The rights of children in the digital environment

Eurochild Position Paper

Eurochild
Putting children at the heart of Europe

January 2025

The rights of children in the digital environment

Eurochild position paper

Executive summary

This paper synthesises Eurochild's vision and recommendations for safeguarding children's rights in digital spaces. While digital environments offer educational and social benefits key for the development of children, they also pose significant risks like cyberbullying, abuse and exploitation, negative mental health outcomes, among others. The paper calls for a nuanced approach based on the prevention and protection from harm with the empowerment of children through the realisation of their rights online. A narrow focus limited to prevention and protection risks leaving out of the conversation considerations on the right to participation, privacy, information, freedom of expression. A balanced, rights-based approach is key to ensuring children's right to participate in the digital environment while guaranteeing their best interests, privacy, safety and healthy development.

This requires that:

- Policy-makers adopt and enforce robust legal frameworks for the protection of children; and
- Companies design their digital services with child rights in mind, including listening to and respecting their views.

Setting the scene

This position paper aims to guide Eurochild's work on promoting and guaranteeing the rights of children in the digital environment. In the following sections, we will outline the holistic approach to protecting children's rights online (section I) and the three priority areas in which Eurochild will focus on in the upcoming years (section II): (i) promoting children's rights through safety- and privacy-by-design; (ii) the fight against child sexual abuse; and (iii) digital wellbeing. It has been compiled in consultation with Eurochild's members' digital task force and acknowledges the views of children expressed in the VOICE project.

The digital environment is becoming increasingly important across most aspects of children's lives. It affords new opportunities for the realisation of children's rights, but also poses significant risks. According to the latest research carried out by ECPAT International, Eurochild and Terre des Hommes ('VOICE research' from now on), children value the relational and entertainment opportunities of the internet, while remaining highly concerned about risks

such as cyberbullying and harassment, inappropriate content and contact and the misuse of their personal information by others[1].

The rights of children should be fully respected, protected and fulfilled, equally offline and online[2]. Therefore, it is essential to create digital environments that are not only safe, but also empower them to become full digital citizens. For this, it is essential that digital products and services respect and enable the full spectrum of children's rights, as defined in the UNCRC General Comment No. 25. The implications of the digital age for children's rights are manifold and ever changing. The General Comment sets out how to implement the four main principles of the UN Convention on the Rights of the Child (UNCRC) in the digital environment, namely: the right to non-discrimination, the best interests of the child, the right to life, survival and development and the right to be heard. It recognises the responsibility states have in putting the necessary means in place to ensure children can enjoy these rights also online, including legislating to ensure business responsibilities to respect, prevent, mitigate and, where appropriate, remedy abuses.

Meaningful access to digital technologies can support children to realize the full range of their civil, political, cultural, economic and social rights. Yet millions of children have no access to the digital environment at all, as 5.3% of school-aged children in Europe are digitally deprived[3]. Meaningful digital inclusion is a pathway to addressing existing (and new) inequalities, which otherwise are likely to increase. Quality of access is key to bridge digital and knowledge divides, which requires a multidimensional approach that includes speed, stability, affordability, language, training, capacity-building, local content and accessibility for children with disabilities. Many countries fail to ensure access to digital devices and internet connection to children in marginalized communities, as well as to digital literacy programs, significantly increasing the risk of online harm.

The digital environment must be safe for children and respect their full range of rights. One in three users of digital services is a child and the time children spend online daily has almost doubled since 2010. However, digital services and products are currently designed for and by adults leading to children's presence to largely go unrecognised and uncatered for on most of the digital platforms where children spend most of their time. Children are consequently exposed to a wide range of significant risks in the digital environment, relating to content, contact, conduct and contract[4], with detrimental effects on the exercise of their rights and their overall wellbeing and mental health. These include, among other things:

- Inappropriate content such as hate speech, violent or radical, including suicide and self-harm, and sexual material;

