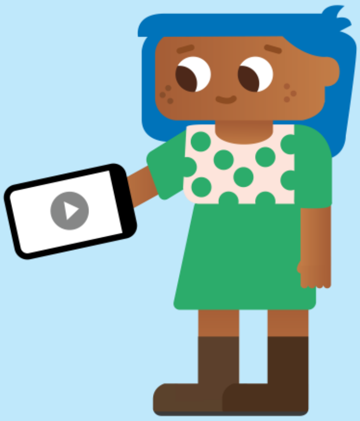
Children’s rights in the digital environment

Taken from “*Unequal Childhoods: Rights on paper should be rights in practice*” - Eurochild 2025 flagship report on children in need across Europe.



Eurochild
Putting children at
the heart of Europe

February 2026

Children’s rights in the digital environment

On 20 November, World Children’s Day, Eurochild released its flagship report titled Unequal Childhoods: Rights on paper should be rights in practice, which compiles information from 84 members across 36 countries in Europe. This sub-report synthesises evidence on children’s rights in the digital environment, with input from members from all countries.

Introduction

In the past years, the impact of digital technologies on children has received increased attention, given the implications on all the rights enshrined in the **United Nations Convention on the Rights of the Child**. Alongside practices and initiatives carried out by Eurochild members, European governments, and the EU itself, Eurochild members report ongoing and evolving risks for children. This reflects the challenges pointed out by the Committee on the Rights of the Child’s **General Comment No. 25** on children’s rights and the digital environment.

As highlighted in the OECD 5Cs typology, these risks can be linked to Content (harmful material), Contact (harmful interactions/grooming), Conduct (inappropriate behaviour such as cyberbullying/sexting), Commerce/Contract (financial scams, data exploitation, hidden costs), and cross-cutting. **These risks are worsened by gaps in platform accountability, inconsistent enforcement of existing rules, lack of ambition in ensuring strong legislation, and structural inequalities.**

EU legislative framework

The EU is a forerunner on children’s rights in the digital environment. Concerning the policy framework, the 2021 EU Strategy on the Rights of the Child sets out a comprehensive framework to upholding children’s rights, while the 2022 strategy for a Better Internet for Kids (BIK+), aims at ensuring children are protected, respected and empowered online in the new Digital Decade. The following legislation play a key role in protecting children’s rights in the digital environment:

1. Protection of children from crimes, including from child sexual abuse

The 2002 **ePrivacy Directive** protects the confidentiality of communication of “electronic communications services”. With the adoption of the **European Electronic Communications Code (EECC)**, which started to apply in late 2020, it expanded that concept to include many OTT messaging services (“number-independent interpersonal communications services”, like WhatsApp-style chat). Once covered by ePrivacy confidentiality, **voluntary Child Sexual Abuse (CSAM) scanning/reporting risked breaching those privacy rules** (since ePrivacy doesn’t contain a general exception for that).

In 2021, The EU adopted the temporary ePrivacy derogation **Regulation**, to allow limited, safeguarded voluntary detection and reporting of CSAM.[1] The derogation was subsequently extended until April 2026, and a proposal to extend it until April 2028 was presented in December 2025.

In 2022, the European Commission proposed a **Regulation to prevent and combat child sexual abuse**, which establishes a set of obligations for online service providers to detect, report and remove child sexual abuse material on their services. Negotiations on the proposal are still ongoing, with trilogues discussions having started in December 2025.

In parallel, in 2024, the European Commission proposed amendments to the **Directive combating the sexual abuse and sexual exploitation of children and child sexual abuse material**, in place since 2011, in order to reflect new technological developments affecting the manifestation of these crimes. Negotiations are progressing, with a focus on penalties, expanding the definition of child sexual abuse offences both offline and online and statutes of limitations periods, and introducing specific requirements for prevention measures and victims support.

In 2025, the JHA Council adopted a decision authorising the European Commission and EU Member States to sign the **United Nations Convention against cybercrime** (adopted by the UNGA in 2024). The Convention aims to harmonise the criminalisation of cyber-related offences among State Parties, strengthen international cooperation in the prosecution of such crimes, and ensure the safeguarding of fundamental rights.

The Council of the EU and the European Parliament have recently reached a political/provisional agreement to update the 2012 **Victims' Rights Directive**, which places stronger emphasis on children as victims of crimes. Under the revised framework, Member States are required to ensure child-friendly services, as well as appropriate support and protection for child victims.

The **Anti-Trafficking Directive**, revised in 2024, ensure early identification of child victims and guarantees specialised support. According to the Directive, Member States shall take appropriate measures, taking into account the specificities of the various forms of exploitation, such as education, training and campaigns, where relevant, with specific attention to the online dimension, to discourage and reduce the demand that fosters all forms of exploitation related to trafficking in human beings.

