Contribution of Asociación por los Derechos Civiles to the Draft General Comment on children's rights in relation to the digital environment

This contribution is a submitted by Asociación por los Derechos Civiles (ADC) a civil society organization based in Buenos Aires, Argentina. ADC endorses and defends people's fundamental rights, advocates for the strengthening of democracy and seeks for an inclusive society. Most of our work is focused on the relationship between digital technologies and fundamental rights. ADC wishes to provide the following comments to the draft for the upcoming General Comment on the rights of the child in relation to the digital environment.

III. General Principles:

- ### A. The right to non-discrimination (art.2):

The paragraph should explicitly mention facial recognition technologies as a source of potential acts of discrimination for which children may not be aware of. The increasing use of facial recognition technologies is particularly troubling for children's right to non-discrimination due to the following reasons. First, studies show a high rate of false positives when these technologies are applied to children[1]. This situation may get worse when children are from minority groups, because facial recognition systems make more errors when deployed on people of color, asians or indigenous communities. Secondly, facial recognition technologies have been used to detect students suspended from school[2] or to control attendance[3]. In some of these cases, fines were imposed because this technology violated the data protection legal

[1] NIST Interagency/Internal Report (NISTIR) - 8280, available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[2] Human Rights Watch. *Facial Recognition Technology in US Schools Threatens Rights,* available at https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights

[3] AccessNow, *In the EU, facial recognition in schools gets an F in data protection,* available at https://www.accessnow.org/in-the-eu-facial-recognition-in-schools-gets-an-f-in-data-protection/

framework[4]. Finally, facial recognition technologies can be used for public safety purposes, resulting in violations to the presumption of innocence and deprivation of liberty, due to false positives that wrongly identify children as criminals.. For these reasons, it is necessary that the General Comment recognizes the discriminatory effect of facial recognition technologies and recommends specific actions to States to prevent their application on children.

- D. The right to be heard (art.12):

Digital technologies can promote children's engagement by discussing issues of their concern. However, if States do not take their contributions seriously, it is likely that children's participation will decline over time. Therefore, in addition to recommending children's participation, the paragraph should recommend States to take into account children's opinions and incorporate them into the policies that are ultimately approved. If these opinions are not considered, States should provide clear explanations of the reasons behind their decision.
Moreover, the paragraph should affirm that the right to be heard is an essential part of the “best interests of the child” principle and that its dynamic content must be analysed in every specific case with particular attention to the child's opinion.

IV. Evolving capacities (art. 5)

This section should stress the relevance of children and adolescents’ education for a beneficial use of technologies, so that children have the tools to interact in the digital environment safely and according to their progressive capacity. Children’s development must be accompanied by their parents and caregivers who must also be

[4] European Data Protection Board. *Facial recognition in school renders Sweden’s first GDPR fine,* available at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_es

trained for this purpose. It's important to focus on quality screen time (i.e. what activities and purposes are pursued), rather than the total time spent as the sole indicator.

V. General measures of implementation by States (art.4):

- ### C. Coordination:

It is not enough to designate a government body if it does not have the necessary staff and budget to carry out its activities. The likelihood of fulfilling obligations will depend, among other things, on States providing adequate funding and staffing to coordinate the programs and policies to be implemented. Therefore, the paragraph should include that the government body must have enough human and financial resources to perform its functions satisfactorily. It is also important that this government body coordinates its work with bodies from other jurisdictions -something particularly important in federal countries- so that actions are applied equally to all children.

- ### D. Data collection and research:

Research is essential to know more about the implications of digital technologies for children. But if conducted without strong safeguards to protect personal information, it may affect children's privacy. Research must use aggregate, de-identified and anonymous data and avoid identifying children whenever possible.
Therefore, to avoid harming their privacy, the paragraph should add that research that will be in the public domain must guarantee the anonymity and preservation of the identity of the child, in case its publication could cause harm to the child.