[1] Participatory research carried out with 500 children and 6,000 caregivers in 15 countries across the globe on their views on online child safety. ECPAT International, Eurochild and Terre des Homes Netherlands, Speaking up for change: Children's and caregivers' voices for safer online experiences, 2024.
[2] UN Convention on the Rights of the Child General Comment No. 25 on children's rights in the digital environment, 02 March 2021.
[3] Ayllón, S., Holmarsdottir, H.B. & Lado, S. (2021). Digitally deprived children in Europe. (DigiGen - working paper series No. 3). doi: 10.6084/m9.figshare.14339054
[4] Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children.

- Harmful contact and conduct, for example cyberbullying and harassment (including from peers), sexual abuse and economic exploitation;
- Harms derived from exploitative contractual arrangements, i.e., dark patterns, profiling and automated processing for user retention and information filtering.
- Cross-cutting harms that fit across various categories, such as those related to privacy, advanced technological features (i.e., AI), as well as health and wellbeing and cognitive, social and emotional development.

More problematic is the fact that research points towards a trend of normalisation of violence by children, while risks keep evolving and changing quickly. The VOICE Research shows that children understand online risks as part of the experience of being online, especially on social media, displaying **high tolerance to risk exposure online**. This acceptance of risk as inherent to their online activities might decrease the likelihood of self-protecting or even reporting, but not decrease the severity or reach of the harm itself. Moreover, research consistently shows that **children tend to not report** content identified as harmful or illegal[5]. Therefore a drastic change in moderation access and tools is required, to give children easy pathways to report harmful content and contact, and find human support if they feel at risk.

As the impact of online risks on children's rights varies, a tailored approach to protection measures is imperative. In fact**, children's rights in the digital environment are deeply interconnected**: safeguarding one right can significantly enable children to exercise other rights. For example, safeguarding children's privacy is a key step towards realising their freedom of expression in digital environments. Similarly, ensuring the safety of children online is often a precondition to ensuring children have agency to develop as digital citizens. These interlinks were very clearly raised by the VOICE research aforementioned, where children called for online measures that protect both their safety and their privacy:

"*We do not think that there is a debate between online safety and privacy. Both of them are important and should be protected*" - Child from Bulgaria

Acknowledging this interplay highlights the need for a balancing exercise of children's rights, in which the best interests of the child (art. 3, UNCRC) plays a key role[6]. Online service providers design algorithms that prioritise the commercial requirement for data or the overexposure to inappropriate content over their duty of care towards children[7]. This is because their business models rely on (i) the selling and sharing of use data to third parties (i.e., behavioral patterns, social characteristics of users, etc.), including that of children; (ii) targeted advertisement; and/or (iii) maximizing the engagement of users to ensure greater

[5] Ofcom, Children's attitudes to reporting content online, 2024.
[6] Livingstone, S., Cantwell, N., Özkul, D, Shekhawat, G., and Kidron, B. (2024). The best interests of the child in the digital environment. Digital Futures for Children centre, LSE and 5Rights Foundation.
[7] See e.g. 5Rights Foundation (2024) Disrupted Childhood: The cost of persuasive design.

What is a Child Rights Impact Assessment?

"A child rights impact assessment is a tool predicting the impact of any proposed law, policy or budgetary allocation, which affects children and the enjoyment of their rights. A child impact assessment needs to be built into government decisions at all levels and as early as possible in the development of policies and laws." (The EU Agency for Fundamental Rights)

visibility of their services and related advertisement. **Child rights impact assessments (CRIAs)**[8] pave the way for a better understanding of the best interests of the child, especially when balanced with other fundamental rights.

EU Member States have a duty to promote children's rights in the digital environment as laid down by the **UN Convention on the Rights of the Child** and **Article 24 of the EU Charter of Fundamental Rights**[9]. The EU has an important legislative role with regard to children's rights in the digital environment, as shown by the Better Internet for Kids Strategy (BIK+) and the EU Strategy for a more effective fight against child sexual abuse (CSA).

