

The children's rights-by-design standard for data use by tech companies

Pedro Hartung,¹ Alana Institute, Brazil

Introduction

In the debates about privacy and data protection, the prevalence of the consent standard in regulatory policies places a much greater responsibility on users, often exempting States or companies from the detrimental use of personal data and privacy violations.

In relation to children, the parental consent mechanism or the age appropriate indicator are even more questionable and usually insufficient, often leading to an illusion of protection. Either due to the lack of choice, the overload of information and consent, or the complexity of data processing, the vast majority of families adhere to the terms of use without full understanding of their meaning.² This generates a constant tension between the responsibility of online platforms or application providers and the families' and children's actual agency to deal with the complexity of the digital world.

However, the centrality of parental consent as the only threshold for assessing child protection in the digital environment could imply a mitigation of the responsibility of companies to ensure safe environments for children, free from violations of their rights.

This paper argues that the responsibility for children's data protection should also include the provider's responsibility as regards children's rights, especially when considering the design and development of any online product or service. Following the provision of Article 3.1, of the Convention on the Rights of the Child (CRC), all the decisions made by the States or also by private actors, such as business enterprises in the digital environment, should always consider their best interests and the promotion and protection of all their rights. Thus, companies should also refrain from violating rights through misuse of practices related to privacy and safety, and actively avoid all forms of economic exploitation, discrimination and infringement of any kind of freedoms.

Thus a children's rights-by-design (CRbD) standard for use of data by tech companies is needed. A CRbD standard would include the design, development and execution of online services or products used by children, in accordance with the CRC provisions and the primary consideration of children's best interests. The paper also highlights the duties of tech companies under the CRC and the possibility of their involvement in the international institutional mechanisms to monitor implementation of the CRC by the UN Committee on the Rights of the Child.

Children's rights violations and developmental impacts by detrimental use of data: who is responsible?

The idea that digital citizenship is achieved within the family or through classroom education on media literacy is an argument frequently used by tech companies,³ and makes their own responsibilities for protection of children from rights' violations mostly invisible in the public debate and in their own terms of use and privacy.

However, if misuse of children's personal data takes place in the digital environment and as a consequence their rights are violated, the greatest onus should not be on parents due to their consent or the lack of media literacy. A prime consideration in this regard must be the unequal power relationship between companies and families and the inability of most people to understand the complexity and opacity of digital relationships and business models in this area.

Therefore, it is critical to understand the different types of detrimental use of children's personal data by companies in the digital environment, highlighting its impact on children's development.

2.1 Privacy violations

It is well known that private actors have gained access to and developed technologies that monitor and collect information about individuals' communications, activities and behaviour on the internet.⁴ This tactic has indeed become the business model to monetize personal data for commercial and behaviour modulation purposes by using persuasive design in what has come to be known as the attention economy.⁵ Platforms and applications are consciously designed to encourage constant use and overexposure, so more data can be collected and stored, frequently ex-

posing users to mass surveillance, interception and data collection.⁶

Considering that children are the largest proportion of users of digital technologies in the world,⁷ the possibilities of violating their privacy and intimacy are even greater through use of social media, browser cookies, email, search engines, video platforms and applications, games, connected toys and things, educational platforms and services etc. This massive data collection raises significant concerns regarding exposure, storage and present and future use of digital tracks, especially concerning the child's development and evolving capacities.

Privacy and confidentiality are key aspects of children's holistic and healthy development, allowing them to make mistakes in a safe environment, promoting self-confidence and developing their maturity, enabling them to explore different dimensions of themselves, and develop their own identity, without risk of surveillance or exposure. Yet the massive digital tracks, data storage and dossiers created through digital technologies could be used in the future, affecting their access to education, employment, health care, and financial services.⁸

2.2 Safety violations: threats to children's moral, physical and mental integrity, and online sexual exploitation and abuse

The massive exposure and easy transit of children's personal data and persistent identifiers – such as name, address, phone number, email address, biometrics, photos, videos, audio recordings of the child, IP addresses – that can be used to track a child's locations and activities over time and across different websites and online services, pose several threats to their physical, mental and sexual integrity, especially through non-authorized and malicious contact, amplifying the risk of offline abuse.