The 2024 **Directive on Violence Against Women and Domestic Violence** establishes comprehensive measures to ensure protection, support, and access to justice for those experiencing violence against women and domestic violence. The Directive also applies to several cyber-violence offences, including non-consensual sharing of intimate or manipulated material and cyber stalking, cyber harassment, cyber flashing, and cyber incitement.

[1] The 2025 report on its implementation gives an overview of the state of play on the implementation of the Regulation, based on the available data.

2. Online safety and platform accountability

The 2022 **Digital Services Act** (DSA), is one of the most important EU digital regulations that protect citizens from online harm. It places limits and obligations on online platforms, varying on the role, size and impact of the platform. It facilitates reporting and take down of illegal content from online platform, while promoting transparency regarding content moderation and recommendation algorithms, prohibiting the deception or manipulation of users. The DSA also bans targeted ads based on profiling where the platform knows with reasonable certainty the user is a minor.

It requires providers of online platforms accessible to minors to ensure high levels of privacy, safety and security, through a safety-by-design approach. Platforms have to identify specific risks to children and adopt measures to mitigate them. In this context, the **Guidelines on the Protection of Minors Online,** published in July 2025, support the DSA implementation by providing non-exhaustive examples of mitigation measures, including age-verification mechanisms. The providers of online services are also prohibited from using minors' personal data to target advertising.

The 2010 **Audiovisual Media Services Directive** (AVMSD) applies to services providing audiovisual content, including video-sharing platforms and video-on-demand platforms. It mandates EU Member States to ensure that platforms protect children from exposure to content that is likely to harm minors' physical, mental or moral development. It also protects minors from advertisements that might cause harm, prohibits audiovisual commercial communications for alcoholic beverages targeting minors, and promotes self-regulation through codes of conduct regarding advertisements of unhealthy foods and beverages.

The 2025 **EU Toy Safety Regulation** recognises that digital technologies create new hazards in toys and points to privacy, cybersecurity and fraud safeguards for connected toys. It also explicitly says safety assessment for digitally connected toys, when appropriate, should consider mental health risks and calls for "safety, security and privacy by design" in the best interests of children.

3. Data protection and privacy

The **2016 General Data Protection Regulation (GDPR)** provides for specific protection for children, as 'they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. When companies offering information society services process children's data, they should obtain explicit consent to process this data either from children themselves (if they are at least between 13 and 16 years old, depending on national laws) or from their parents or caregivers. The GDPR promotes clear and plain language when communicating with children about the processing of their data. Any information and communication with children in this respect should be 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.

The **European Digital Identity (EUDI) Regulation**, adopted in 2024, requires Member States to issue, by 2026, a European digital wallet. The wallet takes the form of an app that allows users to digitally identify themselves, and store and manage identity data and official documents. Very large online platforms that require user authentication to access their services would have to accept and facilitate the use of European digital identity wallets.

4. Emerging tech and commercial practices

The upcoming **Digital Fairness Act** would strengthen online consumer protection by curbing manipulative design and marketing (dark patterns, addictive features, harmful game mechanics, exploitative personalisation and influencer ads), and by fixing misleading pricing and unfair subscription/contract practices. Protecting children is flagged as a key cross-cutting priority throughout.

The **2005 Unfair Commercial Practices Directive** specifically prohibits exhorting children to buy advertised items or persuade their parents or other adults to buy advertised products for them.

The **2022 Digital Markets Act (DMA)** is the EU's law to make the markets in the digital sector fairer and more contestable. In order to do so, the DMA establishes a set of clearly defined objective criteria to identify "gatekeepers", large digital platforms providing the so called "core platform services", such as online search engines, app stores, messenger services. Gatekeepers will have to comply with the obligations and prohibitions listed in the DMA. The DMA is one of the first regulatory tools to comprehensively regulate the gatekeeper power of the largest digital companies.

The **2024 AI Act** sets uniform rules to create a single market for trustworthy AI applications that fully respect fundamental rights, including children's rights. It has entered into force and will apply in full from 2 August 2026, with certain transitional periods extending to 2 August 2027 for specific categories (notably high-risk AI embedded in regulated products). The act classifies AI systems as high risk for some areas of education, such as access or admission to education, systems to evaluate learning outcomes, assessment of educational levels, and detection of students' prohibited behaviour. General provisions will also benefit children once implemented, such as a requirement to watermark deepfakes and other AI-generated materials, and to inform children when they are interacting with AI.