Section I. A multi-stakeholder approach to online child protection

Upholding children's rights online is a shared responsibility where policy-makers and online platforms must not only focus on ensuring children's safety but also on empowering them as users and digital citizens by ensuring the full spectrum of their rights. Beyond, ensuring holistic online child protection requires also the contribution of researchers, businesses who are part of the e-safety supply chain (i.e., content moderation vendors or age verification providers), adults supporting children (caregivers, educators, practitioners), civil society, including helplines and hotlines, and children themselves. For the purpose of this paper, we would like to highlight the need for a holistic and multifaceted approach consisting of prevention and protection from harm; child empowerment; and upholding the responsibilities of all stakeholders.

1. Prevent & protect

Prevention and proactive protective measures must go hand in hand in the digital environment. A classic and somewhat effective prevention effort has been raising the awareness of online risks —both by online platforms and through tailored education for children, parents, and educators— including comprehensive sexual and reproductive health education. Meaningful and effective online safety education mandates a tight collaboration between schools, national authorities and civil society. However, **awareness raising and digital literacy building** efforts have proven insufficient in absence of strong legal frameworks that mandate online service providers to provide safe and age appropriate services to children

[8] CRIAs for digital products and services should as a minimum (i) assess against the UNCRC General comment No. 25 and underpinned by the 5Cs framework; (ii) follow minimum standards on process and criteria, as for example described in section 7.3 of CEN-CENELEC CWA 18016 or the risk self-assessment tool of the UK ICO Children's Code.

[9] (1) "Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. (2) In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration."

by design and default. Moreover, these efforts often leave the most vulnerable children behind, especially those with disabilities, living in poverty or living outside of family care.

Online platforms must therefore **assess and mitigate online risks for children**, putting a special focus on the impact of digital designs on children's rights and development. For this, **child rights impact assessments** are useful tools to help anticipate the negative and harmful effects of their products and services on their rights. Designing online services and products with child rights in mind **('Child Rights by Design'**) is crucial to find avenues that recognise the child's right to participate while addressing their best interests, privacy, safety and developmental needs[10]. Moreover, a risk- and child rights-based approach guarantees that measures put in place to protect children meaningfully encompass a wide range of children's needs and minimise their negative effects on all children's rights.

What is Safety-by-design?

Safety by design is a terminology used to refer to practices that put user safety at the core of designing online platforms and technologies. In practice, this means designing technologies and online features in a way that minimises online risks by anticipating and eliminating online harms before they occur.

One pathway contributing to realising child rights online is embedding **safety- and privacy-by-design** in digital designs. Same as there are specific limits to data collection and advertisement practices to children online, there needs to be minimum standards to age appropriate design and content that can be catered to children. From the side of online service providers, this includes measures ranging from the more general such as effective content moderation or child-friendly reporting mechanisms to the more tailored measures targeting children such as the ones included in the next section. Additionally, there must be robust and child-friendly mechanisms for reporting online harm that connect the child at risk to the relevant support systems at national level.

If encompassed together, these two prevention approaches (awareness raising and child-rights by design) will ensure that children have a better chance to navigate digital environments that are themselves already safe.

For legislators, enshrining safety-by-design principles in policies implies mandating risk and child rights assessments and minimum standards of safety and security for children online. There is existing good practice, codes and technical standards[11] aiming to guide developers and designers in accounting for children's rights when developing digital services. Similarly, different jurisdictions are advancing towards stronger business accountability for harmful and illegal content and behaviours in their platforms[12]. Despite this, political will to legislate the digital environment significantly decreases when it may affect issues such as privacy,

[10] 5Rights Foundation, Child Rights By Design: Guidance for innovators of digital products and services used by children.

