PRELIMINARY VERSION

Deutscher Ethikrat

Ad Hoc Opinion

Protection, Participation and Empowerment of Children and Adolescents in the Digital World

11 June 2026

This translation is a preliminary version that has been produced with the assistance of a machine translation service. Whilst all key passages of the main text have been manually checked and edited for accuracy, formal details in this version may still contain inaccuracies and inconsistencies. A fully revised final version will be made available soon.

PRELIMINARY VERSION

Published by the German Ethics Council

Jägerstraße 22/23 · D-10117 Berlin
Telephone: +49/30/20370-242 · Fax: +49/30/20370-252
Email: kontakt@ethikrat.org
www.ethikrat.org

Acknowledgements

The German Ethics Council would like to express its gratitude for the trusting and collegial exchange with the Independent Expert Commission on the Safety of Children and Young People in Digital Environments of the Federal Ministry of Education, Family Affairs, Senior Citizens, Women and Youth, from whose progress report we have benefited greatly. Special thanks are also due to Stephan Dreyer, Wouter Lueks and Hannes Federrath for their constructive feedback on the draft Opinion and the helpful discussions on the legal and technical aspects of the topic.

Table of contents

1 Introduction and description of the problem 5
2 Legal and technical framework 8
2.1 Legal framework 8
2.2 Technical framework 9
3 Ethical analysis 12
3.1 Protection, participation and empowerment in the digital world 12
3.1.1 Protection 12
3.1.2 Participation 15
3.1.3 Empowerment 17
3.1.4 Interim conclusion: Balancing protection, participation and empowerment 19
3.2 Ethical challenges arising from socio–technical complexity 20
3.2.1 Diversity and dynamics of the digital environment 20
3.2.2 Impact on and vulnerability of different stakeholders 21
3.2.3 Multi-actor responsibility 22
3.3 Effectiveness and side effects of age assurance technologies 25
3.3.1 Effectiveness of age assurance technologies 26
3.3.2 Undesirable side effects of age assurance technologies 27
4 Conclusions and recommendations 32
4.1 Conclusions from the ethical analysis 32
4.2 Recommendations 34
References 41
Members of the German Ethics Council 47

1 Introduction and description of the problem

Social media and other digital technologies play an important and growing role in the daily lives of many children and adolescents.[1] Active and thoughtful use of such platforms, in moderation, can, under the right conditions, contribute positively to the psychosocial development of adolescents and support their identity formation, awareness, education and social participation.[2] However, a growing body of empirical evidence shows that less ideal usage patterns and experiences can have a negative impact on the well-being of children and teenagers: In Germany, in autumn 2025, 21.5 per cent of 10- to 17-year-olds reported risky use of social media and 6.6 per cent reported pathological use[3] , which is associated with significantly more frequently reported symptoms of depression and anxiety, stress, sleep problems and suicidal thoughts.[4] The Risk Atlas published by the Federal Agency for Child and Youth Protection in the Media identifies 43 media phenomena that may pose a risk to minors online.[5] This concerns not only certain types of content such as pornography, hate, violence and extremism , but also activities like cyberbullying, cybergrooming and incitement to self-harm, as well as privacy violations and manipulative business practices. These can occur not only on social media, but also when using other digital services, such as online games, streaming services, messaging apps or AI applications like chatbots.

The European Commission classifies online risks to minors into five categories in its guidelines on the protection of minors under the Digital Services Act (DSA)[6] :

1. *Content risks:* "Minors may be unexpectedly and unintentionally exposed to content that is potentially harmful to them", for example content that promotes self-harm, suicide, eating disorders or extreme violence.
2. *Conduct risks:* These relate to "behaviours that minors may actively engage in online". This includes, for example, minors posting or sending hateful content or messages, violent or pornographic content, depictions of sexual abuse or terrorist content, as well as participating in dangerous challenges.
3. *Contact risks:* These relate to "situations in which minors are the victims of interactions rather than the perpetrators". These include, amongst others, online grooming, sexual coercion and blackmail on the internet, sexual abuse via webcam, cyberbullying, human trafficking for the purpose of sexual exploitation, as well as online fraud practices such as phishing, marketplace fraud and identity theft.
4. *Consumer risks:* These describe risks to which minors may be exposed "in their capacity as consumers in the digital economy". Such risks may, for example, from marketing, profiling and advertising. Added to these are financial risks such as spending large sums of money, risks associated with the purchase of drugs and other illegal or dangerous products, and risks associated with contracts.
5. *Cross-cutting risks:* These span all risk categories and can "significantly impact the lives of minors in a variety of ways." These include, among other things, risks posed by AI chatbots or the use of biometric technologies, risks arising from the excessive use of online platforms, which can lead to addiction, depression, anxiety disorders, disturbed

[1] See Staksrud et al. (2026).
[2] See Agyapong-Opoku et al. (2025); Salehi et al. (2025); Brailovskaia et al. (2025) 13 ff.
[3] See Wiedemann et al. (2026) 14.
[4] See Brailovskaia et al. (2025) 15 ff.
[5] See Brüggen et al. (2022) 102 ff.
[6] http://data.europa.eu/eli/C/2025/5519/oj [14.04.2026]; see also Livingstone and Stoilova (2021).

sleep patterns and social isolation, and additional risks to the privacy, data protection and safety of minors.

In light of these risks and dangers, several countries have proposed or already implemented policy measures to better protect minors. In Australia, children and adolescents under the age of 16 have been prohibited from having social media accounts since 10 December 2025[7] ; in the UK, websites with age-restricted content (such as pornography or violence) have been required to use effective age verification procedures since 25 July 2025[8] . Numerous other countries are discussing or working on legislative initiatives regarding age restrictions for social media.[9] In Germany, both the SPD and CDU in February 2026 and Bündnis 90/Die Grünen in April 2026 called for a statutory age limit of 14 for the use of social media[10] ;and the recommendations of the Independent Expert Commission on the Safety of Children and Young People in Digital Environments, appointed by the Federal Government, are expected in June 2026[11] . In November 2025, a resolution by the European Parliament[12] endorsed EU-wide age-based access restrictions to social media, AI chatbots and video platforms, and in March 2026 the European Commission set up a Special Panel[13] tasked with developing recommendations on child safety online and on possible age limits for social media and other online services in Europe.

Reactions to initiatives to introduce new age limits for access to social media range from enthusiasm for measures perceived as urgently needed to concerns that such age limits and the technical steps required to implement them do not effectively protect minors, but instead lead to negative consequences such as reduced participation and media literacy, as well as breaches of privacy. Consequently, an intense public and political debate has emerged regarding which type or combination of measures is best suited to mitigating risks and harm caused by digital services without, at the same time, causing disproportionate, harmful side effects.

