

Bridging persistent gaps in children's rights online in Europe

Taken from
*Children's Realities in Europe:
Progress & Gaps*
Eurochild 2024 flagship report
on children in need across Europe.



Eurochild
Putting children at
the heart of Europe

February 2025

Bridging persistent gaps in children's rights online in Europe

On 20 November - World Children's Day - Eurochild released its flagship report on children in need titled "Children's Realities in Europe: Progress & Gaps", which compiles information from 57 Eurochild members in 31 countries across Europe. This sub-report presents insights on various aspects related to children's rights and child protection in the digital environment focusing on the needs and gaps highlighted by Eurochild members. This overview is followed by Eurochild recommendations to the European governments to be implemented with the support and guidance of the European Institutions.

Introduction

1. Children's rights in the digital environment

Children's rights are guaranteed by the UN Convention on the Rights of the Child equally online and offline, and regulators and online platforms must respect and safeguard them in the same way. The [UNCRC General Comment No. 25](#) recalls the importance of a **wide range of children's rights** in the digital environment, including but not limited to:

- **The right to access the Internet** (principle of non-discrimination), **to information** (art. 17), **to expression and opinion** (art. 13)
Children's rights to information and to freedom of expression requires states to guarantee that children are able to access a wide range of information that is age appropriate to them, only to be restricted in necessary cases to safeguard their own rights or wellbeing. This includes ensuring the access to internet connection and services.
- **The right to education** (art. 28) and **the right to play** (art. 31)
Children's right to education also guarantees their right to receive digital literacy and skills education, which is key to ensure they can navigate the digital spaces safely and anticipate and respond to online harms.
- **The right to privacy** (art. 16)
Children's right to privacy gives children sovereignty over their personal data, including the right to be forgotten, obliging online platforms to require informed and voluntary consent of the user before collecting their data and avoid commercial exploitation of children's data. It also includes the right of children's online activities and content to not be monitored by others (such as parents) without consent.

- **The right to protection from violence and abuse** (art. 19)

The right to protection from abuse requires state authorities to make the internet a safer place to prevent online forms of abuse, including cyber-bullying, sexual abuse and exploitation and economic exploitation.

These rights are largely interconnected, and are **underpinned by four fundamental principles**, in particular **the right not to be discriminated against** (art. 2), **the obligation to put the best interests of the child at the center of all policies affecting them** (art. 3), **the right to life, survival and development** (art. 6) and **the right to be heard**. Children therefore have rights and freedoms online, and must be protected as well as supported to ensure a complete and safe online experience. All in all, states must protect children from harmful content and abuse without restricting their rights online, by ensuring access to safe digital spaces where their privacy, self-expression, and dignity are guaranteed.

2. The state of play

The digital environment is designed for adults, yet one in three Internet users worldwide is a child¹. This exposes children to a number of significant risks, as the recent Eurochild VOICE Project study with ECPAT International and Terre des Hommes shows: children express their concern about the risks they face on the Internet, ranging from harassment and abuse to inappropriate content and the misuse of their personal data, and are displaying increasingly high tolerance to violence online. These risks can be divided into four categories, relating to content, contact, conduct and contract². These include, among other things:

- Inappropriate content such as hate speech, violent or radical, including suicide and self-harm, and sexual material;
- 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, as well as health and wellbeing and cognitive, social and emotional development.

To address the persistence and increased exposure of children to these risks, the European Union and other countries in Europe are building a regulatory framework that puts particular emphasis on the responsibility of digital platforms to protect minors. The efforts to build on the accountability of online platforms are increasingly shared globally, as a number of countries pass legislation to strengthen the safety of online users. The **United Kingdom** adopted the Online Safety Act in 2023, which puts a range of duties on social media companies and search services, including strong protections for children to prevent them from accessing harmful and age-inappropriate content, while providing for clear and accessible ways to report problems online. In **Australia**, the Online Safety Act 2021 requires

¹ Unicef, *The State of the World's Children 2017: Children in a Digital World*.

² Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children.

online services providers to regulate illegal and offensive online content, and makes them accountable for the safety of people using their services, including children.