[11] For example, but not limited to, the Swedish guide on the rights of children and young people on digital platforms, the Dutch Children's Code, the Irish Fundamentals or the UK ICO's Children's Code. As regards technical standards, see CEN and CENELEC Workshop Agreement CWA 18016 'Age appropriate digital services framework'.

[12] See, for example, the Digital Services Act in the EU, the UK Online Safety Act or the Online Safety Act in Australia.

cybersecurity and freedom of expression and other civil rights, even if at the expense of children's best interests.

2. Empower children

Child empowerment is a core aspect of children's wellbeing online and offline. Digital environments must not only be safe for children, but also enabling and empowering: they should not be considered only as vulnerable individuals in need of protection, but as agents of their own lives.

A child is empowered when they can freely exercise their rights[13]. This means that digital spaces and tools need to **enable the exercise of all their rights** as included in the UNCRC, including the right to non-discrimination; to life, survival and development; to respect for children's views (art. 12); to freedom of thought, religion and speech (art. 14); to privacy (art. 16); to access to information (art. 13); to protection from violence and exploitation (art. 34, 36); and to play (art. 31), among others.

In order to offer such enabling spaces, online platforms and policymakers must take a holistic approach to children's rights, often requiring an exercise of dynamic balancing of rights, on the basis on a CRIA based on the UNCRC and General Comment 25. In fact, online platforms must design their services with the complexities and interplay of children's rights in mind. For example, some online safety measures may require the processing of personal data of the child, hence limit privacy for a legitimate purpose of safety. So limiting the child's right to privacy can be legitimate for safety purposes, but at the same time their right to privacy can be the cornerstone to secure their right to access information. Policy makers and online platforms need to ensure these rights are realised and balanced in the decisions they take, so that not one right has preference over the other.

There are two elements that can support this exercise. First, **the best interests of the child** as outlined in Article 3 of the UNCRC. While this principle is easier to apply at the individual level, policies and regulations that affect children must be drafted in consideration of the general best interests of children. As one core principle of the UNCRC, in some cases the best interests of the child will tend to prioritise children's protection from harm, especially in cases of high risk of severe harm (i.e., abuse).

In other cases, a proportionality analysis may point towards less intrusive measures. All online safety measures targeting children have to also be assessed on their proportionality to the risk they address **and to the effect on the exercise of other rights of the child**. On the one hand, the nature and level of the **risk** may justify in some cases the limiting of some rights – i.e., exposure to child sexual abuse. In others, mitigated risk may signal less need for restrictive measures - i.e., platforms with stronger safety standards might not require the use of more invasive age assurance methods. In parallel, the positive and negative effects on **the exercise of all other rights** must also be considered – i.e., by guaranteeing the safety of

[13] OECD (2024), What Does Child Empowerment Mean Today?: Implications for Education and Well-being, Educational Research and Innovation, OECD Publishing, Paris, https://doi.org/10.1787/8f80ce38-en.

children online we are simultaneously protecting other rights as well, for example freedom of expression or play, but also potentially infringing on the children's right to privacy or access to information or diverse media.

While basic safety is often a precondition for children to obtain all the benefits from their digital experiences and exercise their right to healthy development. However, overly prohibitive safety policies can also be detrimental. This is why a **differentiated approach that accounts for the evolving capacity of children** is needed, adapting the intrusiveness of online safety measures, when appropriate to the risk, between the needs of very young children and teenagers. This way, when developing technological solutions, the balancing act between safety and privacy needs will yield very different outcomes between younger and older children.

Empowerment is also building the agency of children **to make informed decisions**, as children themselves explained in the VOICE Research. In order to be able to make informed decisions, age-appropriate and purposeful information should be provided to the child throughout their user journey. This means not only providing it in the Terms & Conditions, but also when substantial changes are made to their experience (i.e., privacy settings), to ensure the consent obtained and the safeguards adapt to the age and maturity of the child.