The guiding principle for assessing potential measures is the best interests of the child within the meaning of Article 3 of the UN Convention on the Rights of the Child.[14] This encompasses not only protection from harm, but also the right to participation, respect for the child's views and freedom of expression (Art. 12, 13), access to information that promotes development (Art. 17), and the promotion of the child's personality and abilities (Art. 29), including the capacity for responsible media use. The relationship between these various aspects of the child's best interests is not without conflict. Prioritising one aspect may lead to compromises in the realisation of the others.

This gives rise to an ethically significant tension between interests of protection, participation and empowerment, which must be taken into account when determining the best interests of the child. It is primarily for the parents[15] to decide how to resolve this tension, as they are entrusted with the upbringing of their children both under the UN Convention on the Rights of the Child (Art. 18 (1) sentence 2 and Art. 5) and under the Basic Law (Art. 6 (2) sentence 1). Nevertheless,

---

[7] https://www.pm.gov.au/media/albanese-government-protecting-kids-social-media-harms [05.05.2026].
[8] https://www.gov.uk/government/collections/online-safety-act [05.05.2026].
[9] See Global Social Media Age Restriction Tracker: https://social-media-age-tracker.onrender.com [19.05.2026].
[10] See SPD parliamentary group (2026); CDU Germany (2026) 88 ff.; Bündnis 90/Die Grünen parliamentary group (2026).
[11] https://www.bmbfsfj.bund.de/bmbfsfj/themen/kinder-und-jugend/expertenkommission-kinder-und-jugendschutz-in-der-digitalen-welt [05.05.2026].
[12] http://data.europa.eu/eli/C/2026/1708/oj [14.04.2026].
[13] https://digital-strategy.ec.europa.eu/en/policies/panel-child-safety-online [05.05.2026].
[14] The Convention on the Rights of the Child applies to all persons under the age of 18.
[15] This refers to all legal guardians here and in the following.

there is certainly scope for government regulation. Such regulation can and should support parents through a variety of measures and also set limits on their decisions. However, it must not lose sight of the fact that it is primarily the task and responsibility of parents to strike an appropriate balance between conflicting aspects of the child's welfare.

2 Legal and technical framework

An ethical assessment of concepts for the protection of children and adolescents in the digital world requires an understanding of the relevant legal framework on the one hand, and of the functioning and role of digital technologies on the other.

2.1 Legal framework

With regard to the legal framework for the protection of children and teenagers in the digital world, three levels must be distinguished in the German context: the European Union level, the federal level and the state level. This interplay results in a regulatory environment that is already extensive, yet constantly evolving and, in some respects, fragmented.

At EU level, several legal acts are relevant to varying degrees, in particular the Digital Services Act, the Audiovisual Media Services Directive, the AI Act and the General Data Protection Regulation. The European Commission has also announced a Digital Fairness Act in its work programme for the fourth quarter of 2026, which is intended to regulate a range of technologies and commercial practices on the internet in a more consumer-friendly manner.[16]

At federal level, in addition to the aforementioned UN Convention on the Rights of the Child, which has the status of a simple federal law in Germany pursuant to the Act of Consent of 17 February 1992[17] , the Youth Protection Act (JuSchG) is of primary importance, the third section of which regulates "youth protection in the media sector". In addition to the requirements for administrative procedures for the approval and age rating of physical digital media containing films and games, this section sets out requirements for age ratings on film and gaming platforms. In the area of digital services, Section 16 of the JuSchG refers to the State Treaty on the Protection of Minors in the Media (JMStV), concluded between the federal states, with regard to the specific requirements to be applied to the content of digital services. Within the scope of the JMStV, online providers who make their own content available are obliged to carry out an age assessment; in the case of content and functions that are harmful to development – in particular those rated 16 and 18 and over – they must ensure that younger users do not normally have access to the service.

Supervision of the implementation of the JMStV's legal provisions falls to the state media authorities, with the Commission for the Protection of Minors in the Media acting as the central decision-making body.[18] The Federal Agency for Child and Youth Protection in the Media (BzKJ) monitors compliance with labelling requirements for film and gaming platforms and also has extensive responsibilities for the further development of youth media protection. The German regulatory framework for youth media protection makes use of voluntary self-regulation bodies at both levels. On the basis of the JuSchG, self-regulation bodies that have cooperation agreements with the Supreme State Youth Authorities assess from which films and computer games are considered safe. Depending on the outcome of this assessment, the content in question is given an unrestricted rating or a rating for ages six and above, 12 and over, 16 and over, or 18 and above ("Not suitable for minors").[19] The age ratings, which are generally

[16] COM(2025) 870 final, Annex I.
[17] See Research Services of the German Bundestag (2006).
[18] https://www.kjm-online.de/aufsicht [15.04.2026].
[19] https://www.bzkj.de/bzkj/wegweiser/spiele [20.05.2026]; https://www.bzkj.de/bzkj/wegweiser/filme [20.05.2026].

adopted by the Supreme State Youth Authorities, are currently carried out by the Voluntary Self-Regulation of the Film Industry (FSK) and the Voluntary Self-Regulation of Entertainment Software (USK).

In the field of broadcasting and telemedia, the Commission for the Protection of Minors in the Media recognises voluntary self-regulation bodies. These bodies may, at the request, assign age ratings to content and assess the suitability of technical protection measures. Organisations recognised under the JMStV include the Voluntary Self-Regulation of Television, the Voluntary Self-Regulation of Multimedia Service Providers, USK.online and FSK.online. When a JMStV self-regulation body acts as a kind of protective shield: services that have been reviewed or rated by a self-regulation body cannot simply be challenged by the state media authorities. Films, series and games made available online must also display a JuSchG age rating or a JMStV age classification. This does not apply in the same way to apps; here, provider-specific age ratings based on the IARC (International Age Rating Coalition) procedure have become established in many app marketplaces. With its requirements for youth protection mechanisms, which will apply from December 2025, the JMStV also aims to introduce child protection functions that can be activated by parents at the operating system level of end devices (primarily smartphones, computers and games consoles).

With regard to the relationship between the different legal bases, the primacy of EU law over national law must be observed. The Digital Services Act (DSA), which, as an EU regulation, is directly applicable, already stipulates in Article 28 how online platform providers – that is, services that make user-generated content publicly available – must ensure the protection of minors. The provision contains no opening clause for national laws. In accordance with the principle of full harmonisation expressed in Recital 9 of the DSA, member states are therefore, pursuant to Article 114 of the Treaty on the Functioning of the European Union[20] , likely not authorised to oblige platform providers, through national requirements, to provide further protection for minors.[21] However, this difficulty does not arise in the case of measures that fall outside the scope of the DSA or pursue a different protective purpose to that of the regulation. For example, a ban on private mobile phones in schools could be regulated at national level by the federal states.

