

Protecting children online

Selected EU, national and regional laws and initiatives

SUMMARY

The internet has become an integral part of children's lives, offering a wide range of opportunities for learning, exploring, informing and interacting with others. However, this increased online presence also exposes children to numerous risks, including cyberbullying, fraudulent marketing practices, and sexual abuse and exploitation. The scale of these problems is alarming, with a significant proportion of children experiencing online harm every month. Furthermore, the rise of generative artificial intelligence is facilitating some risks, such as the creation and dissemination of convincing but false information.

To address these challenges, the EU has implemented a range of laws and initiatives aimed at protecting children online, while enabling them to explore the digital space and fulfil their potential. These measures include regulations on digital services, audiovisual media services, data protection, and practical tools such as helplines and hotlines to report harmful or illegal content online. In addition, the EU has introduced a digital identity framework, which aims to offer a secure and reliable way to verify age, to prevent children from accessing age-inappropriate content.

National and regional governments are also taking steps to protect children online, with many countries introducing age limits and age verification systems. Some countries or regions have banned smartphones in schools, while others are promoting awareness-raising campaigns and educational programmes to teach children and parents about online safety. Civil society organisations and international bodies are also promoting child online safety, through initiatives such as research, awareness-raising campaigns, and support services.



IN THIS BRIEFING

- Introduction
- EU strategies and declarations protecting children online
- EU laws protecting children online
- National and regional laws and initiatives protecting children online
- Awareness-raising efforts
- Way forward



Introduction

The internet has become an integral part of children's lives, offering many opportunities to learn, create, play, explore, inform and interact with others. [Children](#) are spending more time online than ever and going to the internet sooner. However, this growing and earlier online presence also exposes children to risks to their safety, wellbeing and development. These risks include cyberbullying, dis- and misinformation, promotion of unhealthy habits, and sexual exploitation.

According to the [EU Kids online 2020 survey](#), carried out among children aged 9 to 16, about 1 in 10 children becomes a victim of cyberbullying every month. An equal number of children say they never feel safe online. On a global scale, [Unicef](#) states that 'more than a third of young people in 30 countries report being cyberbullied, with 1 in 5 skipping school because of it'. A 2021 [WeProtect survey](#) found that over half of young people had experienced some form of sexual harm online in their childhood. Girls are particularly vulnerable to online sexual harms, with 7 in 10 girls who responded to the WeProtect survey stating they had received sexually explicit content from an adult, compared with 4 in 10 boys.

Children are vulnerable to misleading or fraudulent [marketing practices](#), which can lead to the exploitation of their personal data for tracking, profiling and targeting. Connected (smart) toys may also pose privacy, security and safety risks, as they often come with a capacity to reveal the location of the user, record conversations and communicate with children remotely. In addition, many digital services are designed in a way that keeps users in the platform as much time as possible, raising concerns about [addiction](#) and long-term effects on physical and mental health.

[Generative artificial intelligence](#) is also facilitating some of these [risks](#), including cyberbullying, [grooming](#) and online child sexual abuse. Children are more vulnerable to AI-generated convincing but false information or [dangerous advice](#), as their cognitive capabilities are still developing.

Sometimes, children are put at risk by their own parents. Many parents share publicly the details of their children's lives online, a phenomenon known as '[sharenting](#)'. According to 2020 [survey](#) among Czech and Spanish parents, more than 9 in 10 parents share their child's full name, and almost 7 in 10 have shared a picture of their child's face. For instance, 3.5 % of Czech parents admitted having shared online a photo of their naked child. This can potentially lead to dangerous [situations](#), such as reusing these images on pornographic websites or paedophile networks. Sometimes, parents are not at all aware of these risks. For example, [interviews](#) carried out by researchers among some Estonian mothers indicate that they are not at all concerned about sharing publicly information about their children on social media, and do not consider the potential risks to privacy.

Children's [own conduct](#) can also increase online risks. Children can use the online environment to overshare their personal details, post hateful or harmful content or participate in dangerous online challenges. [Sexting](#) is another example of user-generated behaviour that may put children at risk of self-produced child pornography material being spread.