Finally, the respect to **children's views** is at the centre of child empowerment, as safeguarded by Article 12 of the UNCRC. By listening to and taking into account children's views, especially when drafting policy and designing online services, we are making children active agents of society. Through concepts such as Child Rights by Design, children can actively contribute to shape online services that cater to their needs more effectively.

3. Upholding the responsibility of all parties: stakeholders recommendations

The last key component of online child protection is its multilateral nature, as upholding the responsibility and accountability of all agents involved is fundamental. This includes, among other stakeholders, building on the **accountability of the state and businesses to prevent and protect children from harm**, as outlined in the UN General Comment No. 25. Moreover, parents and educators also play an important role, beyond building digital literacy, as intermediaries and advocates for children's rights online. A community-based approach to child safety online is crucial to recognise and empower them in their role.

While the desire to regulate the online environment from national and EU policy-makers is increasing, digital policy debates often put children's rights in a secondary note in favour of privacy interests, in many cases disregarding that privacy is also a fundamental right of children. Online platforms repeatedly prioritise commercial interests over the best interests of the child, avoiding prescriptive regulation or delaying compliance, and do not spend sufficient resources in creating solutions that address the complex and emerging risks children face online.

Eurochild therefore recommends that governments and regulatory bodies:

- Support awareness and collaborative digital literacy programmes for children, parents and teachers, following a systemic and community-based approach and ensuring that they are inclusive and effective;
- Support the creation of a diverse landscape of high-quality and age-appropriate content to support children's access to diverse information.
- Adopt and enforce legal frameworks that uphold the responsibility of online platforms to operate and design their products and services in accordance to children's rights. Adopt outcome-based appropriate enforcement measures in accordance, notably the necessary technical standards and frameworks for companies to comply with measures that are viable, implementable and effective.
- Regularly monitor and evaluate the efficiency of regulatory measures and identify emerging systemic needs and gaps, in collaboration with a wide range of stakeholders, especially children.
- Foster collaborative multi-stakeholder spaces where technical and legal solutions can be tested to enhance innovation in solutions that advance children's rights online.
- Develop the necessary tools and support for practitioners to address online harm and build the resilience of the national child protection systems to address the evolving nature of online risks and harms.

Online platforms must:

- Comply with existing regulatory frameworks;
- Foster and commit to initiatives that, beyond legal compliance, support children's rights online and uphold the duty of care towards children; including child-rights-by-design and safety-by-design approaches.
- Respond in a timely manner to any indication of a violation of children's rights within their platforms through a robust prioritisation system, and adhere to the highest transparency standards for managing such violations.
- Exercise socially responsible and inclusive innovation that does not put the commercial interest over that of children;
- Work closely with civil society and children to make sure their online platforms respect children's rights and are inclusive to all children, especially the most vulnerable.

Section II. Priority areas for Eurochild

Priority 1. Promoting children's rights through safety and privacy-by-design

For decades, digital skills have been portrayed as a magical solution for online child protection and empowerment. However, putting the responsibility of online safety and wellbeing on children and families has proven to be inadequate. While building the digital skills of children and families can be a powerful enabler of children's rights[14], there are limits as to what they can understand, especially concerning complex issues like algorithmic triggers or dark patterns. Moreover, in order to guarantee that the rights of all children, no matter their family environment or cognitive abilities, are equally respected, the responsibility to offer safe services should be guaranteed by online platforms.

From games and education technology to search engines, social media recommender systems and chatbots, **Artificial Intelligence (AI)** underpins most of the main digital products and services children use. It is increasingly mediating almost every aspect of their lives, and influencing their development. On the one hand, AI plays a critical role in enhancing safety, for example by proactively detecting and mitigating harmful content, such as cyberbullying, hate speech, or sexual exploitation, in real-time, allowing for faster intervention and support. AI-powered digital solutions can also streamline and strengthen reporting systems for children and their caregivers by making them more accessible to children and supporting triage and streamlining of reports to enforcement and support services. At the same time, children face unacceptable levels of risk from a wide range of applications and are more vulnerable to exploitation or harm caused by negligence or misuse of AI systems. Moreover, AI is exacerbating an already alarming child sexual abuse crisis through programs that can generate incredibly realistic images and videos of child sexual abuse and exploitation at great speed and scale. AI systems that present risks to children must be subject to strict due diligence processes, while those that exploit the vulnerabilities of children should be banned altogether.