The DSA does not apply to most generative AI services, as these applications do not make user-generated content publicly available; AI applications integrated into online platforms are an exception. The AI Regulation generally applies to AI systems; however, it does not contain any explicit and easily manageable requirements regarding the protection concerns.[22] The current JMStV also does not fully cover generative AI applications in which the output is consistently based solely on the input provided by a user.[23]

2.2 Technical framework

Digital technologies are of dual significance in the context of child and youth protection. On the one hand, there are various digital technologies that can endanger children and adolescents, such as social media, but also games and, most recently, especially AI chatbots. On the other hand, there are technologies that may be necessary to ensure the protection of children and

[20] In the case of harmonising European regulations, paragraph 5 of the provision permits national measures that provide greater protection only for the protection of the environment and the working environment.
[21] See Scientific Services of the German Bundestag (2026).
[22] See Dreyer (2025).
[23] See Ukrow (2024).

young people online. Two types of procedures and technologies are of particular relevance here. Firstly, there are age verification technologies, which categorise individuals wishing to access digital services into relevant age groups, such as children under 14. Secondly, there are technologies required to classify services or content according to their suitability for specific age groups. Both aspects require effective, secure and robust technical solutions.

Regarding the classification of content, there are, on the one hand, the aforementioned voluntary self-regulation bodies for different media types (e.g. the Voluntary Self-Regulation of the German Film Industry and the Voluntary Self-Regulation of Television). These rely on established procedures involving experts in the protection of minors when classifying content, although the use of AI-based methods is also on the rise here. On the other hand, platforms and service providers classify content on a voluntary basis. Not least due to the sheer volume of user-generated content, however, they make far greater use of AI-based methods and delegate the moderation or deletion of content to subcontractors, particularly in the Global South.[24] In addition, some parental control apps now also offer AI-based content classification.[25]

There are also various methods for differentiating users by age group. It is important to bear in mind that, in the event of a legal obligation to verify age, all individuals wishing to use age-restricted services will be affected by these measures. This means that, in such cases, adults too must prove that they have reached the minimum age. Decisions regarding additional age verification requirements, such as for social media, can therefore affect a very large number of people, depending on the number and prevalence of the services where such checks would be required. Accordingly, the technical solutions needed to implement them would have to be not only effective and have minimal side effects, but also be scalable.

Based on the classification used in the Australian pilot project[26], four approaches to age verification can be distinguished:

1. *Age verification:* Age is verified using official documents.
2. *Age estimation:* Age is estimated on the basis of biometric characteristics such as voice or photographs.
3. *Age inference:* Age is inferred from a user's behavioural patterns, which are either collected by a platform or determined (additionally) on data from other sources.
4. *Parental control* (in advance) *and consent*: Parents use technical means to authorise access to digital content and services in accordance with their child's age and stage of development. On the one hand, the option to specify the children's age when setting up devices, thereby implementing default settings compliant with youth protection requirements across the system. On the other hand, it also involves technical options that allow parents to grant or deny their children access to specific digital offerings such as apps or websites, or to restrict usage times.

There are different implementations for each of these four basic approaches. Of particular relevance here is the question of whether age verification takes place on users' devices, on the platforms themselves, or via third-party providers. Different forms and combinations of the above-mentioned approaches with different architectures are not only technically distinct but also have very different implications for both the effectiveness, accuracy and robustness of the measures, and their side effects – for example, with regard to privacy.[27] Given the potentially

[24] See Block and Riesewieck (2018).
[25] For example, Helmit, FamiSafe or Qustodio.
[26] See Age Check Certification Scheme (2025).
[27] See Lueks et al. (2026).

large number of people affected by the measures, these implications should be carefully examined.

3 Ethical analysis

An ethical analysis of concepts for the protection of children and adolescents in the digital world must be guided by the overarching goal of the child's best interests. Ethical challenges arise here in at least three forms. Firstly, a multidimensional understanding of the child's best interests itself already gives rise to an ethical tension due to the varying and not easily balanced requirements resulting from interests in participation, protection and empowerment. Secondly, further ethical challenges arise in view of the complexity of the digital world, the varying degrees to which different stakeholders are affected, and the distribution of responsibilities. Thirdly, problematic side effects of age verification measures must also be subjected to ethical analysis, particularly with regard to safeguarding the privacy, anonymity and security of all people who use digital services.

3.1 Protection, participation and empowerment in the digital world

The tension between protection, participation and empowerment is fundamental to the ethical analysis of child and youth protection in the digital world. Any proposed measure must be normatively justifiable against the backdrop of this tension. It must not optimise any of the sometimes conflicting aspects without regard for the others and must draw boundaries in such a way that parents are still left with the necessary scope to balance their child's interests in protection, participation and empowerment on an individual basis. The latter is important not only for safeguarding parental rights, but also because general regulation cannot take into account either the personalities and needs of children and adolescents or their specific life circumstances.

3.1.1 Protection

As outlined at the outset, there is consensus that minors are currently confronted in many areas of the internet with a wide range of risks and age-inappropriate content, which can be classified according to the European Commission's five risk categories. In particular, algorithm-driven platform services with a business model based on data collection and advertising – such as social media, but also, for example, online games, streaming services[28] and AI chatbots – are designed to maximise users' attention, engagement and, ultimately, the time they spend on the platform (keyword: attention economy).[29] Design elements are frequently used that can encourage excessive use (e.g. personalised recommendations, automatic playback, endless feeds that tempt users to scroll continuously, and psychological reward mechanisms such as likes, streaks and randomly distributed virtual prizes, for example from digital "treasure chests"). Similarly, many algorithms promote the spread of misinformation and extreme or disturbing content, as this is particularly attention-grabbing due to its surprising or emotionally charged nature.

These design features pose significant risks to individual self-determination, health and personal rights. Mechanisms that specifically stimulate the reward system and capture attention

[28] In particular, problematic use of online videos has recently increased among children and young people. According to the DAK Media Addiction Study, in 2025 more than a quarter of 10- to 17-year-olds used streaming services, Reels and similar platforms in a risky or pathological manner for the first time. This represents a 60 per cent increase compared to the previous year. Problematic social media use has remained at a similarly high level since 2022. More than a quarter of this age group now also uses generative AI chatbots several times a week or even daily. See Wiedemann et al. (2026).