EU strategies and declarations protecting children online

To frame the EU action aimed at protecting children online, the EU has adopted various declarations and strategies. The [European declaration on digital rights and principles](#) emphasises the importance of helping children 'to make safe and informed choices and express their creativity in the digital environment'. The declaration calls for promoting positive experiences in an age-appropriate and safe digital environment that protects children against harmful and illegal content, exploitation, manipulation and abuse online. It also highlights the need to provide all children with opportunities to acquire the necessary skills and competences in order to navigate and engage in the digital space actively and safely. Finally, it encourages the involvement of children in the development of digital policies that concern them. The importance of involving children in the development of legislation, policies, programmes, services and training on children's rights in the digital world is also highlighted in the [General Comment No. 25 \(2021\)](#) of the United Nations Committee on the Rights of the Child.

The aim to protect, empower and respect children online is highlighted in the [Better Internet for Kids \(BIK+\) strategy](#), which the European Commission published in 2022. The strategy aims to create a safe, diverse, inclusive and non-discriminatory digital space in which children can thrive and fulfil their potential. It is built around three topics: safe digital experience, digital empowerment and active participation. The BIK+ strategy gives an overview of concrete measures and projects the Commission supports. For example, the Commission co-funds the safer internet helplines and hotlines that help minors when confronting harmful or illegal content online. The Commission also organises media literacy campaigns and develops awareness-raising tools and activities.

In 2021, the Commission put forward a general [strategy on the rights of the child](#). The strategy recognises both the potential benefits and the harms of the digital environment for children. It outlines the key actions the Commission plans to take in order to provide children with better protection online, such as facilitating a child-led process aimed at developing a set of principles to which online industries must adhere. The strategy invites EU Member States and the industry to take action – for example, to ensure equal access to digital tools or to give children and parents adequate tools to control their screen time.

EU laws protecting children online

The EU has adopted numerous regulations and directives that contain articles aiming to protect children online. These include the Digital Services Act, the General Data Protection Regulation, the Audiovisual Media Services Directive and various regulations protecting consumers in the EU. While being important, their enforcement remains a challenge, as it requires many resources at various levels and cooperation between EU institutions, Member States authorities, organisations defending children's rights, and various experts. In addition, the evolving nature of technology poses additional difficulties in keeping the regulatory framework up to date.

Digital Services Act

The [Digital Services Act](#) (DSA)¹ is one of the most important EU digital regulations that protects citizens, including minors, from online harm. The DSA places limits and obligations on various digital services, including social media platforms, with rules varying according to the role, size and impact of the online platform. The DSA makes it easier to report and take down illegal content from online platforms, with complaint systems required to be easy to access and user-friendly. The DSA also promotes transparency regarding content moderation and recommendation algorithms, prohibiting the deception or manipulation of users to prevent them from making free and informed choices.

The DSA includes several provisions specifically targeting the protection of minors. The providers of online platforms are required to take measures to ensure a high level of privacy, safety and security of minors. They have to explain how to use their services in a way that minors can understand. In addition, the providers of online services are prohibited from using minors' personal data to target advertising, a step towards protecting minors from exploitative marketing practices. The European Commission is expected to publish, before summer 2025, [guidelines](#) on protection of minors online under the DSA.

[Enforcing](#) the DSA remains challenging. Enforcement is shared between national authorities and the Commission. The [Commission](#) has reportedly stated that enforcing the DSA for children is a priority. However, national enforcement of the DSA remains limited. Several EU Member States have delayed the designation and/or empowerment of their digital service coordinators who are responsible for the application and enforcement of the DSA in each country. The lack of [sufficient staff](#) is also sometimes a challenge.

The Commission has reportedly taken more than [60 enforcement actions](#) since the DSA entered into force in 2022. These range from requests for information to opening formal proceedings. For example, in [May 2024](#) the Commission opened formal proceedings to assess whether Meta, the provider of Instagram and Facebook, has breached the DSA regarding the protection of minors. One

of the aspects investigated was whether Facebook and Instagram exploit the weaknesses and inexperience of minors and cause addictive behaviour. The Commission was also concerned about whether Meta complies with the DSA requirements regarding age verification tools and default privacy settings for minors.

Recently, there have been tensions between the EU and the United States (US) over the enforcement of the DSA. Some Members of US President Donald Trump's administration (such as [US Vice-President J.D. Vance](#)) and some Members of Congress (such as [US Republican congressman Jim Jordan](#)) have accused the DSA of censorship. The Executive Vice-President of the European Commission, [Henna Virkkunen](#), has responded to these claims by recalling that 'the DSA does not regulate speech'.