VI. Civil rights and freedoms

- ### B. Freedom of expression (art.13):

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has highlighted that in environments of prevalent censorship,

individuals may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information[5]. In the case of children, it's particularly important to create a safe space where their communications can be shielded from external interference. Children may suffer cyber bullying or online public shaming for things they post on the internet. Thus, anonymity can reduce the possibility of those actions to happen by not identifying a child' real name with online comments. Also, anonymity is a useful tool for children to be honest and open about their problems or to denounce abuses and other kinds of illegal actions. In addition, encryption is a vital element to secure children's messages and their sensitive data. Therefore, to enhance the efforts to protect children from reprisals for their views, the paragraph should add that States should promote anonymity and encryption and refrain from implementing policies that undermine them.

- D. Freedom of association and peaceful assembly (art.15)

Online civic space is facing many challenges due to the increasing use of technology by state actors to monitor the Internet. This is particularly troublesome in this new context where the pandemic has led the government to discourage people from gathering in the streets, parks and other public places. In this scenario, the internet has become even more important for freedom of association and peaceful assembly. In the case of children, we must seriously consider the chilling effects of surveillance. Given that children may be more prone to be intimidated than adults, techniques like social media intelligence (SOCMINT) and open source intelligence (OSINT) may greatly affect children's ability to associate with their peers and engage in online activism. Therefore, the Commentary should mention that States must refrain from general monitoring of children's social networks or engaging in other mass surveillance actions targeting them.

- F. Birth registration and right to identity (arts.7 and 8):

[5] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. *Encryption and Anonymity follow-up report,* June 2018, available at https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

While digital birth registration systems may enhance children rights to identity, we must not overlook the serious risks of exclusion and discrimination that emerge from this kind of technology. For instance, a system with a binary conception of identity (male/female) may not be respectful of children that perceive themselves outside those traditional categories.

The paragraph does assert that such systems should not hinder children's privacy and identity. However, it doesn't recommend particular measures to accomplish that goal. Thus, it would be convenient to elaborate further by establishing additional guidelines. For instance, the need for every identity system to have a clearly stated purpose, with its proportionality and necessity backed by clear and publicly-available evidence. Moreover, the paragraph should emphasize that the use of biometric data poses several risks and mitigation measures must be taken accordingly. As stated above (see A. The right to non-discrimination) the lack of accuracy in technologies using children'' biometric data should be a reason to disencourage the use of these systems. Finally, there should be an inclusive democratic process prior to deploying such systems, whereby civil society and technology experts may have a meaningful voice in their design and implementation[6].

X. Basic health and welfare (art.24):

The section rightly describes different ways digital technology may enhance children's health and well-bieng. However, it doesn't make any reference to the sensitivity of their health data. Children must be assured their medical record and other health information is accurate, updated and protected from breaches, attacks or undue disclosures. Also, organizations that process children's health data should carry out privacy impact assessments to evaluate the necessity and proportionality of the processing and implement security measures on access control and management of all the information processed in the context of health data.

[6] Privacy International. *Consultation response for ID4D on the Principles on Identification for Sustainable Development: Toward the Digital Age,* available at https://privacyinternational.org/sites/default/files/2020-04/Consultation%20response%20for%20ID4D%20on%20the%20Principles%20on%20Identification%20for%20Sustainable%20Development.pdf

XI. Education, leisure and cultural activities

- ### A. The right to education (art. 28, 29):

The paragraph should recommend states to guarantee that technologies to be used for education must comply with suitable security and privacy standards. That would include encryption and data protection by-default-and-design, avoiding profiling, dark patterns or interference from opaque nudge techniques, and behavioural and emotional analytics[7]. In addition to this, the text should stress that deploying facial recognition technologies in schools -as stated in III.A- can violate the right to education in a safe and open environment, by creating a space where discrimination and disproportionate surveillance may hinder students dignity.

[7] Defend Digital Me. *An open letter to policy makers, data protection authorities, and providers worldwide, regarding rapid technology adoption for educational aims* https://defenddigitalme.org/wp-content/uploads/2020/04/Coalition-open-letter-to-global-edTech-sector-April-27-v5.pdf