. *Mohori Bibee v. Dhurmodas Ghose* (*Mohori Bibee v. Dharmodas Ghose*, 1903) is considered the authority on the question of the status of minors' contracts.

This establishes India's age of contractual capacity as 18 years - the age of legal majority. However, "beneficial contracts" constitute an exception. For instance, a minor cannot partner in a firm per Section 30 of the Indian Partnership Act - but they may benefit from the partnership, not sharing losses barring third-party obligations. Their liability remains confined to a firm asset share, exempted from personal liability. Adults jointly contracting with a minor and third- party bear sole accountability for whole contract conditions. With a minor as an agent, the principal retains liability.

Contracts in the digital age fall into three main categories: (Gangwar, 2022)

i. Formed and performed entirely offline
ii. Formed/performed both offline and online
iii. Formed and performed exclusively online

The first category has existed since the beginning of commerce. Legal systems have put in place policies and rules, although imperfect, governing minors entering these traditional contracts. The latter two categories are modern creations. The second category enjoys both digital and non-digital benefits. For example, minors previously bought physical books, clothes, and food. Now, especially amidst COVID-19, e-commerce for doorstep deliveries has become popular thanks to websites like Amazon, Flipkart, and Myntra. However, these digital transactions supplement rather than replace non-digital commerce. This hybrid system aims to reduce transaction costs while retaining the same ends. The third novel category entails transactions lacking real-world equivalents - like social media account creation, YouTube monetization, app development and sale via Google/Apple stores, esports player contracts, etc. The subject matter inhabits digital realms for exclusively online performance. While technically feasible to form such contracts offline, electronic formation through a few mouse clicks proves more expedient.

Traditional contracts retain policies for minors while modern contracts raise new issues - sometimes complementing the physical world, sometimes exclusively online. Legal frameworks must evolve to address minors' contracts in the digital age. Minors cannot be declared insolvent since they lack contractual capacity. Guardian liability for minor arrangements is also negated regardless of necessities acquisition - liability only holds for guardians themselves acting as principals with minors as agents.

5.2 The Conflict

India has linked the age of consent for data processing to contractual capacity, setting it at 18 years. This differs from the EU's GDPR, which separates consent for contracts and consent for data processing. The age of consent was a contentious issue during the development of the GDPR in 2015. The EU proposed raising it from 13 to 16 years, but critics argued this would prevent children from using social media effectively. As a compromise, under Article 8, the GDPR allows EU member states to set their own age of consent from 13-16 years. (General Data Protection Regulation, 2016)

Concerns raised during the GDPR's development about setting the age too high are also relevant for India setting it at 18 years. These include children lying about their age, reduced investment in online services for children, barriers for at-risk youth accessing information, and impacts on children's critical thinking development.

India's own White Paper on Data Protection (*White paper of the committee of experts on a data protection framework for India*, 2017) highlighted similar concerns about setting the age at 18 and preventing children's internet access and development. Setting a universal age limit fails to account for children's evolving capacity as they mature. Treating all under-18s equally does not recognize their growing abilities.

The UK and Ireland take a more nuanced approach, with lower ages of consent (13-16 years) but added protections for children under 18. This recognizes their changing capacities in a privacy-protected environment. United Kingdom Information Commissioner's Office (ICO), Age-Appropriate Design Code of 2022 provides differentiated standards for various age groups: (Age appropriate design: a code of practice, online services, 2020)

i. Pre-literate and early literacy (ages 0-5)
ii. Primary school years (ages 6-9)
iii. Transition years (ages 10-12)
iv. Early teens (ages 13-15)
v. Approaching adulthood (ages 16-17)

These guidelines recognize the developing aptitudes and requirements of children in different age groups while they grow. Rather than a blanket age threshold of 18 years for "data consent", the Indian government should adopt similarly nuanced guidelines that are bound to the different stages of children's growth. Implementing the age-appropriate design features as specified by the UK code is a worthwhile process in the sense that it would offer proper privacy protection to the children and empower them to safely navigate through the digital world securely. Using the ICO's approach as a model for data consent in India would be progressive rather than the present all-inclusive age limit of 18 years for consent.