In the **European Union**, the General Data Protection Regulation establishes a legal framework to protect privacy and personal data, including setting higher standards for the processing of personal data of children under the age of 16. The Digital Services Act requires providers of online platforms accessible to minors to ensure a high level of privacy, safety and security for them, and prohibits (i) the use of profiling or targeted advertising to minors, and (ii) dark patterns, which manipulate children to make decisions against their best interests including by generating addiction. It also mandates better moderation and removal of illegal content, such as child sexual abuse material (CSAM) and requires platforms to assess and mitigate the effects of their services on children's fundamental rights. The Audiovisual Media Services Directive, which covers all services providing audiovisual content (including video-sharing platforms and social media services), obliges that content which may impair the physical, mental or moral development of minors is only made available in such a way that minors will not normally hear or see it. With these two instruments, the EU is attempting to tackle not only harmful or illegal content, but also risks that may arise from the design of online platforms themselves.

In order to complete this legal framework, and in particular to combat the online sexual abuse crisis that Europe has been experiencing for the last 10 years and which continues to worsen, two other initiatives are currently under discussion. The European Commission proposed to amend the Directive combating the sexual abuse and sexual exploitation of children and child sexual abuse material in line with new technological developments affecting the manifestation of the crime. More concretely, it aims to increase the penalties and extend the definition of child sexual abuse offences both offline and online, and provide specific requirements for prevention and victims support. Secondly, the proposed Regulation to prevent and combat child sexual abuse would establish a set of mandatory obligations for Internet companies to detect, report and remove CSAM on their services, including through detection or blocking orders where necessary.

To guide this regulatory approach, the European Commission launched the Better Internet for Kids Strategy (BIK+). This comprehensive approach aims to improve children's online experience through investing in digital literacy, fostering multi-stakeholder cooperation, and establishing Safer Internet Centers to support awareness and helpline/hotline work at national level and work with children to understand their experiences online.

The implementation of this legislative framework must be guided by the realities of children across all EU Member States. This report compiles information on children's rights in the digital environment extracted from Eurochild's 2024 report on children in need across Europe, "Children's Realities in Europe: Progress & Gaps". The information presented here is based on assessments provided by 57 Eurochild members in 31 countries and territories³.

³ Albania, Belgium, Bulgaria, Croatia, Cyprus, Denmark, England, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Kosovo, Latvia, Malta, Moldova, Netherlands, Northern Ireland, Poland, Portugal, Romania,

Findings from Eurochild Members

1. Common risks and trends across Europe

Across Europe, **children are exposed to a wide range of risks online**, which persist and worsen. As Eurochild members call for more targeted and effective regulation protecting children online, there is an urgent need to address harmful or illegal behaviors and content against children. Eurochild member organisations in **Croatia**⁴ warn about the different natures of these risks: violence, harmful content, breaches of data and privacy and addiction or excessive use of digital media. This requires a multifaceted and multistakeholder response, especially as these risks affect children even before they reach adolescence. In **Belgium**⁵, the average age for an individual to have their first smartphone is 8 years old and in **Greece**, 97% of children over 10 use the Internet. In **Malta**, data suggests that approximately 15% of children **aged 3 to 11** have experienced online abuse, 83% of those experiencing cyberbullying and 26% forms of sexual abuse.

Cyberbullying remains in fact a major concern, as members from seven countries⁶ in the report alert, especially as it becomes a more and more normalised phenomenon. In **Hungary**, a study indicated that 55% of individuals aged 14 to 25 reported experiencing online harassment, with over 90% having received messages from strangers at least once. Eurochild members in the **Netherlands**⁷ worry about the impact of these experiences, especially social media, on children's mental health and wellbeing. As a consequence of additive digital designs, civil society points to the **excessive use of digital media** as an increasing challenge, as highlighted by members in Croatia, Greece, Kosovo, Slovenia and Türkiye. For instance, in Hungary, almost 50% of children and young people aged 15 – 25 felt they spent too much time on social media and gaming.