For example, easy access to child sexual abuse materials and insufficient identification of and action to combat grooming and predatory behaviour in online spaces enables the exponential increase of harmful practices, such as online sexual exploitation and abuse.⁹

The lack of online safety by design and the misuse of children's personal data for harmful and predatory behaviour in digital platforms and services, search engines, livestreaming technologies, social media, chats, message apps and interactive games increasingly affect children's health and development and can have life-long impacts that also involve their families and all society.¹⁰

2.3 Economic exploitation: data-based marketing and digital influencers as business models

As part of several digital business models, personal data are often monetized by the commercial use of profiling and automated decision-making, microtargeting of advertising or even by selling data to third parties.¹¹ In this sense, children's experiences in the digital environment are often exploited for commercial purposes, especially by explicit or thinly veiled marketing strategies directed at them, such as advertising on video platforms, gamified ads, in-app purchases, online games or sponsored content and digital influencers. The massive use of child influencers on digital platforms and applications as a monetization mechanism by tech companies and advertisers is in itself an economic exploitation of a child's image and artistic data. Indeed, such usage

can be categorized as artistic child labour, defined by the presence of: periodicity of artistic production (children are encouraged to post new content frequently, respond to comments and always keep the audience engaged); monetization of the activity (the contents are profitable due to the operation of the platform itself and the presence of advertising by third companies); and expectation of external performance (children are not encouraged to just try out the platforms as self-expression tools or as content creators, but the platform design rewards constant use and engagement, adding more pressure for performance). Artistic child labour is therefore a practice that must always be authorized by the competent authority¹² and companies must always ensure such approval is obtained.

Children are particularly vulnerable to marketing, especially when it is based on personal data and microtargeting.¹³ Research and studies suggest that children up to 6 or 8 years old do not differentiate between advertising and content, nor do they have the necessary judgement to distinguish fiction from reality and, until they are 12, do not understand the persuasive nature of advertising, making them easily influenced by and susceptible to this type of commercial strategy.¹⁴

When children are informed of the presence of advertising in the digital universe, they express general discontent and annoyance. Moreover, marketing to children intensifies problems that jeopardize child development such as: obesity and chronic non-communicable diseases (NCDs), family stress and health impacts, violence, early binge drinking and smoking

habits, unsustainable consumption behaviours, gender stereotypes and precocious eroticism, unsound materialistic values and the free and full enjoyment of cultural rights.¹⁵

Cost benefit estimates in Brazil showed that enforcing restrictions on marketing to children under 12 years old could have important social and economic benefits, resulting in a physically and psychologically healthier population with positive economic results ranging from US\$61 to US\$76 billion after 15 years of a full ban.¹⁶

...children's experiences in the digital environment are often exploited for commercial purposes

It is crucial that the production of children's digital content should find other forms of financing, rather than targeting children through the advertising on their channels. In addition to public or private direct funding, the recent initiative by Google, after agreement with the Federal Trade Commission following alleged violations of the Children's Online Privacy Protection Act (COPPA) Rule,¹⁷ to set up its own US\$100 million fund to support the production of suitable children's content on YouTube over a three-year period¹⁸ is a good example for the establishment of digital spaces for children free from consumerist pressure.

The American Academy of Pediatrics recently issued a new policy statement expressing "concern about the practice of tracking and using children's digital behavior to inform targeted marketing campaigns, which may contribute to health disparities among vulnerable children or populations," suggesting that policymakers should ban all commercial advertising to children younger than 7 years of age, and limit advertising to older children and teenagers, among other recommendations.¹⁹

2.4 Freedom violations: lack of diverse information, behavioural modulation, manipulation and persuasive technologies

Personal data is also used to achieve unprecedented and pervasive strategies of behavioural modulation and manipulation through persuasive design and nudge techniques.²⁰ Children are strongly impacted by such strategies, shaping their habits, perceptions and decisions in different areas,²¹ ranging from

their routine use of technologies²² to serious political statements, consumer habits, religious beliefs and even interpersonal relations.

Those persuasive technologies can have serious impacts on children, creating anxiety, aggression, addiction, compulsion and device dependence as well as diminishing their creativity, autonomy, memory, sleep and education.²³ As a result, children miss the fundamental opportunities to connect with themselves, the physical and outside world and with others. This has a profound impact on their development, self-regulation (executive function), and their physical and mental health.²⁴

...it is important to highlight that children in different countries do not receive equal protection by the same tech companies

Automated decision-making with opaque algorithms and non-transparent nudge techniques based on personal data can lead to limited diversity experiences and developmental opportunities, creating echo chambers and self-referential bubbles, impacting especially children's access to information and different opportunities regarding many spheres, including education, professionalization and enjoyment of culture.

2.5 Discrimination: unequal treatment and protection

Personal data is often used for automated decision-making based on opaque and biased algorithms and non-transparent variables, often resulting in so-called "digital racism" and "digital steering", made possible by website design, user interface, gender and racial profile creation, biometrics data collection²⁵ and filtering and searching mechanisms. These outcomes affect how children interact and are perceived online, especially children of African descent and from minority and indigenous communities.²⁶ Often, automated decision-making in online services discriminates against characteristics such as gender, age, ability, language, ethnicity and socioeconomic status, creating obstacles for the enjoyment of digital opportunities by all children.