6. Digital Age of the Child

The "digital age" refers to the age when a child starts using digital technologies like the internet, smartphones, and social media. The online world is different from the physical world. Children need tailored protections online compared to offline. This paper suggests defining separate privacy ages for children in the digital realm, based on their evolving capacities. Domestic laws define "child" differently based on environment, nature of work, and social conditions. Similar factors should determine digital privacy rights for children. Their digital age should consider the surrounding context and gradually expand privacy rights as they mature. Rather than rigid age thresholds, children's demonstrated maturity and ability to comprehend online risks should guide their digital privacy rights. Technical tools to verify age must balance privacy protections with enabling children to benefit from digital participation. With proper safeguards, children can safely access online services as per their evolving capacities. (Siibak & Mascheroni, 2021) Their fundamental right to

privacy must be upheld while addressing potential harms through balanced regulatory approaches.

Digital services often target youth as primary users, given their adeptness with new technologies. However, minors may be unable to legally consent to digital contracts. Ascertaining age poses challenges online. While children are early adopters of digital applications, they require safeguards around personal data collection and use. Their digital participation should align with evolving capacities, not rigid age cut-offs. Technical tools for age verification must balance privacy protections and enable access to beneficial services. Overly broad age restrictions could impede children's digital literacy and rights. Children's demonstrated maturity level, rather than just age, should determine their digital privacy protections. With proper governance, minors can safely benefit from digital engagement tailored to their evolving abilities. Balanced regulation and design are key to upholding minors' interests in the digital economy while protecting their right to privacy.

Signing up for an account on Instagram involves entering into a contractual relationship with its parent company Meta (formerly known as Facebook). The minimum age to have an Instagram account is 13 years although most social media companies do not have an age verification mechanism in place, potentially enabling under-13-year-olds to enter into these contracts with the company. Even if they did, their policies nevertheless allow minors between the ages of 13 and 18 to enter into contracts with them. The terms of use for these 'Meta Products' include collecting and storing the information and content provided by the user consciously, and the metadata provided unconsciously, and by third parties, among others. Essentially, the consideration provided by the user to partake in these 'free services' is the user's data; minors give information about themselves in return for the opportunity to use the app and engage with the world. Minors exchange information for social media access, unaware of privacy risks. While they benefit from engagement, their data may be exploited without recourse. Influencer minors also provide services to platforms, but lack remedies if arrangements turn sour. They market products without contractual capacity or safeguards. Rather than broad blocking of services, minors need tailored supervision aligned with evolving maturity. Policies and designs should be moderated in a way that the digital space would enable minors to interact online safely. Companies must possess practical policies that put children's data protection first and also shed more light on the commercial transactions undertaken concerning the data. Oversight is needed to uphold children's interests in the digital economy.

This issue brings forth a lot of complex questions such as if courts deem social media accounts "necessary" or "beneficial" to minors, who would set boundaries for them? Is it appropriate for judges to decide the number of accounts that a minor can have or those that are better for their well-being? And if such accounts are hypothetically deemed unnecessary and not beneficial, they

will continue being trapped in void contracts where they don't have any concrete rights. With proper governance, minors could interact online safely per their evolving maturity. The companies should keep the children's data and interests secure while profiting from their participation in their business. Surveillance systems have to guarantee minors' right to privacy on the internet. However, it should be balanced against their rights to access beneficial services and to get accustomed to digital services. Their interests should be protected while they are fully engaged in the internet without unjustly involving them in online activities beyond their capacities.

On the flip side, however, some queries actually reorient the spotlight from the protection of children's contractual interests to the judicial overreach of social media consumption. What is the extent of powers that contract law should possess over the domain of social media today? Even though one might contend that the purposes of such judicial inquiry are not about the regulation of social media, it is hard to see how courts ultimately decide on the enforceability of digital contracts that underscore minors' positions without delving into normative issues of what is a socially optimal level of media consumption. While, this will open another Pandora's box, adding issues of privacy and individual freedom to the existing ones. What initially began as a benign discussion about protecting minors as they engage with the digital world may evolve into a discourse about their permissible interactions and behaviors.

Online activities often mirror the daily realities that children encounter in their homes, schools, and broader communities. Strategies aimed at promoting online safety should not only safeguard the educational and health benefits of digital technologies but also address the potential risks of exposure to violence, exploitation, abuse, and privacy breaches.