One of the impacts that the DSA has had in protecting minors is the successful [withdrawal of the TikTok Lite app](#) from the EU. The app offered rewards, including gift vouchers, for performing certain tasks such as watching videos or liking content. The app was deemed particularly worrying because of its addictive design. The suspension of the TikTok Lite app demonstrates the DSA's potential to hold online platforms accountable for their practices and to prioritise the protection of minors online.

General Data Protection Regulation

The [General Data Protection Regulation](#) (GDPR)² stipulates that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. Such protection should apply, for example, when personal data is used for marketing or profiling purposes.

According to Article 8 GDPR, 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. As seen from Figure 1 below, several EU Member States have used the possibility to lower this age limit to under 16 years of age.

The GDPR promotes [clear and plain language](#) when communicating with children about the processing of their data. According to Article 12 GDPR, any information and communication with children relating to data processing should be 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. This is particularly important to ensure that children effectively understand what is happening with their personal data.

The GDPR is also applied in the context of sharenting. The GDPR gives data subjects the right to request the deletion of their personal data under certain conditions – for example, where the information is no longer necessary for the original purpose, where consent has been withdrawn, or where the personal data processing is unlawful. In practice, however, it might sometimes be difficult for children to apply this right. In a 2024 article, [G.F. Lendvai](#) gives an example of under 13-year-old children whose parents share pictures of them on Facebook. These children do not yet have a right to open an account on Facebook. Presumably, they also do not have the financial resources to hire a lawyer, and their parents might not agree to take down the pictures.

Audiovisual Media Services Directive

The [Audiovisual Media Services Directive](#) (AVMSD)³ protects minors from harmful content as well, including from harmful advertisements. The AVMSD applies to all services with audiovisual content, including video-sharing platforms and video-on-demand platforms such as YouTube and TikTok. It requires EU Member States to ensure that these platforms take measures to protect minors from content that might be harmful for their physical, mental or moral development.

The directive encourages establishing effective reporting, age-verification, parental-control and content-rating systems. The most harmful content, such as pornography or gratuitous violence, should be subject to the strictest access control measures. The AMSD leaves Member States the

flexibility to define harmful content. Moreover, the AMSD protects minors from advertisements that might cause them mental, moral or physical harm. It prohibits advertisements that

- 'directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity;
- directly encourage them to persuade their parents or others to purchase the goods or services being advertised;
- exploit the special trust minors place in parents, teachers or other persons, or
- unreasonably show minors in dangerous situations'.

Furthermore, the directive prohibits audiovisual commercial communications for alcoholic beverages specifically targeted at minors, showing minors consuming them, and encouraging immoderate consumption of such beverages. The directive also promotes self-regulation through codes of conduct regarding advertisements of unhealthy foods and beverages.

Since the directive is not directly applicable, Member States had to [transpose](#) it into national legislation. Most of them have transposed the AVMSD through amendments to their main law governing audiovisual media services.

In terms of enforcement, the AVMSD requires Member States to designate one or more national regulatory authorities or bodies to monitor and enforce compliance with the directive. The [Commission](#) ensures that the directive is implemented by the Member States and interpreted correctly. To support this action, the Commission is advised by the European Regulators Group for Audiovisual Media Services ([ERGA](#)), which brings together the heads or high-level representatives of national independent regulatory bodies in the field of audiovisual services.

European digital identity framework

In April 2024, the EU co-legislators (the European Parliament and the Council) signed [Regulation \(EU\) 2024/1183](#) updating the European digital identity framework. The regulation requires Member States to issue, by 2026 at the latest, a European digital identity 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 such as driving licences, educational diplomas and medical prescriptions. Children could use the wallet, for example, to prove their age to access social media platforms. Very large online platforms that require user authentication for access of their services would have to accept and facilitate the use of European digital identity wallets. This measure might help to ensure that children do not access social media platforms too early.