In addition, it is important to highlight that children in different countries do not receive equal protection by the same tech companies. Often, children and families from the Global South are not granted access rapidly to new and safer technologies or corporate pledges and policies available to children in European or North American countries: YouTube Kids, a Google platform with more marketing restrictions, was launched in the United States in February 2015,²⁷ but in Brazil over a year later – in June 2016.²⁸ Accessibility to terms of use and privacy is also a key problem. For instance, although its use greatly increased during the COVID-19 pandemic, the privacy notice of Google's G Suite education platform is only available in English in Brazilian schools.²⁹ In addition, all the platform's explanatory videos were in English,³⁰ rendering it inaccessible to most users.

Legal duties of private companies under the CRC: with great power comes great responsibility

The UN Convention on the Rights of the Child, in an extremely innovative text for a treaty under public international law, foresees explicitly the protection of children's rights also by private actors,³¹ including business enterprises that directly or indirectly by action or omission impact children and their rights with their products, services or actions in their communities.³²

Article 3, paragraph 1 provides that: "In all actions concerning children, whether carried out by public or private welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." As stated in the Committee's General Comment n. 16, this provision "is also directly applicable to business enterprises that function as private or public social welfare bodies by providing any form of direct services for children, including care, foster care, health, education and the administration of detention facilities."³³

Considering that the internet, its platforms and applications perform a large role and are a powerful element in everyone's daily lives, access to it (or the freedom to connect) was recognized by the UN as a "key means"³⁴ to exercise human rights, and internet access disruption was condemned as a human rights violation.³⁵ Consequently there is no doubt that the internet is a key direct welfare service for children, enabling them to express and fulfil their own human rights.

Therefore, it is understood that the Convention itself can be invoked to ensure that business enterprises in the digital environment undertake children's rights due diligence and do not contribute to their violation. Tech companies with legally constituted offices in countries that have ratified the Convention are bound directly by the text of the Convention itself, requiring them to primarily consider the best interests of the child in all their practices, products and services used by children. Thus, the duties regarding children's rights and their best interests must be a primary legal concern not just for families and the State, but also for businesses.³⁶

The children's rights-by-design (CRbD) standard for data use by companies: CRC for all

Realizing that companies in the digital environment must respect, protect, promote and fulfil the rights of children and their best interests, it is important that the rights involved in data use are clarified and translated into specific provisions for the design and development of products and services: a CRbD standard for data use by tech companies.

4.1 The Convention on the Rights of the Child (CRC) framework

The CRC provides fundamental principles and rights that should be applied systematically both to promote children's rights and development, and to protect them from violations regarding the detrimental use of their data.

Therefore, in all use of children's data in the digital environment, their **best interests shall be a primary consideration** (art. 3.1), guiding all actions taken by internet companies and data holders, even in cases where the processing of children's data has an established legal basis such as consent, performance of a contract, legal obligation, vital interests, public task or any other legitimate purpose. Further, in the design and development of any service or product, the **evolving capacities of the child**³⁷ should be recognized (art. 5), **allowing them to be heard** in the process (art. 12.2). As they are more vulnerable individuals than adults, children's data should always be treated as sensitive personal data, including those related to genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions, and personal data that reveal racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life.

Children's data should never be used to discriminate negatively, impacting their well-being, access to information, digital opportunities and contributing to the perpetuation of models based on bias and digital racism. The best and most advanced technologies and policies for children's data protection must be universally adopted by the same company in all countries with users, for all children, **without any form of discrimination** (art. 2).

Children have **the right to privacy and family life** in the digital environment, including the protection of their personal data (art. 16). Measures to guarantee the confidentiality of their correspondence and private communications and full ownership of their data and right to erase it at any time, are essential.

Children have **the right to be safe and protected from all forms of physical or mental violence**, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse while in the digital environment of companies, their products and services (art. 19.1), including in massive processing, exposure and easy transit of children's personal data and persistent identifiers which may expose or lead to evidence of sexual abuse, for example.

Children **have the right to be protected from any kind of economic exploitation** (art. 32.1 and art. 19.1), including digital commercial exploitation through the monetization of personal data by profiling and automated decision-making, micro-targeting of advertising, selling of data, and by the exploitation of children's images and artistic data.³⁸

Children's right to **freedom of expression** also regards the processing of their data (art. 13.1). This includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, while preventing the use of their data in automated decision-making with opaque algorithms, creating echo chambers and self-referential information bubbles. Moreover, they have **the right to freedom of thought** (art. 14), which prevents the use of non-transparent nudge techniques and persuasive technologies for behavioural modulation and manipulation.