7. Principles and Rights Underlying Privacy

In the early stages of the Internet, the primary focus of Internet governance revolved around the technical aspects of the ecosystem. This entailed engineering efforts to ensure connectivity, with little consideration given to the content being transmitted and its impact on users and society at large. However, over time, Internet governance has evolved to place greater emphasis on the content disseminated on the web. A notable progression has been the determination of what content is appropriate for different segments of society. (Atabey & Scarff, 2023) As discussed earlier, children, as a vulnerable group, require protection from harmful content while still enjoying the benefits of the Internet. Unfortunately, it took a considerable amount of time for Internet governance to formally recognize and address children's rights.

Although the World Summit on the Information Society (WSIS) (*Declaration of principles building the information society: A global challenge in the new millennium*, 2003) acknowledged the significance of children's rights on the Internet in 2003, the establishment of the Internet Governance Forum (IGF) through the 2005 Tunis Agenda (WSIS 2005) did not fully embrace a

comprehensive and positive outlook on how the Internet can improve and advance the lives of children. This deficiency can be attributed to the lack of formal recognition of children's rights within the framework and mechanisms of Internet governance.

The current focus in Internet governance on preventing the spread of child abuse content and illegal contact with child sex offenders falls short of addressing all the issues affecting children's rights. This limited perspective treats children solely as victims, overlooking their rights to autonomy, access, information, privacy, and participation. Such an approach may result in overly strict regulations for children, hindering their self-expression, or prioritizing the online freedoms of adults over the needs of children. Conjoining this is the fact that UN organizations and related bodies have expressed concern about the effect of the internet on children's safety and rights. In September 2014, the UN Committee on the Rights of the Child organized a special day for discussing children's rights and digital media with an aim to develop strategies that will shield the young generation from online dangers without taking away online opportunities.

The United Nations Convention on the Rights of the Child (UNCRC) is a crucial regulation that has been adopted and recognized in most countries as a means to protect children's rights. India being a signatory to the CRC is thereby bound by law to incorporate its principles as a part of national governance. The significance of the CRC in promulgating children's rights has persuaded nations to look for its implementation in the digital world. In 2021, the UN Committee on the Rights of the Child released Comment No. 25 (Committee on the Rights of the Child, 2021) that recommended state parties to implement the CRC in the digital environment.

7.1 Best Interest of the Child Principle

The principle that the child's interest should be given the highest priority becomes even more vital within a digital era when children become more and more active on the internet and in online services. Underpinning this dictum is Article 3 of the UNCRC, which further emphasizes that in all actions concerning children, their best interests must be a primary consideration. In the context of the digital realm, this principle becomes even more crucial as children navigate a complex and rapidly evolving online environment. One of the key challenges in applying this principle in a digital age is the balance of the advantages of digital technologies with the potential threats they pose. On one hand, the internet and social media provide children with a wide range of information, learning materials, social interaction opportunities, and so on, but at the same time, the same technologies could be used by children in such a way that would expose them harmful content, violations of privacy and online threats, such as cyberbullying and exploitation. (Collinson & Persson, 2022) In order to effectively safeguard the digital rights of children and preserve their well-being in an online environment, it becomes imperative to involve not only

policymakers, but also representatives of the industry, educators, and parents who pursue a child-centred approach towards digital designing and regulation. The ICO's Age Appropriate Design Code is a critical body in this context as it places the best interests of the child at the forefront of its requirements for online service providers. By emphasizing the need to consider children's perspectives, vulnerabilities, and rights when designing digital services, the Code aims to create a safer and more child-friendly online environment.

In the digital age children's agency rights become a central pillar towards upholding children's best interests. Ensuring that children are able to make conscious choices about their digital actions, privacy settings, and dealings is a vital step toward letting them experience a sense of freedom and self-actualization. (Dmytro & Myroslava, 2023, p. 8) Ensuring that children are empowered with tools to safeguard their digital privacy and security is a significant component that is part of the right-to-agency principle under Article 3 of the best interests of the child provisions.