Unfair Commercial Practices Directive

The [Unfair Commercial Practices Directive](#)⁴ is another piece of EU legislation relevant to children's protection online. It specifically prohibits exhorting children to buy advertised items or persuade their parents or other adults to buy advertised products for them. In the 2021 [guidelines](#) on this directive, the Commission specified that the Unfair Commercial Practices Directive also applies to influencers. The latter have to declare in their content if they are paid to promote items.

In October 2024, the Commission published the [Digital Fairness Fitness Check](#), evaluating the effectiveness of three EU consumer law directives: the Unfair Commercial Practices Directive, the Consumer Rights Directive, and the Unfair Contract Terms Directive. The Commission assessed whether these directives provide adequate protection for consumers, including minors, in the digital age. During this evaluation, it identified several problematic practices, raising the need for new legislative measures (see section on 'Digital fairness act' below). The Commission found, in particular, that knowledge of consumer rights remains insufficient, and that problematic commercial practices have increased. Many consumers, particularly minors, still have the impression that companies exploit their vulnerabilities for commercial purposes. In addition, many influencers still do not declare clearly if their content is being paid for, and sometimes promote scams or dangerous

products. For example, [many young influencers](#) promote consuming alcoholic drinks in a positive context, without disclosing this clearly as an advertisement.

Pending or future EU laws protecting children online

Proposal for a regulation laying down rules to prevent and combat child sexual abuse

In May 2022, the European Commission proposed to adopt a [regulation](#) laying down rules to prevent and combat child sexual abuse. In the initial proposal, the Commission suggested making it mandatory for providers of both hosting services and interpersonal communication services such as WhatsApp to detect, remove and report child sexual abuse on their services. To facilitate implementation of the regulation, the proposal suggests establishing a European centre to prevent and counter child sexual abuse. The regulation has not yet been adopted; while the European Parliament has adopted its position on the proposal, the Council has yet to do so. The current Presidency of the Council of the EU, Poland, has proposed a [compromise text](#) that tackles one of the proposal's most controversial aspects, namely the compulsory orders to platforms to detect child sexual abuse material on private messaging platforms and services. Some fear this might lead to widespread surveillance of private communications. In the compromise text, these detection orders are deleted.

European Parliament's view

Parliament has highlighted the need to review the above-mentioned EU consumer law directives in the light of providing children with stronger protection online. It believes that further measures are necessary to address the addictive design of online services. It calls on the Commission to create a list of good practices of design features that are not addictive or manipulative, such as 'think before you share', turning all notifications off by default, or more neutral online recommendations.

Source: European Parliament, [Resolution](#) of 12 December 2023 on addictive design of online services and consumer protection in the EU single market.

Digital fairness act

As a result of the [Digital Fairness Fitness Check](#) published in 2024, the Commission concluded that there is a need to develop a digital fairness act to address dark patterns, marketing by social media influencers, the addictive design of digital products, and online profiling when consumer vulnerabilities are exploited for commercial purposes. This act is not expected before 2026. More specifically, the digital fairness act could tackle the following issues:

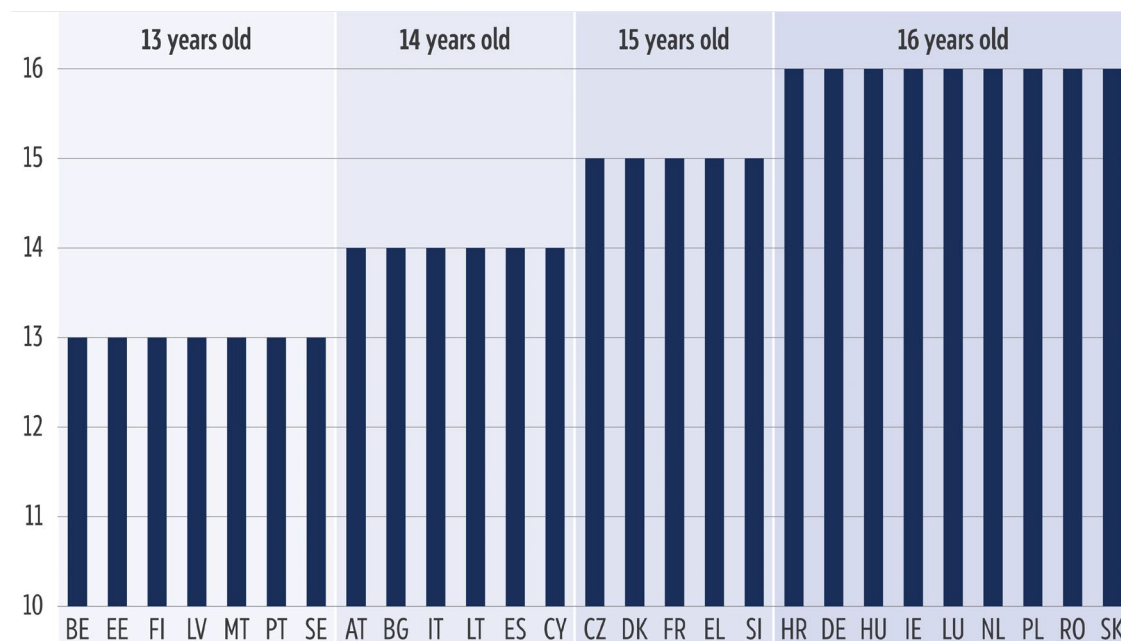
- dark patterns in online interfaces that can unfairly influence consumers' decisions, for example by putting unnecessary pressure on consumers through false urgency claims;
- addictive design of digital services that pushes consumers to keep using the service or spending more money;
- algorithmic personalisation that takes advantage of consumers' vulnerabilities for commercial purposes;
- difficulties with managing digital subscriptions, for example when a consumer wants to unsubscribe;
- problematic commercial practices of social media influencers who do not always indicate the commercial nature of their content.

National and regional laws and initiatives protecting children online

Age limits and verification

One key aspect of protecting children online is the age as of which children can give consent to their personal data processing and access social media platforms. As seen from Figure 1, the minimum age to give consent to their personal data processing by social media platforms varies from one EU Member State to another. At EU level, the GDPR requires parental consent for processing of children's personal data by social media platforms up to 16 years old. However, Member States can lower this age to up to 13 years old. Figure 1⁵ shows that more than half of EU Member States have used the possibility to lower the age at which children can give consent to their personal data processing. Member States have done so in their national data protection regulations.

Figure 1 – Minimum age to give consent for personal data processing by social media platforms



Source: Compiled by the author, based on data gathered by [Linklaters](#) (data from February 2024); graphic by Lucille Killmayer.

France has regulated the age of digital majority in a 2023 [law](#) that seeks to reduce children's exposure to screens, protect them against cyberbullying, and safeguard them from harmful content. According to the law, social media platforms should not be accessible for children younger than 15 years of age, unless their parents or guardians have given consent to open a social media account. Parents can also ask to close a social media account for children under 15 years old.

France has been calling to apply an EU-wide digital majority at 15. In a [speech on Europe at Sorbonne University](#) in April 2024, President Emmanuel Macron said he would support the digital majority being set at 15 at EU level, meaning that children under the age of 15 would have to get their parents' consent to create a social media account. The Danish Prime Minister, [Mette Frederiksen](#), also reportedly wants the EU to impose a 15-year age limit to access social media.

Researchers' opinions vary on the idea of setting the digital majority at a specific age. In his 2024 book *The Anxious Generation*, US social psychologist Jonathan Haidt recommends waiting until adolescence is well under way (around 14 to 16 years old) before introducing smartphones and social

media to children. This is because younger children are more susceptible to negative impacts of screen time and social media. Conversely, in a 2025 paper, [S. Livingstone and K R. Sylwander](#) argue that it is difficult to set a specific age of digital consent, and that individual maturity and skills may vary from one child to another. Moreover, children often [lie](#) about their age when opening a social media account.

EU Member States are also taking other measures to prevent children accessing age-inappropriate content. For example, in June 2024 the Spanish government approved a [draft law](#) banning [minors](#) from accessing digital spaces that employ random reward mechanisms such as lootboxes. These lootboxes allow players of video games to obtain, on a random basis, virtual rewards or prizes. The draft law requires providers of online services to use technical measures, such as age verification or parental control systems (activated by default), to restrict access to harmful content.

The Spanish government is also planning to introduce a mobile application, [Cartera Digital Beta](#), that would enable internet platforms to verify whether a user is over 18. It would operate as a mobile wallet linked to government-issued identification; in the future, this could be replaced by the EU's digital identity system. Similarly, Greece's 2024 [national strategy for the protection of minors from internet addiction](#) envisages the use of a Kids Wallet application to check users' age and allow parents to block certain webpages or set time limits.