Child sexual abuse and exploitation is a very high concern highlighted by Eurochild members, especially as the volume of CSAM shared online is increasing every year, reaching more than 100 million files reported to NCMEC in 2023⁸. In Hungary, the national hotline received 850 reports related to CSAM in 2023, out of 1900. Members in six countries⁹ denounce the growing exposure of children to these abuses, and note the lack of protection and prevention in place. A number of mechanisms can be implemented to provide more appropriate assistance and support to victims, as well as to reinforce the detection and removal of CSAM. This includes supporting the capacity of civil society across Europe, which plays a key role not

Scotland, Serbia, Slovakia, Slovenia, Spain, Türkiye, Ukraine and Wales. To see the full list of members who contributed, please read the full report.

⁴ Ombudsman for Children; "Croatia for Children" Foundation; The Society "Our Children" Opatija; Association "Magical World", Knin; Croatian Association on Early Childhood Intervention; Association Children First.

⁵ Data from the regions of Flanders and Brussels.

⁶ Albania, Bulgaria, Hungary, Malta, Northern Ireland, Poland and Serbia.

⁷ Dutch NGO Coalition for Children's Rights Utrecht University; Dynamics of Youth.

⁸ National Center for Missing and Exploited Children, CyberTipLine 2023 report.

⁹ Albania, Hungary, Spain, Romania, Finland and Malta.

only in raising awareness and promoting digital literacy, but also directly supporting children at risk through helplines, hotlines and victim support services.

Another key finding of this report is the persistence of a **digital divides** in most countries, particularly affecting children in vulnerable situations, living in rural areas or experiencing poverty. These divides risk reinforcing and widening them, for example by depriving the most vulnerable children from playing and communicating with others or accessing information, all key to their healthy development. In **Bulgaria**, Eurochild members¹⁰ highlight the insufficient access to digital devices and Internet connection, especially in economically deprived regions and among marginalised communities. This divide results in a gap in access to digital literacy resources which reinforces risk of exposure to online harms, especially for children with disabilities or special educational needs.

In eight countries, this gap is particularly strong between urban and rural communities¹¹. Members warn about the risks it presents of increasing social exclusion, reproducing and reinforcing existing inequalities. The Fondazione L'Albero della Vita in **Italy** calls for facilitating access to digitalisation for children and adults in vulnerable situations in order to reduce child poverty and social exclusion. In **Romania** the project *Let's Click on Romania*, led by the NGO Workshops Without Borders, aims to bridge this gap by providing refurbished devices to schools and children in vulnerable areas, and has supported over 80,000 children and teachers in 450 schools with 8000 computers since 2020.

Lastly, several members emphasised that, despite the progresses made under the GDPR Regulation, risks to children's privacy and data persist in many countries. In **Croatia**, children are often confronted with breaches and misuses of their personal data. The Estonian Union for Child Welfare calls for better data protection training for teachers, to prevent the disclosure of students' personal data without their knowledge and consent. In **Poland**, the data protection authority has issued much needed guidance on the implementation of the GDPR requirements, although with limited effect.

Across Europe, civil society notes the lack of evidence and research on these issues affecting children. To better understand the extent of these issues, the Estonian Union for Child Welfare stresses the need for conducting more research and studies on children's safety and conduct online. The creation of exhaustive databases documenting the various violations of children's rights would also help to improve the understanding of these infringements and to combat them more effectively, as called for by Eurochild Croatian members¹².

2. The positive role of digital literacy and the limitations of civil society

A critical issue is the **limited impact of digital education and media literacy** for children, parents and teachers, which compromises caregivers' ability to monitor children's online

¹⁰ CONCORDIA Bulgaria Foundation; National Network for Children.

¹¹ Croatia, Spain, Scotland, Wales, Latvia, Serbia, Moldova and Malta.

¹² Ombudsman for Children, Croatia; "Croatia for Children" Foundation; The Society "Our Children" Opatija; Association "Magical World", Knin; Croatian Association on Early Childhood Intervention; Association Children First.

experiences, teacher's ability to use and benefit from digital tools and resources, and increases exposure of children to online risks.