Furthermore, the question of who decides the best interests of the child in the digital era is quite complex and multifaceted. Although, parents, educators, industrial stakeholders, and policymakers are quite significant, what is more important is that they are factored in decision-making processes that affect them, which should be inclusive of them. (Bogani & Schafer, 2022) The inclusion of the 'best interest' of the child in an AI-driven digital age requires a comprehensive and holistic approach, from designing and regulating to deploying these systems. By prioritizing this we will be able to create a more conducive and supportive digital environment for the upcoming generation. It is important to emphasize the fact that all stakeholders should cooperate so that children can use the internet and social media safely; allowing them to get the best of what these platforms can offer. This will also foster awareness and protection from possible present and future dangers.

8. AI and the Digital Child

The advent of the digital era has transformed the fabric of daily life, weaving digital experiences into the developmental journey of children. The immersion of young minds in online spaces is a double-edged sword; while it opens doors to infinite knowledge and connectivity, it also ushers in challenges to privacy and safety that are unprecedented. (*Guidelines on artificial intelligence and children's rights*, 2020) As AI weaves its way into the tapestry of digital interactions, its influence on the privacy and well-being of children has become a focal point of discussion.

8.1 AI's Potential Threats to Online Child Safety

The concept of children's privacy in the era of AI is multifaceted and encompasses the right of minors to control their own information, navigate spaces autonomously, communicate without being intercepted, and make decisions independently. This notion is not only complex but also highly dependent on context and relationships. It involves several factors, including the extent of private life that is exposed, the entities that have access to this information, the purposes for which it is used, and the potential consequences thereof. (*The rights of the child in the digital environment* 2014)

The advent of AI, through the collection and algorithmic processing of data with minimal regulation, presents various risks to all dimensions of children's privacy. These risks are categorized into data-related risks, functional risks, and risks stemming from insufficient oversight. Data risks include the extensive collection of sensitive information about children, which can be accessed and used over long durations and for various purposes, thereby compromising their privacy. (*Children's rights and business principles: Artificial intelligence*, 2020) Several instances highlight the application of AI in public services and spaces impacting children's privacy. For instance, Cadillac Fairview Malls utilized facial recognition technology in Canadian malls' directories without proper consent, capturing and analyzing visitors' facial data. Similarly, the Allegheny Family Screening tool in Pennsylvania employs an algorithm to identify children at risk of neglect or abuse, influencing decisions on when to intervene.

The scope of data collection by AI is vast, generating significant amounts of information, sometimes beyond what is necessary for functionality. This often requires children or their guardians to consent to comprehensive data collection through complex agreements that do not facilitate genuine consent. (Baird, 2023) The diversity of data collected extends to all aspects of children's lives, including data traces left in digital spaces and information collected through AI technologies used by parents, caregivers, and even strangers. Sensitive data collected by AI systems may include personal identifiers that risk children's security and privacy. The sale and sharing of children's data with third parties without prioritizing their interests highlight another aspect of the risk posed by AI. This information, valuable within the data economy, may be used for commercial and institutional purposes unrelated to the initial intent, potentially affecting children's future opportunities and privacy. Functional risks pertain to how AI uses data in processes that can infringe on children's privacy through surveillance, profiling, and decision-making functions. (*Children and AI,* UNICEF) These functions often overlap, with AI applications leading to extensive surveillance and profiling of children, categorizing and assessing them in ways that are difficult to challenge. Oversight risks in AI governance touch upon fairness, transparency, explainability, and accountability of AI systems. (Children's rights and business principles: Artificial intelligence, 2020) These principles play a critical role in securing AI systems that do not

abuse and misuse children's information or have any negative impact on their lives. While AI predicts to promote equality and ensure an inclusive society, the systems sometimes amplify the existing biases or brings about unfair and discriminatory outcomes. Transparency and accountability of AI use are critical for ensuring that AI is used correctly, and especially when it comes to children's data and privacy.

It is important to bring the intersection of children's privacy and AI technology into the light of consideration, for a close examination of risk associated with data, function, and oversight risks. AI implementation and application in the area of children pose the demand for a harmonious method that on the one hand offers the necessary safeguards to children's privacy and on the other leverages technology (Children's rights in the digital age: A download from children around the world 2019).

