Public Consultation on a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

Submission of Defence for Children – ECPAT the Netherlands

Defence for Children – ECPAT the Netherlands welcomes in principle the proposal and recognizes that the proposal can offer an important legal framework to protect children against sexual harm in relation to the online environment. According to the UN Committee on the Rights of the Child, States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment.[1] They should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, **the best interests of every child is a primary consideration.**[2] The proposed regulation guarantees that **all online service providers** take the best interest of the child in consideration and assess and mitigate risks for children in order to prevent sexual harm. In this way **safety-by-design** is promoted, which is also a requirement of the Committee.[3] We support that the **balancing of fundamental rights** needs to be carried out by judicial or independent administrative authorities, rather than by individual companies.

Because the proposed regulation affects many children's rights and the rights of all users of online services, we emphasize the obligation of a continuous process of **child rights impact assessment** to predict the impact of the proposed regulation on children and the enjoyment of their rights.[4] As (technological) developments within the digital environment happen fast, child rights impact evaluation should be structurally imbedded to evaluate the actual impact of implementation to ensure that all rights of all children that are affected are adequately protected. If, exceptionally, the solution chosen is not in the best interests of the child, the grounds for this must be set out in order to show that the child's best interests were a primary consideration despite the result.[5]

For the proposed regulation and procedures to be effective, conditions as **legal certainty** (clear definitions and substantive obligations) and **capacities of services** involved (victim support, law enforcement, judicial authorities, data protection authorities, child rights based procedures) need to be accounted for. However, limited capacity is never a reason for not implementing children's rights.

In a survey (2021) conducted by Defence for Children – ECPAT the Netherlands in partnership with ECPAT International, we asked over **9.000 citizens across 8 European countries** whether "the EU should implement a new law that makes it a legal requirement for online service providers (e.g. social media platforms) to use automated technology tools to detect and flag signs of online sexual exploitation and abuse (e.g. illegal photos or contact with children)". We explained that "these tools continuously check the personal activity of all users on the platform, looking for signs of online sexual exploitation and abuse." This representative research shows that a majority of **68% was in favour of legislation** that will keep children safe online and the use of technology to identify child sexual abuse and exploitation. With this proposal, the European Commission is responding to these calls.

We support that prevention measures should focus on **all forms of child sexual abuse and exploitation**. Besides, the proposed safeguards in the detection order process, including an evaluation of technology by a technical committee, National Coordination Authorities, EU-Centre, Data Protection Authority and the final weighing of fundamental rights by judicial authorities, should **prevent unsafe detection** being approved and implemented on a large scale.

On the issue of obligations of the proposal applying to **all technology** used in online exchanges (including encryption), the Committee on the Rights of the Child emphasises that State parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material when encryption is considered.[6] We find it positive that the principles of **legality, necessity and proportionality are weighed by judicial authorities**. The new regulation should

[1] CRC/C/GC/25 par 37
[2] CRC/C/GC/25 par 12
[3] CRC/C/GC/25 par 70
[4] CRC/C/GC/14 par 35
[5] CRC/C/GC/14 par 97
[6] CRC/C/GC/25 par 70

include strong safeguards, transparency, independent oversight and access to remedy, as well as the integration of privacy-by-design into digital products and services that affect children, regularly review of privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy.[7]

We emphasize that the regulation should **protect all children**, with special attention for groups of children that need extra care and protection, as required by the UN Convention on the Rights of the Child. In this sense, we highlight the necessary special attention for **minor suspects/offenders** that carried out non-consensual creation or sharing of sexualized text or images. For these children, there is a need for child-friendly preventive, safeguarding and restorative justice approaches in all Member States.[8] Furthermore, it should be ensured that **voluntary online sexual behaviour** between youngsters in the same peer group is excluded from prosecution in all Member States (through revision Directive 2011/93/EU) and that the EU-Centre filters this voluntary imagery before sending it to national authorities. Another group that needs special attention is the group of **LGBTQ+ children**, especially when sexual imagery is detected and shared with authorities in countries where sexual minorities are being stigmatized, discriminated or even criminally prosecuted. Finally, **child victims from outside the EU** that appear in detected online child sexual abuse materials in the EU should receive special attention.

We urge to include the **opinion of children** in the consideration, drafting, implementation and evaluation of the proposed regulation. Reflecting the views of the intended beneficiaries of the proposed regulation is their right. We also request a clear plan to avoid **detection gaps** that can occur between the ending of the temporary regulation and the entry into force of this newly proposed regulation and any detection gaps due to long detection order processes after the regulation enters into force. Finally, we advise to determine clear safeguards for the **misuse of technology**, including strict and safe access measures for databases and regularly external audits of all parties concerned (including online service providers).

Important children's rights that are affected by the proposal:
The regulation meets a number of children's rights of the UN Convention on the Rights of the Child, for example Article 19 (protection against violence), Article 34 (protection against sexual exploitation and abuse) and Article 35 (protection against the sale or traffic of children for any purpose). In addition, there are also a number of children's rights that impose requirements and/or need special attention in child rights impact assessments and evaluations of the regulation or when conducting any balancing of rights as part of the implementation of the regulation (amongst others):

- Article 2 – **non-discrimination**: Discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child.[9] Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes.[10] Also risks for discrimination and stereotyping when using artificial intelligence algorithms should be taken into account.