Eurochild members observe that while a high percentage of children and parents use the Internet every day, many of them still lack the necessary digital skills to navigate it safely or use online child protection tools to ensure that their children do so. This is observed across the whole continent: in **Bulgaria**, the first National conference on "Children in the digital world" underlined an insufficient digital literacy among children and their parents, which is directly linked to the risks of online sexual exploitation and abuse and cyberbullying. In **Cyprus**, the Pancyprian Coordinating Committee for the Protection and Welfare of Children regrets that no specific government initiative exists to enhance children media literacy and awareness. In **Slovenia**, the Slovenian Association of Friends for Youth highlights the same lack of adequate digital literacy education, for both children and parents – especially about the risks related to children's online privacy and personal information.

Schools play an important role in building the digital capacities of children. The Estonian Union for Child Welfare stresses out the need for a better cooperation between schools and parents, who are both key actors in supporting children's safety online. In **Serbia** and **Malta**, Eurochild members¹³ advocate for more empowerment and training of educators, and in **Malta** and **Kosovo**¹⁴ there are calls for digital literacy education classes to be integrated directly into the national curriculum. However, this requires that the education system be adapted to include digital support and education, which is still not the case in many countries such as **Latvia**¹⁵.

Civil Society Organisations (CSOs) also contribute significantly to raising awareness on digital education, providing for pedagogical resources and support to children and families. In **Portugal**, the organisation *Miúdos seguros na net* has been working for 20 years helping families, schools and communities to promote online safety for children and young people. In **Northern Ireland**, Children in Northern Ireland published a youth-led research on the impact of social media on teenage girls, revealing experiences of cyberbullying, impacts on self-esteem, body image and mental health and self-harm and putting the children and gender perspective to the forefront. In **Türkiye**, our member Hayat Sende emphasises the importance of activities that integrate screen time with reading, family interaction and face-to-face socialisation to help children develop good practices and reduce the risk of digital addiction.

Eurochild members recognise the role of Safer Internet Centers in their countries as holistic interventions integrating helpline, hotline, awareness raising and child/youth participation altogether. For example, in **Albania, Bulgaria, Cyprus and Portugal**, the Safe Internet Center (SIC)¹⁶ include a support helpline and hotline, which process reports of CSA and provides

¹³ The Network of Organisations for Children of Serbia – MODS; Pomoć deci; SOS Children Villages; Serbia Child Rights Center; Friends of Children of Serbia for Serbia, Malta Foundation for the Wellbeing of Society for Malta.

¹⁴ The Malta Foundation for the Wellbeing of Society for Malta; CONCORDIA Projekte Sociale; Coalition of NGOs for Child Protection-KOME for Kosovo.

¹⁵ Latvian Child Welfare Network; Latvian Protect the Children, Public Ombudsman.

¹⁶ iSIGURT.al for Albania, Safenet in Bulgaria, the Cyprus Pedagogical Institute in Cyprus, Centro Internet Segura for Portugal.

counselling for children and training to caregivers and teachers. However, there is still a need to better equip and empower civil society to effectively support the prevention of online harms in Europe. For example, NGOs in **Hungary** have not been allowed to provide training on online safety for children in schools. In fact, an effective system to combat child sexual abuse online requires strengthening the capacity of civil society to respond, for example by providing clarity on the institutional responsibility for removing or blocking illegal or harmful content as raised by Eurochild members in **Albania**. Psychological support for victims, in cases of abuse or harm online, should also be strengthened for children and for their families, as pointed out by Eurochild members in **Portugal**.

Collaboration across the public sector and civil society is crucial to enable effective and sustainable initiatives. In **Serbia**, the government promoted awareness and safe use of Internet through the recent establishment of a National Contact Center for Safety of Children on the Internet¹⁷. In **Moldova**, A.O. Concordia Proiecte Sociale notes the good information and prevention disseminated by the Ministry of Education and Research through programs on online safety for both teachers and children, and by a platform containing guidance for parents. In **Türkiye**, the Ministry of Family and Social Services provides training on the dangers that children face online, and has established a Social Media Working Group that intervened in over 1,250 cases to protect children from harmful content, although more effective online safeguarding measures are still needed.