[29] See German Ethics Council (2023), Chapter 7.

increase the risk that the use of these technologies will be extended at the expense of other important activities. The algorithmic prioritisation of emotionally disturbing and extreme content, in turn, increases its dissemination and thus the risks associated with such content. The observed consequences include, for example, the development of addictive behaviour, experiences of digital violence and an overall increase in mental health issues. Due to their still-developing sense of identity and emotional regulation, minors are less resilient to these risks and therefore particularly vulnerable.[30]

In view of the increasingly ubiquitous AI chatbots, which are also predominantly operated by large technology companies and designed to collect as much data as possible and maximise user retention time, further risks arise that may, among other things, impair learning and developmental processes (see Section 3.1.3). Furthermore, the formation of an emotional bond with chatbots in particular can create dependencies[31] and increase vulnerability to harmful advice, such as regarding self-harming behaviour, which such tools continue to dispense despite attempts by providers to curb this.[32]

The design features of algorithm-driven platforms described above pose risks not only to minors but also to the development of society as a whole. For example, they make it possible to strategically place and amplify narratives in order to erode trust, pit groups against one another and distort judgement and decision-making processes. These opportunities for abuse are already being exploited to a considerable extent by various actors to manipulatively influence the democratic decision-making process in society.[33] With regard to minors, these forms of manipulation are particularly promising simply because algorithm-driven platforms have become the primary source of information and news, as well as significant spaces for communication, especially for younger people.[34] Furthermore, adolescents may be more vulnerable to such attempts at manipulation.[35]

Given this situation, there is broad agreement that minors should be protected from content, actors and mechanisms that pose a risk to them in a much more comprehensive manner than has been the case to date. However, there are differing views on which protection concepts and approaches best serve the interests of child and youth protection in the digital world.

Introduction of a blanket statutory minimum age for access to certain services, in particular social media

As outlined in more detail in the introduction, the current focus of social and political debate is on countering minors' exposure to harmful content, actors and mechanisms by introducing a statutory minimum age for access to social media.

The hope is that introducing such a blanket restriction will achieve a higher level of protection more quickly or effectively than other approaches. Given the business models described, which run counter to a more youth-friendly or generally people-friendly design of social media and

[30] See Orben et al. (2024).
[31] According to the DAK Media Addiction Study, children and adolescents with high levels of psychosocial stress exhibit more pronounced attachment behaviour when using generative AI chatbots. They report significantly more frequently that they use chatbots to feel less lonely or to distract themselves from negative feelings, that the chatbot understands them better than a human, and that they tell it things they would not otherwise tell anyone else or would only tell close friends. See Wiedemann et al. (2026).
[32] See Common Sense Media (2025).
[33] See German Ethics Council (2023) 273 ff.
[34] See Behre et al. (2025); Rohleder (2023); Society for Innovative Market Research (2022).
[35] See Kops et al. (2025); Ma et al. (2026).

other digital services, and the significant market power of the corporations involved, there appears to be little prospect of sufficiently rapid voluntary improvements.[36] The existing legal framework does provide for intervention at EU level to enforce changes. However, the concern is that these processes take too long, particularly in view of the dynamically evolving usage patterns and the high risks to minors, especially as there is considerable political resistance to attempts at regulation, for example from the US.

A further argument in favour of a statutory minimum age is that this instrument has effectively contributed to protecting minors from risks in the analogue world, ensuring that they are not, or at least less frequently, confronted with problematic situations. Furthermore, there is hope that excluding minors from certain services could, in the long term, also act as an incentive for providers to design safe and youth-friendly digital spaces. For only by providing services that meet the requirements of youth protection the coveted target group of children and adolescents would once again be accessible.

Consistent implementation and expansion of a risk-based, differentiated protection concept

Alternatively, a risk-based protection concept can be considered, which, instead of blanket age limits for certain services, focuses on the risks arising from the specific mechanisms, functions and content of digital services and provides for protective measures tailored to these risks. This essentially corresponds to the risk-based approach set out in Article 28 (1) of the DSA, which the European Commission elaborates on in its guidelines on this provision. The guidelines include measures such as default private account settings for minors, effective moderation and reporting tools, the adaptation of algorithmic recommendation systems to suit young people, download and screenshot blocks for content posted by minors, safety features against cyberbullying, and the deactivation of addictive design features. This approach is also, in principle, reflected in existing options for teen accounts with limited functionality, content filters and parental control features on services such as Instagram, TikTok and ChatGPT.

The implementation of such protective measures by platform providers to date is, however, widely regarded as inadequate. This is justified in particular by the fact that the DSA guidelines are merely advisory in nature and there are no clear guidelines on responsibility or the specific technologies to be used. However, from the perspective of those who advocate a risk-based, differentiated protection concept, the scope for better implementation of content- and mechanism-related protective measures has not yet been fully realised. Efforts and debates aimed at better enforcing existing regulatory instruments, as well as political pressure on providers, are currently developing very dynamically, so that a swift improvement in the level of protection appears achievable through this route. For instance, under the DSA, the European Commission is increasingly taking action against business practices of major online platforms that harm the welfare of minors, including those of TikTok, Instagram, Facebook and Snapchat.[37] In the US, both Meta and Google were ordered to pay damages in March 2026 in two separate proceedings based on different legal grounds due to shortcomings in the protection of minors.[38] The targeted

[36] See, for example, the discussion surrounding the so-called “Facebook Files”: https://www.wsj.com/articles/the-facebook-files-11631713039 [21.05.2026].
[37] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312 [05.05.2026]; https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920 [05.05.2026]; https://ec.europa.eu/commission/presscorner/detail/en/ip_26_723 [05.05.2026].
[38] See Kang and Tan (2026); Kang et al. (2026).

continuation and intensification of efforts to enforce the DSA, with consistent use of the investigative and sanctioning measures provided for therein, therefore has the potential to implement the risk-based protection concept more effectively.

When assessing these two alternative protection concepts, it is important to bear in mind that no set of measures can completely eliminate all risks and that it is therefore important to be able to identify and contain problematic incidents and undesirable developments in good time. To this end, those responsible for the protection of minors need realistic insights into the digital spaces in which minors operate, opportunities for open dialogue with children and adolescents about their experiences in the digital world, and the means to hold providers and individuals to account for actions that undermine the welfare of minors.

Initial findings following the implementation of the "social media delay" for under-16s in Australia show that many teenagers are finding ways to circumvent access restrictions.[39] However, if minors still gain access to age-restricted content through mechanisms such as VPNs (Virtual Private Networks) or with the help of older siblings, friends or parents, or even switch to more problematic alternatives, such as unregulated or illegal services, such usage and the associated problematic consequences would no longer be easily measurable and countermeasures would be more difficult to implement. Youth who only access certain digital spaces without authorisation might also be less inclined to openly speak about negative experiences. At the same time, the overall level of protection on platforms could decline if, due to bans on use by minors, there were no longer any incentive for providers to make their content youth-friendly, and there were no legal means to demand changes.