- Article 3 – **best interest of the child**: The best interest of the child is a principle that must be applied to decisions that affect children in the digital environment. When there are conflicting interests, the best interests of the child must be a primary consideration in all actions regarding the provision, regulation, design, management and use of the digital environment.[11]

- Article 6 – **right to life, survival and development**: State parties should take all appropriate measures to protect children from risks to their right to life, survival and development. In the digital environment, risks relating to content, contact, conduct and contract encompass, among other things, sexual content, sexual exploitation and abuse.[12]

- Article 12 – **child participation**: States parties should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with

[7] CRC/C/GC/25 par 70
[8] CRC/C/GC/25 par 81
[9] CRC/C/GC/25 par 10
[10] CRC/C/GC/25 par 73
[11] CRC/C/GC/25 par 12
[12] CRC/C/GC/25 par 14

children, applying appropriate safeguards, and give their views due consideration when developing products and services.[13] Children must be included in the consideration, development, monitoring and evaluation of this regulation. Children can be very clear about how they would like their digital world to embody their rights.

- Article 16 – **right to privacy**: It can be deduced from jurisprudence of international human rights bodies that the right to privacy contains at least five dimensions which relate to the autonomy and normative agency of individuals including children:[14]
    1. Physical and mental integrity: In this context physical integrity refers to the protection of children against sexual abuse and exploitation. Mental integrity as part of private life affects honour and good reputation, which is highly violated by the distribution of child sexual abuse materials.
    2. Decisional autonomy: This also refers to decisions about having (online) sexual relationships. Note that the age of sexual consent differs in Member States.
    3. Personal identity: Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should therefore require an approach integrating safety-by-design and privacy-by-design, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyberaggression, hate speech or sexual exploitation and abuse.[15]
    4. Information privacy:
        - This covers information produced by the child (for example through diaries, WhatsApp, TikTok, YouTube), as well as information about the child which has been produced by others (schools, medical professionals, law enforcement, courts, social workers, banks, sports clubs and telecom and social media companies).
        - Any processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in case of very young children, that of their parent or caregiver; nor should it take place without the right to object to surveillance, in commercial, educational and care settings, and consideration should always be given to the last privacy-intrusive means available to fulfil the desired purpose.[16]
        - It should be explained to what extent conversations and information shared will be kept confidential, so that the child can decide what information to share or not.
    5. Physical/spacial privacy: This also includes digital spaces where children spent time.

    .
- Article 17– **right of access to information**: States parties should provide children with child-sensitive and age-appropriate information in child-friendly language on their rights in the digital environment. They should facilitate educational programmes for children, parents and caregivers, the general public and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should be informed by research and consultations with children, parents and caregivers.[17]

- Article 39 – **appropriate care for victims of violence**: States parties should establish, coordinate and regularly monitor and evaluate frameworks for the referral of cases and the provision of effective support to children who are victims. Frameworks should include measures for the identification of, therapy and follow-up care for, and the social reintegration of, children who are victims. Training on the identification of children who are victims should be included in referral mechanisms, including for digital service providers.[18]

- Article 40 – **juvenile justice**: Child friendly legal procedures for minor suspects, offenders and victims need to be implemented in all Member States. There needs to be legal certainty that voluntary online

[13] CRC/C/GC/25 par 17
[14] Tobin, J. & Field, S.M. (2019). Art. 16 The Right to Protection of Privacy, Family, Home, Correspondence, Honour, and Reputation. In: Tobin, J. (Ed.) (2019). The UN Convention on the Rights of the Child: A Commentary. Oxford Public International Law.
[15] CRC/C/GC/25 par 77
[16] CRC/C/GC/25 par 75
[17] CRC/C/GC/25 par 32
[18] CRC/C/GC/25 par 45

sexual behaviour between youngsters in the same peer group is not criminalised in all Member States.

Defence for Children - ECPAT the Netherlands

Defence for Children – ECPAT the Netherlands (Defence for Children) is a Dutch NGO promoting and protecting children's rights in the Netherlands and abroad, through legal support and our legal defence centre, advocacy, lobby, research, training and international programmes with partner organizations. Defence for Children has special expertise in the areas of child protection, justice for children, sexual exploitation, violence and abuse of children, migration, and girls' rights. The basis of our work is the UN Convention on the Rights of the Child.

Defence for Children – ECPAT the Netherlands is one organisation, and member of two global networks: Defence for Children International and ECPAT International. Defence for Children International is an international grassroots non-governmental movement that has been promoting and protecting children's rights since 1979, and was involved in the drafting of the UN Convention on the Rights of the Child, as well as other UN instruments and initiatives, for example in the field of justice for children, violence against children and children deprived of liberty. ECPAT International is the world's largest influencing network fully dedicated to ending the sexual exploitation of children, with a membership of 122 civil society organisations in 104 countries.

www.defenceforchildren.nl
info@defenceforchildren.nl