In **Belgium**, the Wallonia-Brussels Federation has adopted a specific media education plan, and the new *Flemish Youth and Children's Rights Policy Plan* include a specific focus on the digital environment. In **Ireland**, the Children's Rights Alliance highlights the progress made in reforming the primary school curriculum to include online safety and digital literacy. However, it calls for more rapid integration of these issues from pre-school through secondary education. Our **Latvian** members¹⁸ also welcome the *Skola 2030* initiative, which aims to promote digital literacy from an early age, by providing learning materials for teachers and integrating digital literacy at all stages of education. Similarly, **Poland's Digital Competence Development Program 2020-2030** aims to enhance digital skills across various sectors, especially critical analysis and AI, including education from pre-school to secondary school.

As children and adolescents are directly affected by these policies and services, they have the right to be involved in the discussion, reflection and decision-making process. To this end, CSOs and governments have introduced a number of **child participation initiatives**. For example, in **Scotland**, the government commissioned the *Children's Parliament* and the *Scottish Youth Parliament* to engage with children on the design of a website providing information for children on screen time and the use of social media. Safer Internet Centres play a key role in elevating the experiences and views of children, as for example the Cyprus Pedagogical Institute's *CyberSafety Youth Panel*, in which the *Cyprus Children's Parliament* actively participates.

¹⁷ The National Contact Center for Safety of Children on the Internet is part of the SIC+ program, sharing knowledge and good practices with the SIC network but not receiving EU funding.

¹⁸ Latvian Child Welfare Network; Latvian Protect the Children.

3. Persistent shortcomings in the regulatory framework

Eurochild and its members welcome the progress made in several countries to improve children's experiences online and to strengthen the legal framework to protect them from illegal or harmful content. For instance, in **Ukraine**, the national legislation is in line with the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and policies address some aspects of cyberbullying. In **Germany**, Eurochild members¹⁹ welcome the new *Act to strengthen structures against sexual violence against children and adolescents*, including child protection in the digital environment, adopted in 2024.

In **Ireland**, the Comisiún na Méan (Media Commission) is developing Online Safety Codes to guide online platforms on appropriate and stricter safeguards for children online. These codes should require safety-by-design to be standard for all digital services, including the use of Child Rights Impact Assessment before any digital services reaches or affects children. On the same issue, the **Netherlands'** government has published guidance on Child Rights Impact Assessments in the digital context.

In **Spain**, a draft legislation has been announced in June 2024, which could be a milestone mandating age-verification systems, and considering children and adolescents as a specific group with specific needs and special protection in the digital environment. In **Croatia**, a draft of a *National Program for the Digital Environment* is currently under discussion. It is of utmost importance that the best interests of children are integrated at the very heart of this regulatory process, as highlighted by Eurochild Danish member²⁰.

Despite advances at EU level, the **legal framework in many European countries remains insufficient** to address today's challenges. In this context, Eurochild members observe gaps both in criminal law and in platform legal accountability²¹. In six countries included in the report²², there are no specific laws protecting children's rights in the digital environment. For instance, in **Albania**, forms of child sexual abuse online such as grooming and sexual extortion are not classified as specific criminal offences against children but rather as forms of other offences such as fraud or extortion. While **Bulgaria** has adopted a Child Protection Act, it lacks specific provisions addressing online harms such as cyberbullying. The same shortcomings are observed in **Malta**. In **Ukraine**, our members²³ regret that online platforms are not legally required to remove illegal or harmful content, including CSAM, unless ordered by a court, nor are they required to take effective preventive measures to protect children from exposure to dangerous or harmful online content.

¹⁹ [Child and Youth Welfare Association \(Arbeitsgemeinschaft für Kinder- und Jugendhilfe - AGJ\)](#); [National Coalition Germany - Network for the Implementation of the UN Convention on the Rights of the Child \(NC\)](#).

²⁰ [Joint Council for Child Issues in Denmark](#).

²¹ 16 countries explicitly highlight the need for better regulation protecting children online: Albania, Croatia, Denmark, Finland, Greece, Ireland, Malta, Netherlands, Northern Ireland, Poland, Portugal, Romania, Serbia, Spain, Türkiye and Ukraine.

²² Bulgaria, Croatia, Denmark, Finland, Greece and Malta.

²³ [Partnership for Every Child](#); Polina Klykova, [Founder of Children's Rights Info](#); [EDUKIDS](#).