Children have the right to privacy and family life in the digital environment, including the protection of their personal data

Children have also **the right to development** (art. 6.2), **health** (art. 24), **education** (art. 28), **to rest – even through disconnecting from the digital world – leisure and play** (art. 31) These provisions ensure that the use of children’s data by companies in the digital environment favours a harmonious, healthy and integral physical, mental, spiritual, moral and social development.

- **Integrate the CRC provisions into all appropriate corporate policies and management processes:** the consideration of children’s rights and best interests should be a primary requirement for the company, integrating due diligence in this regard into the company culture, management and goals, including in the design and development of products and services.⁴²

Children should have online tools to easily access, ratify, erase, restrict or object to processing their data

Any business model that is based on the economic and non-transparent exploitation of children’s data must be replaced by educational designs and architecture of cyberspaces, with transparent nudges for the exercise of citizenship and the **free expression of children’s freedoms, rights and identities** (art. 8), giving children **access to information from a diversity of sources** (art. 17). Children have the right to be part of their online community, **assembling with other children** (art. 15) in a digital environment that is safe, private and free from commercial pressures.

4.2 Specific measures for designers and developers

In order to translate the CRC principles and rights into practice for the protective governance of children’s data by a company, it is important to define specific measures for designers and developers, detailing the CRbD standard for data use. Recent initiatives have explored these measures, such as the UNICEF/ITU Guidelines for Industry on Child Online Protection 2020,³⁹ the Designing for Children Guide⁴⁰ and the UK Age Appropriate Design Code.⁴¹

In order to better organize these recommendations, they are grouped into three categories: (i) company governance; (ii) product or service development; (iii) product or service provision. It should be noted that the measures presented below must always be constantly adapted to ensure protection due to rapid and sometimes disruptive technological development.

(i) **Company governance**

Business administrators and managers have a duty in the governance of their companies to incorporate the CRC and its framework for children’s rights as an inter-sectoral internal policy:

- **Adopt an interdisciplinary perspective to achieve the best interests of the child:** in the design and development of products or services that directly or indirectly impact children, not only the opinion of users (children and families) should be incorporated, but also the perspectives of specialists, such as psychologists, neuroscientists, health-care specialists, educators, and children’s rights experts. This allows a more comprehensive look at the impact of these tools on all dimensions of the child, their development and their rights according to the CRC.
- **Universal adoption of the best technologies and policies available:** to avoid discrimination, companies should adopt the best policies and technologies available for children’s rights and best interests protection in all jurisdictions where their products and services are available.
- **Due diligence of policies and community standards:** companies should enforce and be accountable for their own published terms, policies and community standards, especially regarding privacy policies and age verification and restriction.

(ii) **Product or service development**

Those responsible for researching, developing and approving any product or service in a company must observe the CRC by:

- **Data minimization:** all children’s data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed. Only the minimum amount of personal data that is needed for the purposes of the service should be collected and stored and only for the minimum amount of time possible. Different options should be available for the service related to the data provided.
- **Children’s full control of their data:** children should have online tools to easily access, ratify, erase, restrict or object to processing their data.

- **Commercial-free digital spaces:** products and services for children should be free from commercial pressures and profiling or consumer nudge techniques based on personal data, especially from thinly veiled marketing strategies, like untransparent influencer marketing and product placement. Children under 16 years old should not be targeted with advertising in the digital environment, thus preventing the development of marketing practices directed at them.
- **Promotion of meaningful and non-monetizable experiences:** the design of the service or product should promote autonomous, playful and educational experiences, preventing the monetization of children's experiences such as unauthorized artistic child labour. Considering that monetization is possible due to the design and business model of the online products themselves, child influencers should be closely monitored by companies to avoid economic exploitation and to ensure the child's protection.

...companies have
a duty to prevent
and combat known
or new child sexual
abuse material

- **Nudge techniques in the best interest of the child:** all nudge techniques should be transparent and ethical, promoting children's development, their best interests and digital citizenship. They should not be used to undermine children's freedoms and rights.
- **Safety standards:** companies should seek to safeguard against the improper exposure of children's data and persistent identifiers that facilitate non-authorized and malicious contact. Moreover, companies have a duty to prevent and combat known or new child sexual abuse material from being made available to users or accessible on their platforms and services; target online grooming and predatory behaviour; and ensure that livestreaming and search mechanisms will not expose child sexual exploitation and abuse material and data.⁴³ It is important to have in place processes to immediately remove or block access to child sexual abuse data, and to ensure that relevant third parties with whom the company has a contractual relationship have similarly robust notice and takedown processes.⁴⁴
- **Default settings:** settings must be high-privacy, commercial-free and profiling and geolocation must be inactive by default. In all products and

services used by children it is important to: limit biometrics collection, geolocation and the online hyper exposure of children's data; prevent the economic exploitation of children's vulnerability for marketing purposes; and to restrict profiling that could lead to behaviour modulation or discrimination.