3.1.2 Participation

An ethical assessment of concepts for the protection of children and teenagers in the digital world must also take into account how protective measures affect minors' opportunities for participation. Digital technologies are so deeply embedded into the lives of both adults, children and adolescents that they play a vital role in meeting fundamental information, communication and other social needs. This applies particularly to 12- to 19-year-olds.[40] For them, services such as WhatsApp, TikTok, Instagram and YouTube are now not only communication but also key sources of news and information. 93 per cent use their smartphone daily for an average of almost four hours, primarily for messaging services and social media. The use of AI tools such as ChatGPT is increasing, too: 84 per cent of young people were already using them in 2025 (2023: 38 per cent), mainly for schoolwork and to search for information. For younger children, the digital world also plays a major role.[41] 63 per cent of 10- to 11-year-olds now have their own smartphone, 81 per cent use WhatsApp regularly, 46 per cent use TikTok and 26 per cent use Instagram. Among 8- to 9-year-olds, as many as 33 per cent own a smartphone, 64 per cent use WhatsApp regularly and 17 per cent use TikTok. At the same time, given the overall increasing dominance of digital offerings such as social media and messaging services in society, some information and services are no longer available to the same extent or in the same quality via 'more traditional' media. Many organisations, companies and public figures, for example, create a great deal of content exclusively for social media. Communication and coordination

[39] See Molly Rose Foundation (2026).
[40] See Feierabend et al. (2025a).
[41] See Feierabend et al. (2025b); Kieninger et al. (2024).

within social groups now often take place primarily via chat groups, such as class or family chats.

Against the backdrop of this strong and growing digital penetration, measures to improve the protection of young people online must take into account how the informational, communicative and social needs of children and adolescents can be met and how their rights to well-being, information, education and freedom of expression can be safeguarded. With regard to these participatory interests, several objectives are relevant, some of which are in tension with one another.

Preserving and expanding positive opportunities for digital participation

Digital spaces and tools not only entail the aforementioned risks for children and adolescents, but also open up numerous opportunities. Information can be obtained on specific topics and from different perspectives, regardless of locally accessible libraries. There are diverse ways to engage with others about specific interests and concerns, regardless of geographical proximity. Social media and messaging services are actively used by children and teenagers to maintain friendships and can thus serve as tools for experiencing emotional support and a sense of belonging. They also provide a space for free and public expression of opinion, as well as for creative self-expression. AI tools enable the design and implementation of personalised learning strategies and also open up expanded opportunities for creative self-expression. Digital participation opportunities can be particularly valuable for young people who have fewer local opportunities for contact, access to information and other social infrastructure, for example because they live in sparsely populated areas or have a chronic illness. The same applies to minors with specific interests or needs who cannot always easily connect with like-minded people or those with similar experiences locally (e.g. on queer issues, neurodiversity or disabilities). Even where there is a lack of support or understanding from adults in their personal environment, digital participatory spaces can provide a counterbalance.

Many of the opportunities mentioned could be better realised in digital spaces designed with youth in mind than under the current conditions, with their numerous problematic design features. However, as long as there are no better alternatives, excluding minors from digital services that currently play a major role in enabling their participation in society would undermine children's and adolescents' rights to well-being, information, education and freedom of expression as a whole. These effects could also hit already marginalised groups even harder.

Revitalise opportunities for participation in the analogue world

Children and teenager's opportunities for participation cannot be realised purely through digital means. The time they spend using digital services and activities may be time taken away from other activities where they can experience and practise participation in the real world. Longitudinal studies do indeed show that a shift is taking place between analogue and digital activities. For example, the proportion of 12- to 19-year-olds who meet up with friends at least several times a week fell from 88 per cent to 64 per cent between 2005 and 2025, whilst frequent internet use rose from 60 per cent to 96 per cent during this period. Other analogue activities, such as sport and creative hobbies, have remained stable, however.[42] Particularly in cases of problematic digital media use, interventions that limit screen time in favour of other activities quickly lead to improvements in well-being.[43] Initiatives that promote analogue offerings or

[42] See Feierabend and Rathgeb (2005); Feierabend et al. (2025a).
[43] See Hunt et al. (2018); Davis and Goldfield (2025).

make them available in the first place are therefore seen as a means of strengthening offline activities, which, it is hoped, will contribute to greater overall well-being and opportunities for self-expression among children and adolescents. Better provision of information, education and freedom of expression in the analogue sphere could also, at least in part, offset any age-related usage restrictions on certain digital services.

Involvement of young people in decisions regarding the use of digital technologies

Decisions regarding access to and the opportunity to use digital technologies are of great and immediate significance to the everyday lives of children and adolescents. Children and adolescents therefore wish to be able to contribute their own perspective to such decisions. To meet this legitimate need for participation, they must be involved in decisions regarding access to and opportunities for using digital technology in a manner appropriate to their age. This applies above all to discussions within the family (see Section 3.2.3), but should also include appropriate participation of youth in political decision-making. Initiatives in this direction already exist. For instance, the Independent Expert Commission on the Safety of Children and Young People in Digital Environments has held workshops with young people to incorporate their experiences and wishes into its deliberations and recommendations.[44] Young people are also involved in the European Commission's Special Panel on Child Safety Online through the Commission President's Youth Advisory Board.[45]

3.1.3 Empowerment

During childhood and adolescence, important skills for life are acquired and developed. Consequently, conditions and measures that promote or hinder these processes have particular ethical relevance. Empowerment is closely linked to participation, as learning and development processes take place not only in formal educational settings but in all the actions and experiences of young people. In the context of social media and other digital technologies, it is significant, on the one hand, how the use of such platforms affects learning and development processes overall. On the other hand, the question arises as to how adolescents' abilities to use digital media sensibly and to deal with their challenges, risks and dangers can best be developed and strengthened. Empowerment interests can be identified in relation to both aspects.