In several countries, this lack of effective legal protections may be explained by a weak institutional framework and a **fragmented regulatory approach**, that continue to hinder the effective realisation of children’s rights online. For example, in **Albania**, as three distinct institutions address online safety issues and there is insufficient coordination among them, reporting and removal of harmful or illegal content online is not centralised, creating a slow and inefficient system. Similarly, in **Belgium**, media literacy programs are implemented in a fragmented manner between the Flanders and Wallonia regions, limiting the reach of initiatives and preventing long-term solutions to pressing issues. In **Finland**, lack of coordination prevents the public sector from fully leveraging the expertise that civil society organisations and the private sector could offer to enhance the policies and programs in place.

Many organisations therefore advocate for a **more comprehensive regulatory approach to enhance online safety that aligns with EU standards** and strengthens criminal law and business accountability for online child safety. For instance, in **Portugal**, civil society²⁴ urges stronger financial and criminal penalties for technology companies that fail to detect, report, and remove CSAM. Likewise, the [Child Rights Centre Albania](#) has emphasised the need to better align the national legal framework with the Digital Services Act and calls for increased penalties for CSAM in the country. Through the [TOMAS Project](#), Eurochild is working with member organisations in **Albania**, **North Macedonia**, and **Serbia** to advocate for better regulation combatting CSAM in the Balkans, which could facilitate the accession process to the EU. In the candidate countries for EU membership, such as **Moldova**, active support from the Union to align national legislation with EU frameworks is key.

The [Malta Foundation for the Wellbeing of Society](#) calls for national policies that address all issues related to children’s digital safety, from cyberbullying and online sexual abuse to digital literacy. In **Northern Ireland**, research by [Children in Northern Ireland](#) called for stricter controls by app developers and social media companies to combat cyberbullying and eliminate harmful content.

Besides strengthening national legal frameworks, it is also key to advance in the correct implementation of existing EU policy at national level. For example, in **Poland**, the Polish Data Protection Authority is playing a key role by providing guidance in the implementation process of the *2023 Act on Counteracting Threats of Sexual Offences*, which establishes new standards for the protection of minors in line with the GDPR.

Furthermore, **emerging areas of online activity should be regulated** to safeguard children from new deceptive practices. Eurochild members in **Ireland**, **Slovenia** and **Ukraine** advocate for the implementation of age assurance tools on social media platforms to ensure that children are only exposed to age-appropriate content and experiences. Age verification is becoming a trend in Europe, in some Member States such as Italy, France or **Spain**, where it is mandated to some services as part of newly proposed legislation. However, it is important to note that age verification is not a ‘silver bullet’ and cannot be implemented in isolation, as

²⁴ [Fundação Nossa Senhora do Bom Sucesso](#); [Instituto de Apoio à Criança](#); [Sérgio Costa Araújo](#) (Individual member).

members in **Ireland** recall²⁵. Eurochild members in the **Netherlands**²⁶ also advocate for safeguards protecting “childfluencers” from commercial exploitation, along with stronger regulation on online gambling, particularly within video games.

It seems clear that some solutions to these challenges must be harmonised at EU level. The potential of the EU to advance on online child safety has been demonstrated by the adoption of protective measures in regulations such as the DSA or the GDPR. [The Malta Foundation for the Wellbeing of Society](#) calls for more standardised digital safety measures at EU level and support for national policies that ensure equal access to digital technology for all children.

The importance of smartphones, social media and the increasing amount of time children spend online pose new challenges, especially during school hours. Although the evidence about the causal effect of high levels of use and negative mental health outcomes on children is still mixed, concerns about the effects on their attention span and cognitive skills are widespread across Europe. Faced with these challenges, public authorities are increasingly tempted to adopt various restrictive approaches, especially bans in schools. This is the case in **Hungary, Belgium, and the Netherlands**, while some organisations already advocate for it to be applied homogeneously across the EU. While these bans may be effective to address student’s focus during school hours, it should never prevent children from exploring the relational, social and informational benefits that digital technologies offer to them, which are also key to their development.