Challenges faced by children in the digital environment

1. Child sexual abuse and exploitation

In Europe, one in five children become victims of child sexual abuse and exploitation,[2] and between 70% and 85% of child victims know their abuser. With 20.5 million reports and 63 million files of abuse submitted to the US National Centre for Missing and Exploited Children

[2] Child sexual abuse and exploitation[2] involves forcing or enticing a child to take part in sexual activities, whether or not the child is aware of what is happening. The activities may involve physical contact or non-contact activities. Child sexual abuse includes child sexual exploitation, which involves acts in exchange for something from a third party and/or the perpetrator.

(NCMEC)’s CyberTipline in 2024, the child sexual abuse crisis has reached an unprecedented scale.

Child sexual abuse material (CSAM)

On average, in 2024, an image, video or file containing child sexual abuse material (CSAM)[3] was shared every half a second. The European Union ranks the highest for hosting this content. Instances of child sexual abuse or violence have been flagged by members from almost all countries contributing to this report, and these phenomena are increasing in **Croatia, Cyprus, Estonia**, **France**, **Malta**, **Moldova**, **Portugal**, **Romania**, **Scotland**, and **Spain**.

In **Albania**, there was a rise in cases of child sexual abuse between 2023 and 2024, with 66% of cases involving girls. In **Ireland,** a 110% increase in the amount of CSAM identified online was recorded between 2022 and 2023. Our member in **Switzerland** reports that cyberbullying and online sexual harassment often escalate to online child sexual abuse. In **the Netherlands**, research shows that one in two children have been rexposed to online sexual abuse or inappropriate behaviour, particularly in platforms such as Snapchat, Instagram and WhatsApp. 37% of the affected children never disclosed the harm, and only 4% reported it to the police.

Similarly to other countries in the Balkans, there is the risk that **Bosnia and Herzegovina** may be a significant point on the CSAM trafficking route, due to its limited law enforcement resources, a lack of robust child protection measures and under-resourced child protection systems.

AI-generated CSAM

While, according to NCMEC, AI-generated CSAM reports have increased by 1000% from 2023, in the first half of 2025, the Internet Watch Foundation analysts recorded a 400% increase in AI-generated child sexual abuse imagery. 3,440 AI videos of child sexual abuse were discovered by the Foundation in 2025, marking a 26,362% increase compared to the previous year, where only 13 such videos were found. 65% of these video were classified as representing the most severe types of abuse. In 2024, **the Netherlands** identified 1,472 images that were partially or totally AI-generated child sexual abuse content.

The **non-consensual sharing of intimate images online** represents another form of child sexual abuse, and can be perpetrated both by peers and adults coming in contact with children. The practice is increasingly facilitated by technological developments, including “nudify applications” and artificial intelligence. Members in **Albania**, **Belgium**, **Croatia** and **Italy** have flagged this as a growing concern.

[3] Child sexual abuse material is any image or video showing the sexual abuse or exploitation of a child or any representation of the sexual parts of a child for primarily sexual purposes. CSAM can also be generated by means of technology, meaning the production, via digital media of any kind, of child sexual abuse material and other wholly or partly artificially or digitally created sexualised content of children.

Grooming

Child sexual abuse can also manifest itself as grooming.[4] In 2024, the National Center for Missing & Exploited Children reported a 192% increase in online grooming compared to reports in 2023.

In **Belgium**, cases of grooming are growing, with victims reported to be as young as 12 years old and, in some cases, even younger. In **Italy**, there is a steady increase in cases related to online grooming, especially among younger children. A 2023 national survey in **Malta** found that among 387 children, 9% of children aged 7 to 10 reported chatting with strangers online, increasing risks of grooming. In **Romania** the normalisation of sexual exploitation in vulnerable communities has been observed, along with increased online recruitment and a rising number of cases involving boys.

Online harassment, **and sexual extortion**[5] have become more common. In **Serbia**, a 2022 report highlighted the existence of **Telegram groups sharing explicit content**, including material involving minors, prompting investigations by Serbia's Special Prosecutor's Office for High-Tech Crime.

2. Online safety and platform accountability

There is a gap between children's rights standards and the lived realities of many digital services. Rather than being safe by design, children's online experiences are frequently shaped by engagement-driven systems, opaque design choices, and uneven enforcement. The insights shared by Eurochild members highlight the need to prevent and tackle the negative effects of the digital environment on children.

Excessive time spent in the digital environment

While screens have the potential to help people get informed and learn content and skills and it is important to have an approach which focuses more on the quality of the time spent in front of screens rather than the quantity, excessive screen time is a common concern among Eurochild members. Several inputs highlight growing concerns about **excessive or problematic digital use**, which has negative consequences on sleep, concentration, anxiety, low self-esteem, or wider mental health impacts, alongside calls for better evidence and monitoring.