Therefore, there is a need to shift from traditional approaches relying on parental controls and digital literacy towards a focus on digital designs that respect children's rights and are safe, private and secure for children by design and default. In order to protect children across the EU, it is fundamental that design aspects are checked against children's rights before market entry or retrofitted to be able to operate in the EU market, through the correct implementation of existing legislation (i.e., the AI Act and the Digital Services Act).

This includes making design choices that, among others:

- Are based on an assessment of their potential impact on the full spectrum of children's rights, namely on the basis of a child rights impact assessment.
- Set out proportionate, appropriate, effective, inclusive and privacy-preserving age assurance measures, where necessary;

[14] Livingstone, S. Stoilova, M. and Rahali, M. (2023). Realising children's rights in the digital age: the role of digital skills. KU Leuven, ySKILLS.

- Minimise the collection and exploitation of children's data and prioritise the best interests of the child in the use of such data[15];
- Present terms and conditions in a way that is age appropriate[16] and understandable for children and reiterated along the user journey (i.e. when specific settings are changed);
- Ensure settings are "high privacy" by default for child users (including interaction with other accounts, chat functions, comments, livestreaming and shareability of the content, etc.) and have clear processes for modifying them according to their evolving capacities;
- Turn off profiling options by default, especially for the purpose of targeted advertisement[17];
- Prioritise the best interests of the child over commercial imperatives, particularly avoiding functions designed to maximise engagement, extended use or that make it difficult to turn off or exit the online experience;
- Provide clear and accessible information (i.e., about privacy settings, functionalities limiting exposure to harmful content or contact, etc.) to children to promote the agency and empower children to make autonomous decisions.
- Provide inclusive, effective and privacy-respecting parental control features which promote communication around safety between caregivers and children to support the learning of self-regulation and best practices;
- Provide tools for effective and age-appropriate reporting and redress;
- Rely on children and child rights experts for roles and responsibilities dedicated to the protection of minors.

Doing this meaningfully implies building on safety and privacy with design choices that account for and respect a wider array of children's rights – including their best interests, promoting their agency, enabling their development and listening to their views. Therefore, a core aspect of safety-by-design is involving children actively and giving them a seat at the decision making table that will determine the features and measures that will keep them safe in their digital environments.

[15] In full compliance with the GDPR, which requires children below the age of digital consent to have verifiable parental consent for the processing of their data (Art. 8), enhanced data protection for children by design and default and data protection standards (Art. 6, 8, 12 and 40).
[16] 5Rights Foundation, Tick to Agree – Age appropriate presentation of published terms, 2024.
[17] In full compliance with the GDPR, the AI act and the DSA.

Priority 2. Fight against child sexual abuse and exploitation (CSAE)[18]

A particularly severe harm to which children are exposed to is child sexual abuse and exploitation, which, facilitated by technology, is growing exponentially in recent years[19]. In Europe, data suggests that approximately 1 in 5 children becomes a victim of sexual violence.[20]

The National Center for Missing and Exploited Children, registered a drastic increase in reports of online child sexual exploitation. The number of reports of suspected child sexual abuse rose from 1 million in 2010 to 36.2 million reports in 2023 globally. Online platforms submitted almost 55 million images and 50 million videos to the CyberTipline in 2023. This year has also marked the biggest increase in reports related to online enticement (which includes grooming), which have increased by 300% from just 2021[21]. NCMEC reports that 90% of reports involving the upload of CSAM belonged to users outside the United States. According to the Internet Watch Foundation, Europe has advanced to the largest host of child sexual abuse material in the world, hosting around 60% of such material in 2021[22]. The high report numbers have also resulted in high removal numbers[23].