Protecting and promoting learning, knowledge and skills acquisition

Meta-analyses show a mixed picture of the impact of digital tools on pupils' learning performance. In particular, their use outside school has a detrimental effect on learning outcomes, especially among younger children and minors from educationally disadvantaged households. Factors with negative effects on academic performance include screen time, parents' screen time, cyberbullying, smartphone addiction and social media. In a school context, the potential for distraction posed by smartphones or reading on digital devices also has negative consequences. Conversely, the targeted use of learning technologies such as technology-assisted

[44] https://www.bmbfsfj.bund.de/bmbfsfj/themen/kinder-und-jugend/kinder-und-jugendschutz/junge-menschen-beteiligen-wenn-es-um-digitalen-kinder-und-jugendschutz-geht--280504 [21.05.2026].
[45] https://commission.europa.eu/topics/digital-economy-and-society/protect-our-children-also-online_en [21.05.2026].

feedback, intelligent tutoring systems or interactive learning videos is associated with positive effects.[46]

The perception that the use of smartphones in school leads to attention and concentration problems has already prompted several federal states to ban or severely restrict the use of such devices in schools altogether, or for specific types of schools or age groups.[47] Other risks, such as the unauthorised creation and use of recordings for cyberbullying, can also be cited as arguments for keeping schools – as specially protected spaces for the learning and personal development of children and adolescents – largely[48] free from the private use of mobile devices. Regulations requiring private devices to be handed in whilst on school premises would have the advantage of largely relieving teachers of the task of identifying and penalising potential breaches. Where the use of digital technologies in lessons cannot be carried out on school devices, private devices could be returned for this purpose.

In view of the rapidly increasing use of generative AI tools by minors[49] , there is, on the one hand, a legitimate concern that improper use, primarily aimed at avoiding mental effort, could negatively impact learning processes or even lead to a decline in skills (deskilling).[50] Unlike adults, minors run the risk of failing to acquire basic skills in the first place if tasks are handed over to AI to an excessive degree, particularly during crucial developmental phases.[51] However, the use of AI can also be beneficial to learning if it focuses, for example, on coaching and reflection processes, meaning that the impact is likely to depend crucially on actual usage patterns.[52] Given the high complexity and dynamism of developments, there is a strong case for providing resources and structures that enable educational institutions to respond flexibly to developments, in order to optimise educational processes and learning outcomes in the digital transformation, using a mix of digital and analogue approaches and tools.

Protecting and promoting the development of social skills

Mechanisms and conditions that promote or hinder the participation of minors in digital and analogue situations also affect the development of social skills, as these are practised through interaction with other people. In this respect, the objectives mentioned in the section on participation are also relevant to the social empowerment of children and teenagers.

In addition, other aspects are gaining ethical significance, particularly those relating to the direct interplay between digital media use and face-to-face interactions. Firstly, this includes situations in which people focus their attention on digital devices rather than on those around them. This phenomenon, also known as “phubbing”, has a negative impact on the well-being of minors, both when they engage in it themselves and when they are on the receiving end of it.[53] Secondly, in connection with the increasing use of messaging services, social media and, more recently, generative AI in particular, there is concern that excessive use may impair the development of social skills and the formation of stable social contacts. There is evidence that adolescents are becoming increasingly less confident in communicating and presenting themselves

[46] Hattie 2008; 2023 (cited in Independent Expert Commission on ‘Child and Youth Protection in the Digital World’ (2026) 33 ff.).
[47] See Brand (2026) Section 3.
[48] Exceptions may apply, for example, to pupils whose private use of devices serves a medical purpose or promotes equality.
[49] See Feierabend et al. (2025a).
[50] See Stadler et al. (2024); Kosmyna et al. (2025).
[51] See Burns et al. (2026).
[52] See OECD (2026); Scheiter et al. (2025).
[53] See Nuñez and Radtke (2024); Wiedemann et al. (2025).

without digital support such as visual filters and AI-assisted wording tools.[54] Particularly with regard to AI chatbots, which simulate a personal relationship, there is the additional factor that these are increasingly being used in place of humans as personal advisors or emotional support.[55] The deliberate creation and promotion of spaces and situations in which young people interact with others without resorting to digital technologies could therefore help to mitigate or offset negative consequences for the development of social skills.

Strengthening digital media literacy

Digital media literacy among children and teenagers, as well as among the adults who support them as they grow up, is not only important for using digital tools in a way that supports rather than hinder learning and development potential. It is also essential for empowering all those involved, particularly adolescents themselves, to deal with the diverse risks and dangers described. Minors must learn not only to recognise problematic content, mechanisms and behaviours in themselves and others as early as possible, but also to respond appropriately to problematic situations, to take remedial action themselves or to seek help from suitable sources. To date, both the development of such skills and the support young people receive in developing these competencies have been inadequate. For instance, whilst many adolescents are aware that algorithms exist and influence them when using social media and AI tools, they rarely reflect on this and consequently experience little in the way of competent self-regulation and self-efficacy in this area.[56] In Year 8, more than 40 per cent of pupils in Germany achieve only rudimentary digital skills. Despite increased digitalisation in schools, these skills have actually declined since 2018.[57] Furthermore, there are indications that these skills are distributed unequally across social groups and that educational approaches to teaching media literacy skills, such as critical source evaluation and data protection, are lacking.[58] Given this situation and the importance of media literacy for young people's ability and resilience in the face of digital dangers and risks, improvements in this area are essential.

3.1.4 Interim conclusion: Balancing protection, participation and empowerment

It is clear that the interests and objectives outlined in the previous sections cannot all be equally fulfilled by individual measures. Furthermore, prioritising certain measures may have a negative impact on other interests and objectives. Where possible, youth protection measures should not result in youth participating less in social interactions, feeling increasingly excluded, learning less about how to deal critically with online information, and having a poorer command of digital communication techniques later in their working lives. Therefore, any measures under consideration should be carefully examined with regard to all three dimensions of the child's best interests – protection, participation and empowerment – and the potential negative consequences of their introduction and their omission should be taken into account.

In particular, blanket bans on the use of certain services that go beyond already established minimum age limits would restrict the opportunities for many adolescents to participate in the

[54] See Institute for Youth Culture Research and Cultural Mediation (2024); (2026).
[55] See Yu et al. (2025); Wiedemann et al. (2026).
[56] See Kelly (2025). Comparative data for adults suggest that this problem is not simply 'outgrown' over the course of a lifetime: even among the adult population, there are significant weaknesses in information seeking and evaluation, as well as in the understanding of algorithmic selection mechanisms, with clear differences according to age, education and social status. See Eder and Sjøvaag (2024).
[57] See Eickelmann et al. (2024) 61 ff.
[58] See Eickelmann et al. (2024) 73 ff., 135 f.

digital space. At the same time, they could lead to workarounds that undermine protection efforts and make it more difficult to engage transparently with problematic features of digital services and to redesign them. For even well-functioning access restrictions can be circumvented with sufficient creativity, and the motivation for such circumventions grows the more comprehensive the restriction is. Risk-based approaches to content- and mechanism-specific risk control, by contrast, are more compatible with the participation and empowerment interests of children and teenagers and, due to the likely higher level of acceptance associated with them, also reduce the risk of digital activities shifting to less regulated areas.

However, the effectiveness of specific measures, the potential side effects and interactions that may arise, whether they conflict with other aspects of children's welfare, and how specific approaches to promoting children's welfare should be assessed ethically overall depend on further factors, which are examined in more detail in the following section.