8.2 The Transformative Role of AI in Child Online Safety

Digital playgrounds are giving children tremendous scope to learn, entertain, and interact socially. Yet, this digital playground has several riders attached, such as exposure to inappropriate content, cyberbullying, and predation. AI shines through this bleak terrain reflecting its own ideas on the online safety of children. (Bogani & Schafer, 2022) AI-driven content filters represent a truly advanced step, using intelligent algorithms to sift through digital content and ensure that they are exposed to only that content which is suitable for them. These filters extend beyond blocking out keywords by using natural language processing (NLP) and image recognition to understand the context and meaning of the digital content. Social media, another predominant aspect of the digital life of children also presents another arena where AI can contribute the greatest. AI-powered surveillance systems can automatically detect odd patterns, including cyberbullying and in this way can make the parents or guardians vigilant in real-time, thereby ensuring children's well-being. In addition, AI proves to be an effective tool in the determination of online predators by observing the patterns of communication and drawing attention to suspicious activities. This preventive methodology empowers law enforcement and administrators to intervene even before harm can occur. (Guidelines on artificial intelligence and children's rights, 2020) Educational AI assistants can also play a pivotal role in teaching children about online privacy. These assistants can be interactive during the sessions which can be helpful to children to understand the importance of keeping personal information private and recognizing potential online threats. (Irwin et al., 2021)

Generation in a digital age, children nowadays are navigating through a complicated online spectrum of endless chances coupled with lot of risks. AI stands symbolically as a junction where technology meets ethics, embarking on a mission of turning the internet into a safe haven for children. (Livingstone et

al., 2019) By harnessing AI responsibly, society can unlock a future where the digital realm is a safe space for children to learn, grow, and connect. However, achieving this vision requires vigilance, collaboration, and an unwavering commitment to upholding the privacy and well-being of the youngest members of the digital community.

9. Children's Data Privacy Regime in the United Kingdom

The United Kingdom has realized how vital it is to protect children from exposure to unwanted content in a dynamically changing digital arena. In fact, it has created an extensive legal framework to guarantee that their rights are defended. The implementation of the UK GDPR and the Age Appropriate Design Code in 2020 allows for the adequate protection of children from those whose intent is to misuse and abuse their personal data and prioritize their well-being.

Children's personal data is considered especially vulnerable in the UK. Thus, further measures are introduced to protect their personal rights. To illustrate, ensuring that a child of 13 and above is able to give their explicit consent is also mandatory before any processing of their personal data. Such obligation will arm the children with the knowledge to make the right choices regarding their data, hence, accelerating the transparency and accountability in data handling procedures.

The Age Appropriate Design Code of the UK GDPR translates into real life and its rules are in line with international ones, such as the UNCRC, establishing a comprehensive approach towards the protection of children using digital services. The code outlines key provisions that are essential for protecting children's privacy such as enabling high default privacy settings, minimal collection of data and retention, limiting the possibility of sharing data, and also providing parents controls and filtering restrictions and geological services.

By mandating high privacy settings as the default option, unless there is a compelling reason otherwise, the code ensures that children's privacy is prioritized from the outset, creating a safer online environment. Additionally, online services are required to collect and retain only the minimum amount of personal data necessary, reducing the potential risks associated with excessive data processing. Furthermore, the code emphasizes the importance of limiting the dissemination of children's data, aligning with the principle of restricting data sharing. Geolocation services are also required to be switched off by default, preventing unnecessary tracking and monitoring of children's physical locations, thereby enhancing their privacy and safety online. The code addresses pertinent issues relating to parental control and profiling thereby emphasising the need to consider the impact of these practices on children's privacy. The UK's legal framework concerning children's privacy issues is comprehensive, forward-looking, and developed in accordance with international standards. It prioritizes children's safety and well-being,

supported by the principle of acting in their best interests and protecting their privacy.

10. Legal regime in India

The recently passed Digital Personal Data Protection Act of 2023 in India includes provisions related to processing the personal data of children under the age of 18. The Act is intended to provide legislative expression to the contours of the right to privacy as outlined by the Supreme Court of India in the *Puttaswamy* (*Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors*, 2018) Judgement and since then, by other constitutional Courts. Specifically, Section 9 requires parental consent, requires data processing to align with children's well-being, and bans tracking, behavioral monitoring, or targeted ads directed at children.