CSAE is also a growing concern to children themselves, as raised by the VOICE research. **Child sexual abuse is a serious violation of children's rights as laid down by the UN Convention on the Rights of the Child and the EU Charter**, not only because every child has the right to be protected from all forms of abuse, but also because the disclosure of photos and videos of a child breaches their right to privacy. Revictimisation has devastating effects on victims, and can go on for years and decades, due to the relatively easy resharing of the material depicting their abuse. Moreover, the devastating effects on children's wellbeing and capacity to freely participate in society pose limits to other rights, such as freedom of speech or right to development.

In order to tackle this crisis, several steps are needed. First, **prevention** efforts are key. While national action such as awareness raising and social protection measures work domestically, at a global level online platforms should assess the risk of being used for the purpose of child sexual abuse in order to put **mitigation measures that remove or adjust the features that enable the proliferation of child sexual abuse**, ultimately refining their services for children's safety. Prevention and detection of child sexual abuse material must go hand in hand to ensure we can protect victims of the crime. **Detecting CSAE** allows preventing re-victimisation by facilitating the removal of the material depicting the abuse of a child, and supports the identification and rescue of victims. The complexity and ethical considerations of automated

[18] For Eurochild's definition of child sexual abuse, please check our child protection policy.
[19] IWF Annual Report 2023.
[20] Council of Europe, ONE in FIVE, accessed 23 November 2021.
[21] Cybertipline 2023 report, National Centre for Missing and Exploited Children.
[22] Europe remains 'global hub' for hosting of online child sexual abuse material, Internet Watch Foundation, 2022.
[23] For example in Germany, studies find a 98% removal rate within 2 days in 2023.

detection technologies, however, require the imposition of strong technological and legal safeguards that ensure that all children's rights are protected and balanced when being deployed (i.e., operated under a judicial mandate, guaranteed effectiveness, security and privacy standards, transparency, etc.).

Finally, strong referral mechanisms to **law enforcement** and better capacity of agencies to fight the crime. National child protection systems should better incorporate the interlinks between offline and online child sexual abuse and build the capacity of their staff to address the dimensions of technology-facilitated child sexual abuse (i.e., by integrating child protection agencies' with digital reporting frameworks).

Many online service providers have been voluntarily detecting child sexual abuse material in order to remove the material and protect child victims. However, *voluntary* detection and reporting has proven insufficient to protect children adequately – as online platforms put different measures in place, children are left unevenly protected across platforms. Moreover, platform accountability binds all online platforms to put in place measures to protect children from harm, as mandated by the UNCRC General Comment No. 25. Finally, the scale of the crime requires the EU to set out consistent obligations to online providers who risk being used for the purpose of abusing children, to detect and remove all instances of child sexual abuse in their services.

Priority 3. The digital wellbeing of children

Children are highlighting concerns on the negative effect of technology on their mental health and wellbeing[24]. Mental health became a particularly important topic among children and young people since the Covid-19 crisis, with research showing that young people's mental health has worsened since the pandemic[25]. While during this period digital technologies played an essential role for the social development and participation of children (i.e., videogames[26]), heightened exposure to inappropriate content, conduct and contact risks have been proven to have negative effects on children's overall wellbeing. However, there is a need to further explore the effect of more nuanced issues such as excessive screen time or datafication.

Research shows that the trend of online violence normalisation that is becoming predominant online has negative effects on the wellbeing of children. For example, children have reported feeling guilty and frustrated when they feel uncomfortable after being exposed to content that has become normalised. [27]. There is also increasing evidence of pornography's role in shaping and fueling violence against women and girls. According to UNICEF, exposure to

[24] ECPAT International, Eurochild and Terre des Homes Netherlands, Speaking up for change: children's and caregivers' voices for safer online experiences, 2024.
[25] OECD, Health at a Glance: Europe, 2022
[26] See the Play Apart Together Campaign of the World Health Organisation.
[27] Livingston et al. (2022). Young people experiencing internet-related mental health difficulties: the benefits and risks of digital skills. DOI:10.5281/zenodo.7372552

pornography at a young age can result in poor mental health, sexism, sexual violence, and the objectification of women, as well as normalisation of abusive and misogynistic behaviours[28].