3.2 Ethical challenges arising from socio–technical complexity

Improving the protection, participation and empowerment of minors in the digital world poses ethical challenges in several respects. Firstly, it must do justice to the complexity and dynamism of the digital environment; secondly, it must take account of the diversity of needs, vulnerabilities and abilities of the individuals involved; and thirdly, it must hold the various actors operating at the individual, organisational and state levels to account in such a way that they work together effectively to fulfil this task.

3.2.1 Diversity and dynamics of the digital environment

The current strong focus of public and political discourse on social media falls short. Many children and adolescents use a wide range of diverse digital technologies in their everyday lives. In addition to social media, these include popular messaging services (particularly WhatsApp), online games and streaming platforms, as well as, increasingly, generative AI applications – notably chatbots, but also image and video generators. Such applications are also sources of digital risks and dangers; they are partly operated by the same major technology companies that are behind popular social media platforms, and are furthermore directly interconnected via tracking services that are deeply integrated throughout the online world. The boundaries between different services are also blurred. For instance, WhatsApp now offers the option to subscribe to or create public channels, the music service Spotify features copies of YouTube shorts, and online games that are used extensively by children simultaneously allow interaction with strangers via chat functions, for example.

The rapidly evolving portfolio of generative AI applications presents the additional challenge that AI offerings are becoming increasingly integrated into all areas of the digital world and are thus becoming ubiquitous. AI chatbots and services for summarising and generating content are now an integral part of many software applications and platforms used on a daily basis, ranging from search engines and messenger services to internet browsers and word processing programmes. They are also being integrated ever more deeply into the software of smartphones and other digital devices, through which all digital activities ultimately take place.[59] Should such services or some of their functions be deemed unsuitable for certain age groups, age-based regulation would present even more complex challenges than the restrictions on social media

[59] https://android-developers.googleblog.com/2026/02/the-intelligent-os-making-ai-agents.html [21.05. 2026].

use currently under discussion. Mitigating the risks associated with these services is therefore significantly more difficult than for social media: due to the deep integration into diverse areas of life and other technologies described above, but also because users often do not need to register to use AI tools, which, moreover, do not need to be embedded in platforms and are therefore not subject to regulation under the DSA.

How to deal with these challenges is a question of deliberation. However, it is important to also take interactions into account here. If access to social media is banned but AI chatbots are left untouched, there is a risk that children and adolescents will increasingly turn to such services to meet their informational, communicative and emotional needs, with potentially even more problematic consequences, for example in terms of emotional dependency, risks of addiction and a loss of cognitive or social skills.

3.2.2 Impact on and vulnerability of different stakeholders

Children and teenagers are rightly seen as a particularly vulnerable group who should be protected from the attention–economy mechanisms of profit-driven digital platforms in particular. However, susceptibility to such mechanisms affects all age groups, and not all minors are affected to the same extent. Children and adolescents with specific issues or needs for which they receive little or no support in their personal environment, minors affected by poverty or family conflicts, or those whose parents, for other reasons, are unable or unwilling to provide positive guidance on digital safety measures or the development of media literacy, are more vulnerable to the many risks and dangers of the digital world than young people to whom such factors do not apply.

Parents are the second group affected. They face the greatest challenges when it comes to teaching media literacy and enforcing usage restrictions, and, depending on their circumstances, may have access to very different resources to engage in this work. Not only do the time, knowledge and technical equipment available to protect one's own children from digital risks and dangers vary considerably, but so too do the emotional capacities required to resolve conflicts over media use within the family in a constructive manner. Furthermore, even committed parents have limited scope for influence, as social dynamics among peers play an increasingly significant role in the development of digital usage patterns, particularly from adolescence onwards.

Teachers and other adults involved in youth education and support, as well as the institutions in which they operate – such as schools, youth welfare organisations, public authorities – also play a vital role in shaping and enforcing youth protection in the digital world. At the same time, they are themselves affected by the associated challenges, particularly when they are expected to mitigate risks and dangers with insufficient time and financial and technical resources. This applies all the more as these risks and dangers are shaped by market-driven technologies that are rapidly evolving and almost impossible to control, yet increasingly permeate almost every aspect of everyday life.

Finally, society as a whole can also be considered vulnerable if its youngest members are at risk of harm as a result of these developments. Preventing such harm is challenging in itself, as decision-making at the political level is distributed among a multitude of different actors and is thus fragmented. Above all, however, measures necessary to prevent harm must be enforced against the power of internationally operating technology conglomerates.

3.2.3 Multi-actor responsibility

To ensure the protection, participation and empowerment of children and adolescents in digital spaces as effectively as possible, successful cooperation between various actors is required. For such situations, the German Ethics Council has developed the concept of multi-actor responsibility[60] , in which the responsibilities of various stakeholders operating at the individual, organisational and state levels are clearly identified and distinguished from one another, whilst also taking their interactions into account.

Individual level

At the individual level, it is primarily the parents' responsibility to protect their children from the dangers of the digital world, whilst at the same time ensuring that they have sufficient opportunities to participate in digital activities and become proficient with digital technology. Article 6 (2), first sentence, of the Basic Law entrusts parents with the care and upbringing of their children, which today also includes shaping their children's relationship with the digital world. In fulfilling this responsibility, parents are bound by the best interests of the child. When making decisions regarding access to digital services within the scope of their parental care, they must balance their children's interests in protection, participation and empowerment in such a way that their well-being is promoted to the greatest possible extent.

By virtue of their right to bring up their children, parents may, in principle, assess what serves their child's best interests and what does not, in accordance with their respective educational beliefs. Although the state, pursuant to Article 6 (2), second sentence, of the Basic Law, shall ensure that parents fulfil their duty and responsibility to care for and bring up their children, this supervisory role only justifies intervention in parental rights if the parents' educational views and the decisions based on them endanger the child's welfare, i.e. if there is an immediate significant risk to the physical, mental or emotional well-being of a minor. There must be a high probability that the danger will develop into significant harm as the situation progresses. Minor parenting errors or vague and uncertain potential harms do not trigger the State's duty of supervision. If it cannot be clearly assessed whether a decision serves the child's best interests or not, the State must respect the parents' right to bring up their children.

Accordingly, parents must be granted considerable discretion when deciding at what stage and to what extent they allow their children access to digital services. Whilst the balancing of the child's interests in protection, participation and empowerment required for this decision can be objectified to a limited extent, However, there is a relatively broad scope within which one may, with good reasons in each case, hold differing views as to whether priority should be given to the interests of protection or those of participation and empowerment. Within this scope, it is the task and responsibility of parents to assess whether access to the digital services in question serves the best interests of their child or not.