Some countries specify to which technical conditions the age verification systems have to correspond. For example, a [guidance document](#) on age verification systems published by German regulators in October 2024 highlights the need to use various age verification systems, depending on the risk incurred. These should all ensure the safety and wellbeing of children.

In October 2024, France published a [detailed mandatory technical standard](#) applicable to age verification systems used by providers of adult content. According to this standard, these systems should respect the conditions of independence, confidentiality and security. The [standard](#) has been applicable since January 2025, and failure to comply with it can result in fines of up to €150 000 or 2 % of the worldwide annual turnover for a first offence.

Bullying and cyberbullying

EU Member States are also introducing legislative changes to provide children with better protection against bullying and [cyberbullying](#), making it easier to prevent and report these incidents. Measures against cyberbullying are often taken together with measures against bullying, since both phenomena often occur alongside each other.

Some countries have updated the definition of bullying or cyberbullying in their national law. There are notable differences between these national definitions, making it difficult to compare statistics on bullying and cyberbullying between Member States. France, for example, states in its updated [Education Code](#) (2022) that:

No pupil or student may be subjected to acts of harassment resulting from comments or behaviour committed within the educational establishment or outside school or university life, with the aim or effect of undermining his or her dignity, altering his or her physical or mental health, or degrading his or her learning conditions.

In comparison, an Italian [law](#) of May 2024 includes in its cyberbullying definition not only acts of harassment, but also:

any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, illicit processing of personal data to the detriment of minors, carried out electronically, as well as the dissemination of online content concerning one or more members of the minor's family whose intentional and predominant purpose is to isolate a minor or a group of minors by engaging in serious abuse, harmful attack, or ridicule.

Several Member States have taken measures seeking to facilitate reporting of cyberbullying. For example, [France](#) requires social media platforms to publish messages calling to fight against cyberbullying and provide a phone number, where people can report cyberbullying and illegal content. In emergency cases involving an imminent serious threat to a person, social media platforms have to reply to legal requests at the latest within eight hours.

In addition to legislative changes, Member States are adopting programmes and action plans on cyberbullying and preventing violence in schools. For example, Croatia has published a [2020-2024 action plan for preventing violence in schools](#).

Sharenting

Several EU Member States have implemented or proposed legislative changes to establish boundaries on parents who share publicly information about their children online. For instance, France adopted a [law](#) in 2024 that addresses cases where parents disagree about posting content featuring their child. In the event of disagreement among parents, one parent has a right to prohibit the other parent from sharing images of their child. If the dissemination of images undermines the child's dignity or moral integrity, individuals or social services assisting the child can also request that the court transfer the parental authority regarding the exercise of image rights.

Similarly, in 2024 [Italy](#) proposed legislation that would grant minors the right to the removal of any online content featuring them from the age of 14. In addition, Italy aims to tighten regulations on 'baby influencers'. Under the proposed rules, if parents profit from sharing images of their children, they would be required to transfer the earnings to a bank account in the child's name, which would become accessible to the child on turning 18 years old.

Mobile phone bans in schools

The issue of banning mobile phones or smartphones in schools is currently on the agenda of educators and politicians in several EU Member States. While some Member States have already implemented a ban, others are still debating the matter. For example, [Greece](#), [France](#), [Italy](#), [Latvia](#), [Hungary](#), the [Netherlands](#) and [Portugal](#) have taken a decision at national level to prohibit mobile phones in schools (see Table 1). However, the specifics of this ban vary from one country to another. Typically, the ban applies not only during classes but also during breaks. In France, the law prohibits younger children from using mobile phones, including during school-based activities outside of school. In some cases, such as Hungary, this decision has sparked protests. [Unesco](#) has recommended banning smartphones in classrooms, except when used to support learning. According to [Unesco](#), as of 2024, 79 countries worldwide (40% of those surveyed) had implemented a ban on smartphones in schools.