In **Bulgaria**, 17% of children experience problematic levels of time spent on digital devices, while 26% are intensive users, almost continuously online. In **Switzerland,** 30% of children report feeling stressed by social media, and in **Czechia** many children display fear or anxiety of being without mobile phone or being unable to use it (nomophobia). In **Hungary**, children spend on average 85.7 minutes per day in front of a screen. Eurochild members in **Denmark**,

[4] Grooming is the process of establishing/building a relationship with a child, either in person or through the use of the internet or other digital technologies, in preparation for abuse, including sexual abuse, exploitation and radicalisation. Grooming for sexual purposes is also referred to as sexual solicitation.

[5] Sexual extortion is the blackmailing of a person with the help of sexualised images of that person in order to extort sexual acts or material, money, or other benefits from them under the threat of sharing the material without the consent of the depicted person (e.g. posting images on social media).

Malta and **Portugal** express concerns about the increasingly young age at which children start engaging with social media, as well as the growing number of children demonstrating problematic internet use. **Stalking and cybercrime** are the main dangers for children online in **France**.

Exposure to harmful content

Children can be unexpectedly and unintentionally exposed to content that potentially harms them, including hateful content, harmful content, illegal content and disinformation. These types of content are widely considered to have serious negative consequences on children's mental health and physical wellbeing, for example as a result of content promoting self-harm, suicide, eating disorders, misogynistic content, or extreme violence. These also include legal but non-age-appropriate content, such as pornography and gambling. Instances of harmful or inappropriate content have been flagged by members in **Croatia**, **the Netherlands**, **Turkiye**, **Ukraine** and **Wales**.

In **England**, boys aged 11–14 are exposed to harmful content within 30 minutes of being online, with 79% encountering violent content. In **Greece**, 34% of elementary school children and 61% of middle and high school children reported having seen harmful or inappropriate content online, 60% of which occurred by accident. Children in **Scotland** report significant concerns about AI-generated material, misogynistic content and extremely violent content.

While members in **Austria** highlight concerns linked to children's exposure to toxic role model, including toxic masculinity, in **Belgium**, emerging risks include toxic masculinity online and its impact on children's understanding of gender roles.

In **Luxembourg**, there has been **increasing exposure to age-inappropriate content on social networks**, **particularly from influencers**. Controlling the use of content depicting children is difficult and there is also a lack of parental awareness of the risks.

In **Luxembourg** and **Spain** there are concerns about the link between the **exposure of minors to pornography** and the increase in sexual violence between minors. At least half of the children aged 12-17 in **Estonia** have encountered sexual content online.

Cyberbullying

Between 13% and 29% of 15-year-old students across different EU Member States report being frequently bullied, including falling victim of cyberbullying.[6]

Members in **Croatia**, **Cyprus**, **Hungary**, **Luxembourg**, **Moldova**, **Romania**, **Scotland** and **Sweden**, report a worrying increase in cyberbullying, with children acting both as victims

[6] Cyberbullying involves the posting or sending of electronic messages, including pictures or videos, aimed at harassing, threatening or targeting another person. Although currently there is no EU-wide definition of cyberbullying, the European Commission will adopt an Action Plan against Cyberbullying in early 2026. Eurochild contribution to the open consultation can be found here.

and perpetrators. The frequency of cyberbullying and harassment appears high, and girls and adolescents from single-parents families are among the most targeted groups.

In **Denmark,** one in ten children aged 11-15 years old is subjected to digital bullying very often, often, or occasionally, and in **Estonia** 19% of children in the same age range experienced cyberbullying at least once in the last few months. **Latvia** highlights the severe impact that positing online with the purpose of publicly humiliating someone has on children's mental health and wellbeing. **Ireland** notes that while girls are primarily targeted by harassment and verbal abuse on social media, boys are more often victimized on gaming platforms. In **Switzerland**, 29% of adolescents reported experiencing online sexual harassment in 2022, up from 19% in 2014, with girls particularly affected. **Cyberbullying and online sexual harassment** often overlap and can **escalate into online child sexual exploitation and abuse**.

3. Data protection and age verification

Violations to the right of privacy and identity is an area of concern. In **Hungary** and **Turkiye**, members highlight the lack of safeguards for the protection of children's personal data and insufficient restrictions on publicly accessible information. In **Italy**, there is an urgent need for regulatory frameworks to safeguard children's data, image rights, and consent in the digital sphere. In **Sweden**, an increasing number of children report that their **private images are being shared without consent and manipulated using artificial intelligence (AI).** These altered images are often **combined with falsehoods and rumours**, and their rapid spread contributes significantly to **children's distress**.