- **Parental controls and mediation:** online tools to facilitate parental controls and mediation are important. However, children should have age appropriate and transparent information about how this works and how it affects their privacy. Design solutions could encourage parents and children to talk frequently about their experience online.

- **The right to use, play and participate without data collection:** data processing shouldn't be the only way children can use, play and participate in the digital environment. It is important to have options that are free from data processing, allowing all children to be part of their online community.

- **The right to disconnect:** outdoor and nature experiences and face-to-face interpersonal relationships are essential for children's development, making it urgent that offline experiences are considered and practiced as one of the strategies that companies should take into consideration in design. Time restriction mechanisms should be promoted for families and caregivers and design strategies (like persuasive design) that encourage constant use of tech products and services should be discouraged.

(iii) Product and service provision

Once the product or service is launched, the company must ensure that its actual functioning is in accordance the CRC and its framework:

- **Children's data protection impact assessments (CDPIA):** the CDPIA is an important process to identify and minimize risks to children in digital products or services that are likely to be accessed by children.⁴⁵ This involves the description of the data processing; consultation with children and parents; assessment of the necessity, proportionality and compliance of the data processing; identification and assessment

of risks;⁴⁶ and the identification of measures to eliminate or mitigate the risks.

- **Detrimental use of data:** processing children's data should always be in their best interests, preventing any use shown to be detrimental to their well-being, such as persuasive design to extend engagement, marketing and behavioural advertising.

Processing children's data should always be in their best interests

- **Age appropriate:** the indication of an age for the use of a particular service or platform is an important tool for parental mediation and to adapt the usability of a product or service to a specific age range and developmental stage. However, it cannot serve as a validation for the detrimental use of data, and should always be considered as a protective feature, respecting the best interests and rights of the child as user.
- **Transparency, accessibility and legibility:** the mechanisms of data processing must be transparent and the terms of use and privacy of all products and services used by children must provide all the information regarding the use of data in a simple, clear and accessible manner, suitable for understanding by different children and families. Translation into different languages and accessibility, via other audio-visual resources, for people with disabilities must be available when appropriate. Privacy tools, settings and remedies should be accessible, meaningful and child-friendly, thus creating learning opportunities. Constant access to privacy tools should be available during use.
- **No data sharing:** children's data are sensitive and should not be disclosed to third parties, unless a compelling reason is given, such as the child's safety and best interests.

4.3 International monitoring and governance of tech companies' practices: protection without borders

Big tech companies have gained immense power in organizing life in today's society, even greater than

that of some State institutions. Their services are transnational and as the internet clearly transcends physical borders, an effective model of children's data governance should incorporate human rights international mechanisms to monitor business practices.

Good and important efforts have already been made by the UN system to strengthen the business sector's commitment to human rights and, especially, children's rights, such as the Children's Rights and Business Principles.⁴⁷ However, it is necessary to go further by recognizing that under the Convention companies already have duties and monitoring and reporting mechanisms to the Committee on the Rights of the Child should apply also to them.

As demonstrated above, states should not be the only actors urged to address corporate duties and monitoring the implementation of the CRC through the existing international institutional mechanisms should also extend to global tech companies. For example, tech companies could be subject to the same procedures as member states and directly receive communications from the Committee to contribute voluntarily to State's reports, Universal Periodic Reviews and Special Procedures on topics that regard implementation of CRbD standards in their services and products. In this way, companies could also be subject to complaints and enquiry procedures and general comments/recommendations from the Committee.

...tech companies have a duty ... to respect, protect, promote and fulfill the rights of children and their best interests in all decisions related to data governance

It is also important to note that, although the United States is one of only three countries that have not yet ratified the Convention, large US technology companies have offices in other countries, thus binding them to the provisions of the Convention itself and enabling the Committee to address them directly.

Conclusion

The digital environment is an important, though complex and dynamic, space for the socialization of children. Their protection and safety in cyberspaces cannot be the responsibility of parents and caregivers alone and nor can this be achieved simply through media literacy and with responsible and self-aware users.

The design of services and products matters. It forms the architecture in which children will be able or not to express their potentialities, identities and rights. It is the means by which children will find a safe and caring environment, or will experience the permanence of a business model with numerous violations of their rights through practices that permit privacy and safety violations, economic exploitation, freedom violations and discrimination.