While this aims to protect children's privacy, it may undermine children's autonomy and decision-making abilities. Children have evolved capacities and the ability to make rational decisions about their privacy at different ages. Rigid age restrictions may prevent even mature teenagers from controlling their own data and experiences online. Moreover, relying on parental consent is questionable given the low digital literacy rates in India. It may enable parents to restrict access to certain information based on ideological grounds, harming children exploring issues of gender and sexual identity. A better approach may be a flexible, risk-based system that empowers children as they gain competence. The requirement of "verifiable consent" also raises issues. (Livingstone et al., 2019) Verifying age and parental consent online is challenging. The rules will need to provide clarity on consent mechanisms and potential age verification systems.

While restrictions on tracking and behavioural monitoring aim to protect privacy, they may also prevent platforms from protecting children from harmful content. Some safeguards may be necessary, but an outright ban could undermine child safety. Scope remains for the upcoming rules to address gaps regarding risk-based approaches, defining well-being, and balancing privacy with safety. The main laws covering online crimes against children in India are the Protection of Children from Sexual Offences (POCSO) Act 2012, the Information Technology Act 2000, and the Indian Penal Code, 1860. POCSO criminalizes sexual exploitation of children online including using them for pornography, grooming, and pornographic performances. Section 67B of the IT Act also bans publishing or sharing material showing children in sexually explicit ways. Additionally, Section 66E of the IT Act protects children by prohibiting the distribution of private, intimate images without consent. Other provisions like Sections 66C and 66D punish identity theft and impersonation online, which could also be used against children. Section 43A makes companies liable if they negligently handle children's personal data without security safeguards. While the Indian Penal Code does not specifically mention cybercrimes against children, some of its general offenses like financial fraud,

sexual harassment, stalking, and intimidation would apply if committed through digital means targeting children.

With increased internet access, online availability of child sexual abuse material has become a major concern addressed by Indian courts. The High Court has directed intermediaries to implement filters, provide reporting tools, and proactively identify websites distributing such illegal content. The landmark judgment *Justice K.S. Puttaswamy vs Union of India* judgment established privacy as a fundamental right under the Indian constitution, beyond just a contractual provision. Articles 19 and 21 of the Constitution were interpreted to guarantee the right to informational privacy as a basic freedom.

Justice Chandrachud emphasized in his ruling that privacy enables people to control important aspects of their lives and thus protects individual autonomy. Personal lifestyle choices are an integral part of one's privacy and should not face unreasonable restrictions. With increased internet access, the availability of child sexual abuse material online has become a major issue addressed by Indian courts. In the Re: *Prajwala ad Kamlesh Vaswai v. Association of India*, (*Kamlesh Vaswai v. Association of India*, 2016) the Supreme Court instructed intermediaries to implement filters, provide reporting tools, and proactively identify websites distributing such illegal content.

While these cases relate to the informational privacy of children, as their personal data is made available without guardian consent, privacy concerns were not the main focus. Rather, the court rulings centered on tackling the distribution of abusive material itself as well as intermediary obligations in limiting access to such content. The judicial directives around child sexual abuse content online aim primarily to curb distribution and access from a child protection standpoint rather than a privacy standpoint per se.

In 2012, the Srikrishna Committee drafted guidelines for a data privacy law in India but did not substantially link contractual ability to the age of consent for data collection. It recognized that vulnerable groups like children need special protections in the consent process. Later, the Justice Srikrishna Committee addressed child privacy more comprehensively. It proposed rules requiring fresh consent from individuals when they turn 18, with their data access not being discontinued during this transition process. Entities handling children's data would have to register as "Big Data Guardians" with additional oversight.

While initial privacy discussions gave limited attention to child users, more recent expert panels have made specific recommendations to encode stronger safeguards for children into India's data privacy regime. However, the actual regulations drafted are still awaited, and their ability to protect child rights in the digital economy remains to be seen. Overall, more nuance is required in India's approach to children's data to respect evolving autonomy while also providing appropriate oversight and protection aligned with their best interests. The specifics of the upcoming rules will be critical.