Sharenting and childfluencers/kidsfluencer

Eurochild members are particularly alarmed by the phenomena of **sharenting**[7] and **childfluencers**[8] due to their major implications for privacy and child protection, often in a regulatory grey zone and with inconsistent safeguards.

These risks are recognised as particularly alarming by many Eurochild members, notably in **Cyprus**, **Germany**, **Hungary**, **Ireland**, **the Netherlands** and **Sweden**. In **Greece**, the sharing of children's personal data and photographs on the internet by adult caregivers is widespread. In **Slovenia** families frequently post images of their children in promotional contexts, such as advertising products or destinations. In **Italy**, **Malta** and **Romania** increasing attention is being paid to the protection of children's digital rights, safety, and privacy, in light of the rise of childfluencers. Sharenting and childfluencers have emerged as causes for investigation in **Ireland**, raising concerns about children's privacy and safety, child labour, and questions of

[7] Sharenting refers to parents sharing large amounts of potentially sensitive content about their children on social media, especially when done by an account with a large following. This commercialisation of children's images and identities online raises questions of consent, dignity, safety, and exploitation.

[8] The phenomenon of 'childfluencer' or 'kidfluencer', consists of children who have gained a considerable online following by creating content on social media channels, it is often linked to advertising, and in most cases managed and guided by their parents.

consent. In a joint British-Irish study, this area has been described as a 'legal lacuna', unregulated within any child labour, privacy, consent or online safety laws.

Although these issues remain largely unregulated in many countries, some are beginning to explore legislative or policy responses. In **Belgium**, a new bill aimed at regulating sharenting is currently under discussion in Parliament.

4. Emerging tech and commercial practices

Artificial Intelligence

There are growing concerns about the misuse of emerging technologies, including AI, in **Belgium**, **Czechia**, **Germany**, **Greece**, **Italy**, **Malta**, **the Netherlands**, **Scotland**, **Serbia**, **Spain**, **Sweden** and **Switzerland**.

Not only are these countries concerned about the use of AI to facilitate child sexual abuse material, but they are also worried about the impact of AI on a wide range of children's rights. Broader impacts might include bias and discrimination, profiling, and the use of AI in recommender systems that can intensify exposure to harmful content. For these reasons, German Children's Fund is conducting a study on the interlinkages between AI and children's rights, and another on the use of biometric data of children in AI training and children's right to privacy.

Online gambling

Online gambling and gambling-like features are seen as a significant child rights concern in **Austria**, **Hungary**, **Malta** and **Serbia**. These risks are linked to addictive design, unwanted spending, and exposure to age-inappropriate commercial content.

In **Italy,** online gaming and gambling platforms are reported to facilitate grooming and foster risky behaviour. In **Portugal**, an increasing number of children and young people are engaging in online gambling for money. Similar concerns are raised in **Switzerland**, where youth gambling is so widespread that nearly half of Swiss young people report having gambled.

Gaming and advertising

Many games and gaming platforms might expose children to risks, from harmful contact and harassment to addictive design and gambling-like monetization, undermining children's rights to protection, privacy, health and safe participation. These concerns are mentioned by numerous members, including in **Belgium**, **Cyprus**, **Hungary**, **Italy**, **Portugal** and **Scotland**.

In **Bulgaria**, there are calls for a comprehensive analysis of screen and gaming-related addictions. In **Ireland** a study found a strong correlation between gaming and gambling. In **Switzerland**, in 2018, 8.5% of 12- to 19-year-olds were problematic internet users, and among them, video games seem to be responsible in 13% of cases. In **Ukraine**, the growth of online gaming has also created opportunities for potential grooming and exposure to inappropriate behaviour.

In **Belgium**, online gaming, and the combination with social features, advertising and AI is an emerging risk, especially as it is often unclear under which legal framework online games are regulated. In **Spain** these concerns are also linked to the advertising of unhealthy products targeted at children.

5. The digital divide

Members from nearly all countries have described the extent of the digital divide, which is the unequal access to and effective use of digital technology, encompassing four interrelated dimensions: motivational, material, skills, and usage access. Inequalities are driven by income, education, migration background, geography (rural/remote), disability, and family context.

More recently, the **Outcome document** of the High-Level Meeting of the United Nations General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society, published in December 2025, further reinforced this focus. The document recognises that children are among the most active users of the Internet, while also acknowledging the significant challenges they face. It states that "*the benefits of digitalization are not yet available to many children and young people as a result of inequalities in connectivity, digital literacy, equipment, skills and educational facilities (para 37)*"

Children in vulnerable situations, including children in poverty, children in care, children with disabilities, and children with a migrant background and ethnic minority origin and children living in rural areas are repeatedly identified as most affected.