Therefore, tech companies have a duty under the CRC to respect, protect, promote and fulfill the rights of children and their best interests in all decisions related to data governance in their services or products. The adoption of a CRbD standard for data use is more than an essential self-regulatory practice; it is engrained in the CRC international legal provisions, even making it possible for companies to participate in the mechanisms for monitoring the implementation of the CRC by the UN Committee on the Rights of the Child.

The effective implementation of a CRbD standard for data use by tech companies is an imperative step towards fair, just and reasonable governance of children's data and the full protection and promotion of their rights.

This paper was developed by members of the Working Group on Good Governance of Children's Data. Learn more about the project ►

Good Governance of Children's Data project

The Office of Global Insight and Policy is bringing together 17 global experts in a project to explore trends in the governance of children's data, including the tensions between different rules and norms, emerging concepts and practice, and implications for policy and regulation. Debate on the future of children's data affects a diverse range of issues, including data ownership and control, data fiduciaries, profiling for digital marketing purposes, child-friendly privacy notices, data erasure upon request, age verification, parental responsibility, data protection by design and default, algorithmic bias, and individual and group data.

The project aims to highlight the gap between the world we want for children and today's reality, developing a manifesto on how children's data could be optimally managed and what steps need to be taken. To help develop this manifesto, members of the working group will publish short analyses of different approaches to data governance.

Endnotes

- 1 Lawyer and researcher on Children's Rights and Coordinator of the Child and Consumerism Program at Alana Institute/Brazil, focused on children's digital rights. Pedro Hartung is a professor at Fundação Getulio Vargas-SP in Advocacy and Social Transformation; he holds a PhD in Public Law from the University of São Paulo and was a visiting Researcher at Harvard Law School and at the Child Advocacy Program at the same institution. He was also a visiting Researcher at the Max-Planck-Institute of Public Law in Heidelberg/Germany and the former counselor at Conanda - National Council for the Rights of Children and Adolescents in Brazil and coordinating professor at the Luiz Gama Human Rights Clinic at the University of São Paulo Law School.
- 2 van der Hof, S. and Lievens, E (2018). The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR. *Communications Law* Vol. 23, No. 1, p. 22. Available at SSRN: <https://ssrn.com/abstract=3107660>.
- 3 See more at: https://edu.google.com/latest-news/future-of-the-classroom/digital-responsibility/?modal_active=none.
- 4 A/HRC/28/39, Summary of the Human Rights Council panel discussion on the right to privacy in the digital age.
- 5 Vivrekar, D. (2018). Persuasive Design Techniques in the Attention Economy: User Awareness, Theory, and Ethics. Master thesis at Stanford University. June 6, 2018. Available at: https://stacks.stanford.edu/file/druid:rq188wb9000/Masters_Thesis_Devangi_Vivrekar_2018.pdfhttps://stacks.stanford.edu/file/druid:rq188wb9000/Masters_Thesis_Devangi_Vivrekar_2018.pdf
- 6 A/RES/69/166, 69/166. The Right to Privacy in the Digital Age. Resolution adopted by the General Assembly on 18 December 2014. Available at: <https://undocs.org/en/A/RES/69/166>
- 7 UNICEF (2017). Children in a Digital World, The State of the World's Children 2017, p.1. Available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf
- 8 Montgomery, K.C., Chester, J. and Milosevic., T. (2017). Children's Privacy in the Big Data Era: Research Opportunities, *Pediatrics*, 140 (Supplement 2) S117-S121. Available at: https://pediatrics.aappublications.org/content/140/Supplement_2/S117.
- 9 End Violence Against Children, Safe Online website: <https://www.end-violence.org/safe-online>.
- 10 WePROTECT Global Alliance. (2019). Global Threat Assessment 2019: Working Together to End the Sexual Exploitation of Children Online, p. 40. Available at: <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-Global+Threat+Assessment.pdf>.
- 11 See Lievens, E. et al (2019). The Child Right to Protection against Economic Exploitation in the Digital World. Submission to the Committee on the Rights of the Child in View of Their Intention to Draft a General Comment on Children's Rights in Relation to the Digital Environment (May 2019), pp. 1-2. Available at: <https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/OtherStakeholders/EvaLievensSimonevanderHofetal.pdf>; Radesky, J., Reid Chassiakos, Y., Ameenuddin, N., Navsaria, D. (2020). Digital Advertising to Children, Council on Communication and Media, *Pediatrics* June 2020, e20201681. Available at: <https://pediatrics.aappublications.org/content/early/2020/06/18/peds.2020-1681/tab-article-info>; UNICEF (2018). Children and Digital Marketing: Rights, Risks and Responsibilities - Discussion Paper. Available at: https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities.pdf; Araújo, C.S., Magno G., Meira, W., Almeida, V., Hartung, P. and Doneda, D. (2017). Characterizing Videos: Audience and Advertising in Youtube Channels for Kids. In: Ciampaglia, G., Mashhadi, A., Yasserli, T. (eds) (2017). *Social Informatics. 2017. Lecture Notes in Computer Science*, vol 10539. Springer.
- 12 International Labour Organization (1973). Minimum Age Convention, Article 8.1. Available at: https://www.ilo.org/dyn/normlex/en/f?p=NORML+EXPUB:12100:0::NO::P12100_ILO_CODE:C138
- 13 European Commission (2016). Study on the impact of Marketing through Social Media, Online Games and Mobile Applications on Children's Behaviour. Available at: https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en.
- 14 Report by Professor Yves de la Taille on PL 5921/2001 developed by request of the Federal Psychology Council, 'Advertising Aimed at Children: Psychological Considerations'. Available at: https://site.cfp.org.br/wp-content/uploads/2008/10/cartilha_publicidade_infantil.pdf.