11. Conclusion

This paper delves into the critical discussion surrounding the protection of children's privacy and their safety on the internet within the context of digital governance. This research on the state of children's privacy in India vis-á-vis global standards for children as "netizens" seeks to alert the policymakers of the need to tailor the legal framework to the special needs of children for their specific digital rights. While some countries have already enacted privacy policies that also address children's protection within the privacy regulations framework, India has an opportunity to create a framework that prioritizes the well-being of children without being bound by existing norms. Drawing insights from international instruments and legislative developments, several recommendations emerge for enhancing the privacy and data protection of children:

i. *Data Minimization Approach*: Emphasize the necessity of collecting only the necessary personal information to avoid over-specificity and potential profiling. Data collection should operate when a child is only active in the usability of the service, and minimal data should be saved and shared with the outside world.
ii. *Multi-stakeholder approach*: To navigate through AI's potential, as well as its pitfalls, a multi-stakeholder approach is imperative to negotiate these in the context of child online safety. Governments, technology corporations, educators, and guardians need to develop and execute policies that ensure protection of children in the digital environment.
iii. *Digital Literacy:* The difference between professional knowledge of the internet and essential knowledge is imperative to safeguard their digital world. Digital literacy should allow children to get hold of digital tools, engage with them for fun and learning, socialize, and be safe, among other benefits.
iv. *Curriculum Integration of Digital Skills and Wellness Modules*: Campaigning on the inclusion of the notion of digital literacy within the school and university courses, just as is practiced in many countries, such as in the Philippines, digital upskills mobilization alongside constant reskilling become a must due to the ever-changing nature of the digital environment.
v. *Shift the Onus of Protection onto Providers*: Consumers are becoming increasingly aware of data privacy issues and providers need to ensure that they guarantee users a higher degree of transparency and control. Recent examples of data privacy problems reflecting the sense of self-determination, which should be possessed by the individuals, have led to better sorting of their sharing practices on data.

By implementing these recommendations and fostering a culture of digital responsibility and empowerment, India can pave the way for a safer and more inclusive digital environment for children, ensuring their rights and well-being are safeguarded in the digital age.

References

Age-appropriate design: a code of practice for online services, Code of practice (2020) (United Kingdom).

Atabey, A., & Scarff, R. (2023). The fairness principle: A tool to protect children's rights in their interaction with emotional AI in educational settings. *Global Privacy Law Review*, *4*(1), 5–16.

Baird, D. E. (2023, March 27). Protecting children's rights and data privacy in the age of AI. *Medium*. https://derekebaird.medium.com/the-importance-of-protecting-childrens-rights-and-data-privacy-in-the-age-of-ai-c154d22f9d0f.

Bogani, R., & Schafer, B. (2022). Artificial intelligence and children's rights. In M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, & R. Andorno (Eds.), *The Cambridge handbook of information technology, life sciences and human rights* (pp. 215–230). Cambridge University Press.

Cavoukian, A., & Popa, C. (2016). Embedding privacy into what's next: Privacy by Design for the Internet of Things. *Ryerson University Privacy & Big Data Institute*, 1–10.

Charisi, V., Chaudron, S., Gioia, R. D., Vuorikari, R., Planas, M. E., Sanchez, I., & Gómez, E. (2022). *Artificial intelligence and the rights of the child: Towards an integrated agenda for research and policy* (EUR 31048 EN). European Commission.

Charter of fundamental rights of the European Union (2000/C 364/01). (2000). European Commission.

Children and AI Where are the opportunities and risks? (n.d.). UNICEF and World Economic Forum. https://www.unicef.org/innovation/sites/unicef.org.innovation/files/2018-11/Children%20and%20AI_Short%20Verson%20(3).pdf.

Children and AI. UNICEF. https://www.unicef.org/innovation/sites/unicef.org.innovation/files/201811/Children%20+%20AI%20Framework_%20Long%20Version.pdf.

Children rights in the digital age | Trends in 2024. (2024). Digital Watch Observatory. https://dig.watch/topics/childrens-rights.

Children's rights and business principles: Artificial intelligence. (2020). UNICEF. https://www. unicef.org/globalinsight/reports/childrens-rights-and-business-principles-artificial-intelligence.

Children's rights in the digital age: A download from children around the world (2019). EU Kids Online project. https://eprints.lse.ac.uk/101065/1/Sonia_Livingstone_EU_Kids_Online_2019.pdf.

Children's Parliament. (2023). *Exploring children's rights and AI: Summary report*. Scottish AI Alliance and The Alan Turing Institute.

Collinson, J., & Persson, J. (2022). What does the 'best interests of the child' mean for protecting children's digital rights? A narrative literature

review in the context of the ICO's Age-appropriate design code. *Communications Law*, *27*(3), 132–148.