In **Cyprus,** less than half the population (49.5%) had at least a basic level of digital skills in 2023, which is below the European Union average of 55.6%, and the digital divide persists across age groups. In **Albania**, the digital divide particularly affects children living in rural areas, where infrastructure is limited and schools lack basic technologies. Despite widely available internet coverage and digital services, in **Estonia**, **Slovenia** and **Turkiye**, economic barriers, lack of digital skills, inadequate inclusive solutions for vulnerable children and language gaps persist. Around 40% of eighth-grade pupils in Germany demonstrate only basic digital skills, with those from low education or migrant families particularly affected.

In **Czechia,** the children most affected by the digital divide are those living in socially excluded areas. In **Croatia** and **Italy** disparities affect children from poor families, living in rural areas, migrant children, children with developmental difficulties and children in out-of-home care. In **Serbia** 35% of households in Roma settlements lack internet access at home, and only 15% have computers or tablets. In **the Netherlands**, digital skills are highly dependent on parental education. According to the Basic Education Act, in **Finland**, all learning materials, as well as tools required for it, are free of charge. However, in practice there are differences in the digital devices that pupils use, as some families can afford more advanced equipment than others.

Nevertheless, initiatives to tackle these needs have been put in place. In **Austria**, the initiative *Broadband Austria 2030* seeks to bridge the urban-rural digital divide, supporting children's digital rights and inclusion. In **England**, through the 2025 initiative "*ON*", schools across the country are given free access to educational materials and peer-to-peer programs, alongside resources for youth clubs and families. **Malta** has launched the Digital Decade Strategic Roadmap 2023–2030, prioritising digital skills for vulnerable groups, and the Digital Education Strategy 2024–2030, on equality and inclusion.

Good practices and initiatives

Several countries reported positive initiatives and services aimed at strengthening online safety and protecting children's rights in the digital environment.

1. Legislative and policy initiatives

- In **Slovenia** and **Hungary**, recent legal amendments have introduced restrictions on children's use of smart devices in schools.
- In **Belgium**, a new bill to regulate sharenting is being discussed in the parliament. Additionally, in 2023 the Belgian government voted to fund a national coordination centre for the online safety of children, although this needs to be operational and properly funded.
- In **Germany**, a 2021 amendment to the Youth Protection Act introduced the concept of "personal integrity", requiring media self-regulation bodies to review their tools to include, beyond content risks, also contact, conduct, data safety and security.
- In **Hungary**, the Child Protection Act explicitly states that children have the right to receive education and training that supports a responsible use of the internet and digital media.
- The **UK** Online Safety Code seeks to address harmful and illegal content on video-sharing platform services.
- **Ireland** has introduced an individual complaints mechanism, although this has not been implemented yet.
- In **Latvia**, Article 50 of the Law on the Protection of the Rights of the Child prohibits providing children with access to harmful content; however, there are currently no sanctions in place for violation limiting its effectiveness.
- In **Switzerland** the Digital Trust Label evaluates digital services in terms of transparency, privacy, and child data protection, currently focusing on companies.
- **Greece** is introducing a "Kids Wallet" age-verification tool to protect children online, though civil society organisations have raised concerns that it may introduce new risks and privacy-related challenges.
- In **Spain** and **Turkiye**, draft legislations on the protection of minors in the digital environment are under development.

2. Initiatives promoted by the institution

Numerous initiatives to uphold the rights of children in the digital environment are being carried out by European countries:

- In 2024, the European Commission-funded *Digital Children project* in **Bulgaria** (which supports safenet.bg) organised **educational initiatives on online safety for 27,000 children**, **trained over 100 young people, over 1,000 parents and 797 teachers.**
- In **Belgium**, the Flemish government has invested in media and digital literacy, but initiatives should be scaled up and more efforts are needed to reach children in vulnerable positions.
- In **Czechia**, the project *Don't Create Digital Footprints for Children*, co-led by the police, aims at preventing sharing of children's personal information through sharenting.
- In **England**, in 2025, *ON* was launched — a comprehensive initiative aimed at strengthening digital literacy and promoting the well-being of children and young people. Schools across the country are given free access to educational materials and peer-to-peer programes, alongside resources for youth clubs and families.
- In **Moldova** the Ministry of Education and the Office of the Ombudsman delivered training for teachers on the use of digital technologies and to create interactive and effective learning experiences. They also organised school-based activities to raise children's awareness of their fundamental rights.
- In **Hungary, the National Media and Infocommunications Authority launched a nationwide campaign**, *Dare to Ask for Help*, to enable parents and children to recognise online abuse and seek help.
- In **Ireland**, *Media Literacy Ireland*, launched by the Media Regulator, provides educational resources to help young people, teachers and caregivers to better understand children's rights in the online sphere. The Irish Internet Safety Awareness Centre provides information and resources for schools and families on online safety. Its Webwise Youth Panel provides young people with the opportunity to share their views and inform policymaking at national and European levels.
- In **Portugal** the judiciary police developed the *Rayuela Project,* a videogame designed for students aged 10 to 15 to prevent cybercrime.
- In **Serbia** the *GovTech* programme funds innovative digital solutions for public sector challenges, while the Digital Serbia Initiative promotes AI and digital skills.
- In **Switzerland,** the project *Clickandstop.ch* allows users to report child sexual abuse material anonymously, linking reports directly to law enforcement and hotline networks.

Safer Internet Centres across countries play a crucial role in prevention, awareness-raising, and the implementation of child safety initiatives. These include:

- In **Albania**, the *NetSMARTkids* campaign, co-financed by the European Union and CRCA-ECPAT Albania, in partnership with ALO 116 Albania and iSIGURT.al, was launched in 2025, reaching over 7,400 pupils and 600 parents and teachers across

170 schools nationwide, and aiming to enhance digital literacy and promote safer online environments for children.

- In **Cyprus**, the Safer Internet Youth Panel enables children to express opinions and exchange knowledge and experiences on the creative and safe use of the internet and digital technologies.
- In **Croatia**, the Centre for Safer Internet provides free and anonymous services such as helplines and education on online safety through workshops, lectures and school programmes for children, parents, and professionals.
- In **Latvia**, the Safer Internet Centre developed an online self-help tool in 2022.
- The Centre in **Romania** runs a 24/7 hotline allowing anonymous reporting of abusive material, grooming, hate speech and disinformation.

3. Initiatives carried out by Eurochild members

Eurochild's members are actively engaged in protecting children's rights in the digital environment through concrete initiatives.

- In Albania, **the platform iSIGURT.AL** provides children, parents, and educators with the possibility to report cases of online child sexual exploitation and abuse, cyberbullying, and other online harm. It offers timely **responses, assistance, and referrals to law enforcement and child protection agencies**, and plays a crucial role in **raising awareness** about online safety and promoting responsible internet use.
- In **Estonia**, the Estonian Union for Child Welfare operates a free hotline, enabling the public to report child sexual abuse material anonymously.
- In **Germany**, the German Children's Fund published a legal opinion outlining cases that may infringe personal rights and endanger children's well-being, and proposes a graduated consent model that limits parental decision-making and considers the child's age and capacity.
- In **Italy**, Telefono Azzurro provides integrated helpline and online reporting services, combining psychological support with referral to authorities in cases of online abuse. It also calls for the extension of digital literacy programmes in schools and stronger collaborations with technology companies.
- **Two tools by The Smile of the Child seek to protect children in the digital world.** The first is a **training programme, Safe and Creative Internet Browsing**, intended to enhance children's critical thinking and responsibility in the digital world. The second is the **Children's Online Redress Sandbox**, which aims to create a standardised blueprint for online redress mechanisms. Young people will participate as equal experts in its co-design and are an integral part of the project.
- In **Scotland** the Children's Parliament has collaborated with the Scottish AI Alliance and the Alan Turing Institute to develop 12 calls to action to ensure that their human rights are upheld in the development and use of AI.
- In **Malta**, the Malta Foundation for the Wellbeing of Society not only developed the *P.O.P.-Up project*, but also partnered with the United Nations International Telecommunications Union to train over 115 psycho-social professionals across the

education sector and in cooperation with the police cybercrime unit, delivered specialised training to 26 officers.

Recommendations

1. Protect children from child sexual abuse and exploitation

- Adopt and implement without delay a comprehensive, long-term and robust Regulation to prevent and combat child sexual abuse, and ensure the extension of the temporary ePrivacy derogation while negotiating for a permanent framework to detect, report and remove child sexual abuse material. Ensure a strengthening of the current Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material.
- Ensure a prevention-first, victim-centered approach aligned with the Victims' Rights Directive and the revised Anti-Trafficking Directive, including child-friendly services and safe referral pathways.
- Support the enlargement countries in aligning with all legislation linked to children's rights in the digital environment, with a specific focus on those protecting them from child sexual abuse and exploitation.