Table 1 – Mobile phone (smartphone) bans in selected EU Member States

Member State	Mobile phones banned in elementary schools	Mobile phones banned in secondary schools	Exceptions
Greece	Yes	Yes	Permitted for health-related needs
France	Yes	Yes, in lower secondary schools	Permitted for educational purposes and medical reasons
Italy	Yes	Yes, in lower secondary schools	Permitted only in individual cases, e.g. in case of a disability

Member State	Mobile phones banned in elementary schools	Mobile phones banned in secondary schools	Exceptions
Latvia	Yes (in grades 1-6)	No	Schools are free to decide on the details of the ban
Hungary	Yes	Yes	Schools are free to decide how to implement the ban and which exceptions to envisage
Netherlands	Yes	Yes	Permitted for educational purposes and medical reasons
Portugal	Yes (in grades 1-6)	No	Schools are free to decide how to implement the ban

Source: Compiled by the author, based on various sources (e.g. French [law](#) of 2018 on the use of mobile phones in schools; [Euronews](#); [Saeima](#); [Rijksoverheid](#)).

Germany and Spain have devolved the decision on banning smartphones in schools to their federal states and autonomous regions, respectively. For instance, [Bavaria](#) in Germany and [Extremadura](#) in Spain have opted to ban smartphones in schools, with exceptions for educational purposes, whereas Lower Saxony in Germany and the [Basque country](#) in Spain have left the decision to individual schools. [Lower Saxony](#), in particular, is actively campaigning against a blanket ban. Similarly, several school leaders in [Estonia](#) do not support a comprehensive ban on smartphone use in schools, although they do favour the introduction of consistent rules on their use.

Belgium has also adopted a regional approach, with [Flanders](#), [Wallonia](#) and the [German-speaking Community](#) all deciding to ban smartphones and other smart devices in schools. Furthermore, [royal decrees](#) in Belgium prohibit the sale of mobile phones and smartphones specifically designed for children under the age of seven, including those with a playful design, simple operation and minimal keys. However, mobile phones and smartphones made for older children are still permitted, even if they have a playful design. Toys that look like mobile phones but in fact are not mobile phones are permitted. Additionally, it is forbidden to advertise mobile phone use targeting children under seven years old.

France is considering introducing a prevention message on mobile device packaging and advertisements, similar to those used for alcoholic beverages, warning of the risks of excessive use on the physical, psychological and cognitive development of young children. The proposal was made in a 2023 [draft law](#) aimed at reducing children's excessive exposure to screens.

Some Member States have banned the use of specific applications because of privacy concerns. For example, [Denmark](#) banned the use of Google Chromebooks and Workspace in schools in 2022, after the Elsinore municipality found that they did not comply with the GDPR requirements. The same year, [Microsoft 365](#) was banned in schools in Germany's Baden-Württemberg state for the same reason.

Other initiatives seek to reduce addiction to mobile phones by limiting their use to specific time-periods. For instance, the Basque country has launched the [NoPhoneChallenge](#), a week-long initiative encouraging children to abstain from using their phones.

Awareness-raising efforts

Many schools, parents, health professionals, ministries and non-governmental organisations are raising awareness about the negative effects of digital technologies and helping to identify best practice. National initiatives, such as the French [Children Online Protection Lab](#), play a crucial role

in exploring, promoting, developing and evaluating solutions aimed at improving the safety of minors in the digital world.

International organisations, too, have launched multiple initiatives to promote awareness of child safety online. For instance, the International Telecommunication Union (ITU) has established a multi-stakeholder network – the [ITU Child Online Protection initiative](#) – that develops practical tools to assist governments, industry and educators in protecting children online. The [ITU Guidelines on Child Online Protection](#) provide recommendations for all relevant stakeholders on how to contribute to the development of a safe and empowering online environment for children and young people.

Hundreds of thousands of parents in various European countries have joined the [Smartphone Free Childhood campaign](#), initiated by parents in the United Kingdom. The movement has [WhatsApp groups](#) in several EU Member States. The campaign [website](#) offers information on topics such as how to discuss children and smartphones with other parents. The campaign has also developed [guides](#), which recommend banning smartphones in schools and suggest that parents be informed about the negative effects of smartphones, with the encouragement to consider alternative options such as brick phones. Numerous other similar campaigns are hosted on the [change.org website](#), where citizens are calling for measures such as [banning](#) smartphones and social media for children under the age of 16.