Recommendations

Based on the input from Eurochild members included in this sub-report, Eurochild calls Member States to:

1. Implement legislative and non-legislative actions to strengthen national prevention and protection of children from online harms by:
 - Developing **national strategies to enforce children’s rights with a comprehensive approach targeting or including online safety**, most notably the rise of child sexual abuse and cyberbullying;
 - **Ensuring a strong CSOs ecosystem capable of preventing and addressing online harm against children**, including through capacity building on awareness raising and support to victims, and empowering them to report and remove illegal and harmful content online. A good model in this regard is the establishment of Safer Internet Centers;
 - Ensuring **more effective support to children and families who are victims of abuse**, including psychological support. The Barnahaus model should serve as a reference for developing and implementing these programs;

²⁵ [Children’s Right Alliance](#) in Ireland.

²⁶ [Dutch NGO Coalition for Children’s Rights Utrecht University; Dynamics of Youth](#).

- Promoting the **collaboration of all stakeholders** to promote dialogue and find common solutions, including with public authorities and private actors (children, caregivers, teachers, government, law enforcement, industry, CSOs);
 - Establishing data collection mechanisms on online harms and access to victim support and conduct more research on children’s safety and conduct online – including through youth-led research;
 - Improving **access to digital devices and Internet connectivity** in poorer and rural regions, as well as among marginalised communities, and better equip and train caregivers of children with special needs and disabilities to promote safe online experiences;
2. Guarantee more effective provision of digital and media literacy for children and caregivers, including parents and teachers by:
- Developing **sustainable national initiatives on digital literacy and integrating media education in school** curriculum;
 - **Training parents and caregivers, including teachers, on digital literacy**, focusing on the prevention of child sexual abuse, cyberbullying, and privacy breaches, as well as fostering dialogue between adults and children;
3. Reinforce the regulatory framework at national level by advancing on the implementation of EU legislation and addressing online harms in a more comprehensive manner, including by:
- Enacting **targeted regulations addressing all forms of online harm against children**, including grooming, sextortion, AI- and self-generated CSAM and cyberbullying; and identify legislative gaps such as online gaming, gambling and commercial exploitation;
 - Ensuring the **implementation of existing EU regulations at national level** (GDPR, DSA, AVMSD), including through Online Safety Codes promoting safety-by-design and mandating the use of Child Rights Impact Assessments;
 - Working within the EU institutions to enhance **the accountability of online platforms at EU level**, including stricter controls on platform design, such as age assurance tools and child-friendly reporting tools, and harmful content detection and removal. Strong penalties should be enforced for companies that fail to comply with these obligations;
4. Ensure the voices and experiences of children are heard and taken into account in national policies for protecting children in the digital environment. The creation of youth panels or youth parliaments is a valuable model for this.

Summary

Across Europe, there is a shared need to improve legislative and non-legislative mechanisms to protect children from online risks. Firstly, **many children lack safe and sufficient access to the Internet**, creating and exacerbating pre-existing inequalities that particularly affect the most vulnerable children. Secondly, both **children and their caregivers often have inadequate education and digital literacy**, further exposing children to online risks, including the negative effects of excessive use, harassment or sexual abuse and exploitation.

To address these issues, it is crucial to **enhance prevention and education** efforts for both children and adults, by integrating digital education into school curricula and building the capacity of civil society to prevent online harms and support victims. Collaboration among civil society, public authorities and industry is key to leverage each other's expertise to implement sustainable and effective solutions.

However, **without appropriate legislation, prevention will always fall short**. Legislation must be clarified and strengthened to criminalise all forms of online abuse and exploitation, and mandate online platforms to put the appropriate safeguards in place for all online harms to children. To guarantee the rights of all children equally across Europe, legal solutions enacted at national level should be coherent with a harmonised approach across the EU.

At Eurochild, we remain committed to foster digital policy that respects and accounts for the full spectrum of children's rights while putting the best interests of the child at the centre, especially of the most vulnerable children. Supporting and empowering civil society is key to build the prevention capacity of the ecosystem at national level. Legislators at EU and national level must ensure holistic and effective legislative and non-legislative solutions that, based on children's views, build on the responsibility of online platforms to provide safe digital experiences to children.

For more information, contact:

Fabiola Bas Palomares

Lead Policy & Advocacy Officer – online safety

Fabiola.palomares@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