- 15 See for example, research published by the Ministry of Justice of Brazil and carried out by Federal University of Ceará – GRIM – Research Group on the Relations between Childhood, Youth and Media. Available at: https://www.defesadoconsumidor.gov.br/images/manuais/publicidade_infantil.pdf; WHO (2010). Set of recommendations on the marketing of foods and non-alcoholic beverages to children. Geneva, World Health Organization. Available at: <http://www.who.int/dietphysicalactivity/publications/recsmarketing/en/>; World Health Assembly Resolution WHA63.14 (n.d.). Marketing of Food and Non-alcoholic Beverages to Children; Grover, A. (2014). Report of the Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health. Available at: <https://undocs.org/A/HRC/26/31>; UNICEF (2014). Children’s Rights and Business Principles. Available at: https://www.unicef.org/csr/css/Workbook_2.0_Second_Edition_29092014_LR.pdf. Shaheed, F. (2014). Report of the Special Rapporteur in the Field of Cultural Rights. Available at: <https://undocs.org/A/69/286>.
- 16 The Economist Intelligence Unit (2017). The Impacts of Banning Advertising Directed at Children in Brazil. Available at: http://criancaeconsumo.org.br/wp-content/uploads/2014/02/TheEconomist_EN.pdf.
- 17 See more at: <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>.
- 18 See more at: <https://youtube.googleblog.com/2019/09/an-update-on-kids.html>.
- 19 Radesky, J., Reid Chassiakos, Y., Ameenuddin, N., Navsaria, D. (2020). Digital Advertising to Children, Council on Communication and Media, *Pediatrics* June 2020, e20201681. Available at: <https://pediatrics.aappublications.org/content/early/2020/06/18/peds.2020-1681/tab-article-info>
- 20 Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, pp. 375-376.
- 21 Kidron, B., Evans, A. and Afia, J. (2018). *Disrupted Childhood: The Cost of Persuasive Design*, London: 5Rights. Available at: <https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf>.
- 22 Ibid. pp. 20-26.
- 23 Ibid. pp. 30.
- 24 Yogman, M., Garner, A., Hutchinson, J. et al (2018). The Power of Play: A Pediatric Role in Enhancing Development in Young Children, *Pediatrics*. 142(3): e20182058.
- 25 Pugliese, J. (2012). *Biometrics: Bodies, Technologies, Biopolitics*, Routledge, p. 95; Magnet, S.A. (2011). *When Biometrics Fail. Gender, Race, and the Technology of Identity*, Durham, London: Duke University Press, p. 41.
- 26 Bedi, S. (2019). *Private Racism*, Cambridge University Press, pp. 82-112. Available at: <https://www.cambridge.org/core/books/private-racism/digital-racism/B5CE20ED1BF1C4D04F59F956C84BD781>.
- 27 The Guardian, YouTube Kids app launches in the US for Android and iOS, 23.3.2015. Available at: <https://www.theguardian.com/technology/2015/feb/23/youtube-kids-app-android-us-only>.
- 28 Caputo, V. (2016). Google lança YouTube Kids, app para crianças, no Brasil. Available at: <https://exame.com/tecnologia/google-lanca-youtube-kids-para-criancas-no-brasil/>.
- 29 Accessed on 6.7.2020 at: https://gsuite.google.com/intl/pt-BR/terms/education_privacy.html
- 30 Accessed on 6.7.2020 at: https://edu.google.com/intl/pt-BR/why-google/privacy-security/?modal_active=none
- 31 Legal theories have explored the concept of the horizontal effect of human rights in private relations (Third Party Effect, *Drittwirkung*), highlighting the possibility of direct or indirect legal binding of private agents to human and fundamental rights norms. See: Drzemczewski, A. (1979). The European Human Rights Convention and Relations between Private Parties, *Netherlands International Law Review*, 26(2), 163-181.
- 32 Wapler, F. (2015). *Kinderrechte und Kindeswohl*, Tübingen: Mohr Siebeck, pp. 243-244.
- 33 UN/CRC/C/GC/16. General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children’s rights, item 16, p. 6. Available at: <https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf>.
- 34 La Rue, F. (2011). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/17/27, item. 20, p. 7.
- 35 Human Rights Council (2016). The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/32/L.20, 27 June 2016, p. 3. Available at: <https://www.refworld.org/docid/57e916464.html>
- 36 See UNICEF (2014). Children Are Everyone’s Business, Workbook 2.0. Available at: <https://www.unicef.org/csr/88.htm>.
- 37 According to General Comment No. 20, para. 18, “the Committee defines evolving capacities as an enabling principle that addresses the process of maturation and learning through which children progressively acquire competencies, understanding and increasing levels of agency to take responsibility and exercise their rights.”
- 38 International Labour Organization (1973). Minimum Age Convention, Article 8.1. Available at: https://www.ilo.org/dyn/normlex/en/f?p=NORML_EXPUB:12100:0::NO::P12100_ILO_CODE:C138
- 39 International Telecommunication Union Development sector (2020). Guidelines for Industry on Child Online Protection. Available at: https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_967b2ded811f48c6b57c7c5f68e58a02.pdf
- 40 DC4R (2018). Designing for Children’s Rights Guide: Integrating Children’s Rights and Ethics into the Design Process. Available at: <https://childrensdesignguide.org/#principles>.
- 41 Information Commissioner’s Office (2020). Age Appropriate Design: A Code of Practice for Online Services. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.