There is a clear link between the amount of time children spend online and the likelihood of risk exposure[29]. However, the relationship between mental health and online usage is not straight forward, as it relies heavily on the type of usage (rather than quantity) and on preexisting vulnerabilities or mental health conditions[30]. For example, it has been reported that children from vulnerable backgrounds, including those living in poverty, with special education needs or physical or mental disabilities, or experiencing challenges with their mental health, experience more of the negative impacts of digital technology on their wellbeing[31].

As it is relatively difficult to capture large-scale effects of online platforms on all children, it becomes more relevant to focus on the specific mechanisms that enable harm or exacerbate risks. There is some consensus that both child factors (i.e., demographic characteristics) and parent factors (i.e., parental perception and mediation) play a role to children's wellbeing[32]. Some studies reveal that the impact of online usage on mental health, especially in contributing to depressive symptoms linked to body image and eating disorders or linked to image-based sexual abuse, is larger for girls than it is for boys[33]. Children participating in the VOICE research highlighted concerns related to personal and social confidence, anxiety disorders, addiction and isolation.

The emphasis of online platforms on maximizing engagement, the use of popularity metrics and algorithmic biases have shown to exacerbate many of these risk factors, making it more difficult for children to 'escape' vicious dynamics on their wellbeing (often referred to as "dark patterns"). Therefore, the pathway towards improving digital wellbeing outcomes for children heavily relies on safety-by-design. In addition, it is very important that governments integrate better the dimensions of online harms in policies and investment targeted at mental health outcomes, while ensuring practitioners that work with children are well resourced and skilled in addressing these issues.

[28] UK Government Equalities Office (GEO), 2021. The relationship between pornography use and harmful sexual attitudes and behaviours.

[29] Livingstone, et al. (2019). Children's data and privacy online. Growing up in a digital age: An evidence review

[30] D'Hombres, B., Kovacic, M., Schnepf S. and Blaskó, Z. (2024). Loneliness and social media use in the European Union. Fairness policy brief 2/2024. European Commission – Joint Research Centre, JRC135806

[31] Internet Matters, (2023), Index Report 2023: Children's Wellbeing in a Digital World.

[32] Cao S., Li H., (2023), A scoping Review of Digital Well-being in Early Childhood: Definitions, Measurements, Contributors, and Interventions.

[33] Park K., Ging D., Murphy S., McGrath C., (2023), 'The impact of the use of social media on women and girls'.

Conclusion

Digital engagement is not an isolated sphere of children's lives, but an integral part for their development and the realisation of their rights. However, evolving and increasingly complex risks threaten their safety and privacy (i.e., persuasive design and OCSEA) and their mental and physical wellbeing. Therefore, online child safety requires a more integrated approach that encompasses traditional awareness raising and parental responsibility with online platform accountability towards children's rights. Online platforms must implement existing legislation, including the DSA and AI Act, and design their services and products in a way that enables children to exercise their rights, from safety and privacy to information and freedom of speech. It is crucial that legislators hold them accountable for doing so, develop strong digital rules and enforce current legislation.

For more information, contact:
Fabiola Bas Palomares
Lead Policy & Advocacy Officer – online safety
Fabiola.palomares@eurochild.org

Mieke Schuurman
Director of Child Rights and Capacity Building
mieke.schuurman@eurochild.org

Eurochild AISBL
Avenue des Arts 7/8, 1210 Brussels
Tel. +32 (0)2 511 70 83
info@eurochild.org – www.eurochild.org

© Eurochild 2025