Civil society organisations have also raised awareness about the potential negative impacts of smartphones and social media on minors. In 2023, six civil society organisations⁶ joined forces with the [Spanish Data Protection Agency](#), the Attorney General's Office and the [Spanish National Markets and Competition Commission](#), to agree on a proposal for a [state pact](#) in response to the negative impact the use of the internet and social media can have on minors in certain circumstances. The pact acknowledges that compulsive technology use constitutes a significant public health issue, and calls for adjusting public policies accordingly. It advocates organising targeted awareness-raising campaigns, and recommends strengthening existing helplines, establishing new support channels, and setting up specialised treatment centres for behavioural addictions.

In October 2023, the [Spanish Data Protection Agency](#) and the Spanish Association of Paediatrics launched the *Cambia el Plan* campaign aimed at mitigating the risks associated with the misuse of screens on children's and adolescents' health and wellbeing. The campaign aims to raise awareness among parents and caregivers, and reduce the physical, mental, sexual and social risks linked to excessive and uncontrolled screen use.

Moreover, various local and regional authorities have organised information sessions and workshops on the safe use of digital technologies. For example, the [Basque country](#) in Spain has held workshops on the educational use of mobile devices, assisting schools in regulating the use of these devices.

[Safer Internet Centres](#) in Member States, co-funded by the EU, carry out activities designed to keep children safe online. For instance, in [Ireland](#), the [Webwise initiative](#) helps teachers to teach about online safety, and provides information and advice to parents. In June 2024, the Irish Minister for Education launched the [Bí Cineálta](#) ('Be Kind') procedures, to prevent and address bullying behaviour for primary, post-primary and special schools.

Way forward

The EU has made some progress in protecting children online through a range of laws, initiatives, and awareness-raising campaigns. The regulatory framework established by the EU and its Member States provides some support in safeguarding children's digital rights and promoting online safety. However, much work remains to be done to ensure that children are fully protected from the risks and harms associated with the digital environment, while at the same time being able to take full advantage of the benefits of digital tools. The [European Commission](#) has announced that it will carry out an EU-wide inquiry on the impacts of social media on wellbeing and publish an action plan against cyberbullying.

One of the areas that requires attention is the [enforcement](#) of existing laws. While the EU and Member States have adopted various legislative acts aimed at protecting children online, the enforcement of these rules is not always easy; children tend to find creative ways to circumvent the existing rules. Additionally, there is a need for greater cooperation among various actors and levels of governance. Many online risks and challenges are global. To address them and ensure that children are protected regardless of their geographical location, it might be beneficial to learn from the lessons of other countries.

As technology continues to evolve and new challenges emerge, pundits consider it essential that policymakers, regulators, and stakeholders remain vigilant and address emerging threats, ultimately ensuring a safer and empowering online environment for children.

MAIN REFERENCES

O'Neill, B., [The influence of social media on the development of children and young people](#), Policy Department for Structural and Cohesion Policies, European Parliament, 2023.

Organisation for Economic Co-operation and Development, [Children in the digital environment](#), 2021.

ENDNOTES

- ¹ Signed into law in October 2022.
- ² Signed into law in April 2016.
- ³ Signed into law in November 2018. It updates a previous directive on the same topic.
- ⁴ Signed into law in May 2005.
- ⁵ Country codes: Belgium (BE), Bulgaria (BG), Czechia (CZ), Denmark (DK), Germany (DE), Estonia (EE), Ireland (IE), Greece (EL), Spain (ES), France (FR), Croatia (HR), Italy (IT), Cyprus (CY), Latvia (LV), Lithuania (LT), Luxembourg (LU), Hungary (HU), Malta (MT), Netherlands (NL), Austria (AT), Poland (PL), Portugal (PT), Romania (RO), Slovenia (SI), Slovakia (SK), Finland (FI), Sweden (SE).
- ⁶ European Association for Digital Transition (AETD), Save The Children, ANAR Foundation, iCMedia, Dale Una Vuelta and Unicef.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Any AI-generated content in this text has been reviewed by the author. GPT@JRC was used to improve the readability of the text and broaden the range of sources available to the author.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2025.

Photo credits: © Sandwish / Adobe Stock.

eprs@ep.europa.eu (contact)

<https://eprs.in.ep.europa.eu> (intranet)

www.europarl.europa.eu/thinktank (internet)

<http://epthinktank.eu> (blog)