Committee of Experts under the Chairmanship of Justice B.N Srikrishna. (2018). *A free and fair digital economy protecting privacy, empowering Indians*. Ministry of Electronics and Information Technology. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Committee on the Rights of the Child. (2014). *Report of the 2014 day of general discussion "digital media and children's rights"*. OHCHR. https://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf.

Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations. https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/UN_CRC_General%20comment%20No.%2025%20(2021)%20on%20children's%20rights%20in%20relation%20to%20the%20digital%20environment_En.pdf.

Convention on the rights of the child (No. 44/25). (1989). General Assembly resolution. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_44_25.pdf.

Declaration of principles building the information society: A global challenge in the new millennium (WSIS-03/GENEVA/DOC/4-E). (2003). World Summit on the Information Society. https://www.itu.int/net/wsis/docs/geneva/official/dop.html.

Dmytro, B., & Myroslava, B. (2023). Challenges for children's rights in connection with the development of artificial intelligence. *Visegrad Journal on Human Rights*, *2*.

Gangwar, S. (2022). Minors' contracts in the digital age. *Liverpool Law Review*. https://doi.org/10.1007/s10991-022-09298-3.

General Data Protection Regulation, Regulations No. 2016/679 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Guidelines on artificial intelligence and children's rights. (2020). Council of Europe. https://rm.coe.int/guidelines-on-artificial-intelligence-and-children-s-rights/1680a1d821.

Irwin, J., Dharamshi, A., & Zon, N. (2021). *Children's privacy in the age of artificial intelligence*. Canadian Standards Association.

Joint committee on the personal data protection bill, 2019 (17th Lok Sabha). (2021). Lok Sabha Secretariat. https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors, Supreme Court, September 26, 2018, AIR 2018 SC (SUPP) 1841 (India).

Kamlesh Vaswai v. Association of India, Supreme Court, February 26, 2016, 177/2013 (India).

King, J., & Meinhar, C. (2024). *White paper: Rethinking privacy in the AI era policy provocations for a data-centric world*. Stanford University Human Centered Artificial Intelligence. https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online Growing up in a digital age*: London School of Economics and Political Science*. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf.

Mohori Bibee v. Dharmodas Ghose, Judicial Committee of the Privy Council, March 4, 1903, ILR (1903) 30 CAL 539 (PC) (India).

Pedró, F., Subosa, M., Rivas, A., & Valverde, P. (2019). *Artificial intelligence in education: Challenges and opportunities for sustainable development* (ED-2019/WS/8). UNESCO.

Recommendation of the council on children in the digital environment (OECD/LEGAL/0389). (2021). OECD.

Rue, F. L. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/17/27). Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

Shmueli, B., & Prigat, A. B. (2011). Privacy for children. *Columbia Human Rights Law Review*, *42*, 759–795. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1746540.

Siibak, A., & Mascheroni, G. (2021). Children's data and privacy in the digital age. *CO:RE Short Report Series on Key Topics*. https://www.ssoar.info/ssoar/bitstream/handle/document/76251/ssoar-2021-siibak_et_al-Childrens_data_and_privacy_in.pdf?sequence=4.

The rights of the child in the digital environment (2014). Committee on the Rights of the Child.

The rights of the child in the digital environment. (2023). African Committee of Experts on the Rights and Welfare of the Child. https://www.acerwc.africa/sites/default/files/2023-02/DAC%20CONCEPT%20NOTE%202023_EN.pdf.

The state of the world's children 2017: Children in a digital world. (2017). UNICEF.

UC Berkeley Human Rights Center. (2019). *Executive summary artificial intelligence and children's rights*. UNICEF. https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf.

UNICEF & Ministry of Foreign Affairs of Finland. (2021). *Policy guidance on AI for children*. UNICEF.

UNICEF. (2014). *Children's Rights in the Digital Age* (ISSN 1816-7551). UN ECLAC.

White paper of the committee of experts on a data protection framework for India. (2017). Ministry of Electronics and Information Technology. https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

World Summit on the Information Society. (2005). *Tunis agenda for the information society* (WSIS-05/TUNIS/DOC/6(Rev. 1)-E). United Nations. https://digitallibrary.un.org/record/565827/files/6rev1.pdf.