- 42 See: UNICEF/ITU (2015). Guidelines for Industry on Child Online Protection, p. 12. Available at: <https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf>.
- 43 See: WeProtect (n.d.). Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. Available at: <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5e6123f79f9a545c228c7d1b/1583424503764/11+Voluntary+principles+-+formal+letter.pdf>
- 44 See: UNICEF/ITU (2015). Guidelines for Industry on Child Online Protection, p. 12. Available at: <https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf>.
- 45 The dData protection impact assessment (DPIA) proposed in the United Kingdom age-appropriate design is an excellent guide and can be helpful to other jurisdictions. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/>.
- 46 Such as, “physical harm; online grooming or other sexual exploitation; social anxiety, self-esteem issues, bullying or peer pressure; access to harmful or inappropriate content; misinformation or undue restriction on information; encouraging excessive risk-taking or unhealthy behavior; undermining parental authority or responsibility; loss of autonomy or rights (including control over data); compulsive use or attention deficit disorders; excessive screen time; interrupted or inadequate sleep patterns; economic exploitation or unfair commercial pressure; or any other significant economic, social or developmental disadvantage.” In: Age-appropriate Design: A Code of Practice for Online Services, 2. Data Protection Impact Assessments. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/>
- 47 See: <https://www.unicef.org/csr/88.htm>.

UNICEF works in the world’s toughest places to reach the most disadvantaged children and adolescents — and to protect the rights of every child, everywhere. Across 190 countries and territories, we do whatever it takes to help children survive, thrive and fulfill their potential, from early childhood through adolescence. And we never give up.

The Office of Global Insight and Policy serves as UNICEF’s internal think-tank, investigating issues with implications for children, equipping the organization to more effectively shape the global discourse, and preparing it for the future by scanning the horizon for frontier issues and ways of working. With dedicated expertise in seven policy areas — digital technology, human capital, governance, the environment, society, markets, and finance — the Global Insight team assists the organization in interpreting, and engaging in, a rapidly changing world.

Office of Global Insight and Policy
United Nations Children’s Fund
3 United Nations Plaza, New York, NY, 10017, USA

© United Nations Children’s Fund (UNICEF), November 2020

The author would like to thank Isabella Henriques, Marina Meira, Jasmina Byrne, Linda Raftree and Emma Day for their review of and input on this paper.

This is a working document. It has been prepared to facilitate the exchange of knowledge and to stimulate discussion. The text has not been edited to official publication standards and UNICEF accepts no responsibility for errors. The statements in this publication are the views of the author(s) and do not necessarily reflect the policies or the views of UNICEF. The designations in this publication do not imply an opinion on legal status of any country or territory, or of its authorities, or the delimitation of frontiers.



This document is interactive and designed for digital viewing.



Please consider the environment and refrain from printing.