2. Make platform accountability work for children in practice

- Use the Digital Services Act and the Guidelines on the Protection of Minors Online to require platforms, especially very large platforms, to implement safety-by-design defaults for services likely to be accessed by children, including high-privacy settings, reduced exposure to harmful content, friction against harmful contact (including grooming).
- Ensure child-friendly reporting, complaint handling and redress, with trauma-informed processes.

3. Tackle addictive and manipulative design and harmful commercial practices

- Ensure the Digital Fairness Act explicitly addresses children's risks from dark patterns, addictive engagement features, harmful personalisation, coercive subscription journeys, exploitative game mechanics, and influencer marketing, banning or strictly restricting the most harmful practices for minors.
- Apply the Unfair Commercial Practices Directive to strengthen protections against commercial pressure on children, and ensure the revised Audiovisual Media Services Directive protects children from harmful audiovisual content and problematic advertising practices (including exposure to age-inappropriate commercial content).

4. Guarantee children’s privacy and data protection

- Ensure that current simplification efforts do not weaken children’s protections under the GDPR. Ensure age assurance mechanisms are effective, inclusive, and respect children’s rights. The development of a public, rights-based approach to age assurance will build on the EU Digital Identity Wallet, once it is fully implemented and proven to work effectively.
- Raise awareness around the issues of sharenting and childfluencers, protecting children’s privacy, dignity and protection from exploitation, and clarifying responsibilities for parents/guardians, platforms, advertisers and agencies.

5. Protect children from harms linked to AI and other emerging technologies

- Ensure that current simplification efforts do not weaken protections under the AI Act, and implement it in a way that meaningfully protects children, including robust risk management for systems affecting education, opportunities and access to services, and strong transparency around AI-generated/manipulated content.
- Apply the Toy Safety Regulation to connected products used by children, safety, security and privacy by design, and mental health considerations where relevant, to prevent emerging risks from digitally connected toys and similar products.

6. Close the digital divide as a children’s rights issue

- Invest via the European Child Guarantee, and the next Multiannual Financial Framework to address unequal access to devices, connectivity, accessibility, skills and meaningful use, prioritising children in vulnerable situations.
- Embed digital, media and privacy literacy in curricula and professional training (education, child protection and social services), including skills to recognise manipulation, misinformation, grooming and privacy risks.

7. Strengthen evidence, enforcement and participation

- Invest in child-rights-based research (including longitudinal work on social media, gaming and AI impacts), with disaggregation that reflects inequalities and intersecting risks.
- Improve enforcement capacity and coordination across regulators (digital services, data protection, consumer, audiovisual and gambling regulators), addressing the gap between standards on paper and children’s lived realities.

For more information, contact:
Francesca Pisanu
EU Advocacy Officer, Eurochild
francesca.pisanu@eurochild.org

Sofia Montresor
Policy & Advocacy Intern – Online Safety, Eurochild
sofia.montresor@eurochild.org

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

ANNEX A: Trends identified across Eurochild members

	CSAM	*Grooming*	*Excesive time online*	*Harmful content*	*Cyber bullying*	*Online hate speech*	*Share Nting*	*Child fluencers*	*Privacy and data protection concerns*	*Misuse of AI*	*Online gambling*	*Risks in gaming platforms*	*Digital divide*
AL	■		■				■	■					■
AT	■		■	■	■	■		■		■		■	■
BE	■	■	■	■	■	■		■	■		■	■	
BA	■	■						■				■	
BG									■		■		■
HR	■		■			■		■				■	■
CY	■				■		■	■			■	■	■
CZ		■	■			■		■	■			■	■
DK							■	■	■			■	
GB-EN	■		■			■						■	
EE	■						■	■					■
FI													■
FR	■	■											
DE		■		■	■							■	■
EL	■	■	■	■	■	■	■	■				■	
HU				■			■	■	■	■	■	■	■
IR	■			■	■	■	■	■			■	■	■
IT	■	■	■	■	■	■		■	■	■	■	■	■
XK	■											■	■
LV	■					■	■	■					■

LU								■				■	■
MT		■		■	■	■	■	■	■	■		■	■
MD	■						■	■				■	■
NL	■	■		■	■	■						■	■
PL						■							■
PT	■								■	■	■	■	■
RO	■		■	■	■		■	■				■	■
GB-SCT	■	■				■	■	■	■		■	■	■
RS	■	■				■	■	■	■	■		■	■
SI	■			■	■		■	■	■			■	■
ES	■	■	■			■	■	■					
SE	■	■				■		■	■				
CH	■	■				■	■	■	■		■	■	■
TR	■					■	■	■	■			■	■
UA	■		■			■		■	■			■	■
GB-WLS						■						■	■