This is not contradicted by the fact that there are certainly parents who would find it a relief and welcome it if the state were to free them of this responsibility and regulate access to digital services for minors more or less completely. The interest of these parents in not having to regulate their children's access to digital services themselves, due to the time required and the associated potential for family conflict, is certainly understandable. However, it does not justify

[60] See German Ethics Council (2017) 239 ff.

curtailing the discretion of those parents who, in accordance with their own educational principles, wish to and should be able to judge for themselves whether access to certain digital services is in their child's best interests or not.

In order to make this assessment properly, parents should involve their children in decisions regarding access to digital services in a manner appropriate to their age. In particular, the interests of participation and empowerment can generally be better assessed and weighed up if parents ask their children to explain seriously why and for what purpose they wish to have access to the service in question. Individual, family-based usage rules and for time and content limits can also form part of this dialogue. Furthermore, age-appropriate involvement is particularly necessary in order to meet the growing need for self-determination among children and adolescents and to prepare them appropriately for a fully self-determined use of digital services through increasing transfer of responsibility.

Alongside parents, teachers and other adults working in youth education and support also have a duty, at an individual level, to protect the children entrusted to their care from the dangers of the digital world, whilst at the same time ensuring that these children enjoy sufficient digital participation and empowerment. In particular, those working in educational institutions bear a significant share of the responsibility for teaching the ability to deal competently and with increasing personal responsibility with the diverse opportunities and risks of digital technologies.

Organisational and governmental level

To ensure that both parents and other responsible adults can fulfil their responsibilities, certain framework conditions are required, which must be guaranteed through cooperation between stakeholders at the organisational and governmental levels. The most important of these framework conditions is to design social media and other digital technologies in such a way that children and adolescents are exposed to as little risk as possible through their use. To this end, the requirements set out in Article 28 of the DSA for online platforms accessible to minors must be met in all cases. Furthermore, however, digital services should be designed in such a way as to minimise systemic risks for all people, as is already laid down in Articles 34 and 35 of the DSA and in the forthcoming Digital Fairness Act. This would enable children and adolescents to use digital services relatively safely, and allow parents to support their children's interests in participation and empowerment without concern.

In this context, it is important to highlight an existing protection gap regarding generative AI. The DSA applies only to online platforms, but not to generative AI applications, because the latter do not make user-generated content publicly accessible, as defined by the DSA for the term 'online platform'. Although generative AI does fall under the AI Act, this does not contain any explicit provisions regarding the protection of minors.[61] As the JMStV is also not yet fully prepared for generative AI applications, the regulatory framework for child protection needs to be modernised in order to adequately address the challenges posed by generative AI.[62]

At the level of organisations, responsibility for ensuring that platforms are designed accordingly lies first and foremost with the platform operators themselves, who, regardless of legal regulation, are already ethically obliged not to pursue their business interests at the expense of the protection of minors in particular, but also of other users. The state has a responsibility to give concrete form to this ethical obligation through legal regulation, as well as to ensure that the

[61] See Dreyer (2025).
[62] See Ukrow (2024).

resulting legal obligations are actually fulfilled. As the necessary regulation has been or will be implemented at European level through the DSA, as well as through the AI Act, the General Data Protection Regulation, the Audiovisual Media Services Directive and the Digital Fairness Act, the European Commission, together with the Member States, bears the responsibility for ensuring compliance with the resulting legal obligations.

Stakeholders at organisational and governmental levels must also ensure, as far as possible, that parents are actually able to fulfil their responsibility to regulate their children's access to digital services in accordance with their own parenting values. A key prerequisite for this is that parents are sufficiently aware of the dangers posed to their children by digital services. Although these dangers are now also being discussed in the wider public sphere, it cannot be assumed that this awareness is already sufficiently widespread. It is therefore essential that both platform providers and the relevant authorities provide comprehensive information about relevant risks. Paediatricians' practices could also be involved in this endeavour; for example, they could raise the issue of digital media use during routine check-ups and draw parents' attention to the associated risks and the need for appropriate limits.

In order to responsibly manage their child's access to digital content in line with their own parenting values, parents also need independent information on which age groups a particular digital service is suitable for. Furthermore, user-friendly technical tools are important that enable parents to either allow or block access to individual services or specific features within services, and to set time limits on their children's digital activities, both for individual services and overall. If devices were configured so that, simply by entering an age, all digital services not recommended for that age were initially blocked, but could then be re-enabled individually and as granularly as possible (barring any mandatory restrictions) it would be feasible, to set up configurations that take account of a child's individual development with a manageable amount of effort.

However, to ensure that it is not only the children of particularly tech-savvy parents who are protected in this way, there must also receive comprehensive information about such technical options. This information must be designed in such a way that it enables as many parents as possible to use the available technical options to protect their children. In cases where this is not possible, the state must ensure that the parents concerned receive the necessary technical support, for example through digital mentors.

Nevertheless, cases may remain in which children are not adequately protected by parental supervision. Accordingly, public authorities also have a responsibility to ensure that children's welfare is not jeopardised by access to digital services. Where a serious interest in the protection of children and adolescents clearly takes precedence over their interests in participation and empowerment, the state must, by virtue of its constitutional duty to protect, prevent access to the services in question, even without regard to any contrary wishes of the parents. In particular when it comes to content that, under the Criminal Code or Section 4 of the JMStV, must not be made available to minors, these requirements are readily met. In order to protect minors as far as possible from such content, access to the relevant digital services should always be controlled by reliable age verification technologies that ensure the services are accessible only to adults.[63]

But even beyond that, there are undoubtedly digital services which, whilst perhaps not affecting children's welfare to such a massive extent or at every age, do so significantly enough—at least

[63] For content under Section 4 (2), first sentence, of the JMStV, a corresponding requirement is already set out in Section 4 (2), second sentence, of the JMStV.

in the case of younger children – that restricting access, irrespective of the parents' wishes, seems necessary. However, this can only be assessed on a case-by-case basis. A statutory minimum age for an entire category of services or a whole type of service would also affect services that do not harm the welfare of children and teenagers, or even promote it or provide special safeguards for their protection (e.g. social media platforms specifically for young people). A risk-based approach therefore seems more appropriate, which also underpins the European Commission's guidelines on Article 28 of the DSA. These provide that the Commission shall require providers to determine an appropriate minimum age for their respective service themselves and, where necessary, to verify this using age verification technology adapted to the level of risk. However, both the appropriateness of this self-assessment and its effective implementation should then be reviewed independently of the providers.

3.3 Effectiveness and side effects of age assurance technologies

To protect minors from content on the internet that poses a particular risk to them, such as pornography, it is essential to categorise individuals wishing to access such content into age groups. Accordingly, providers of online platforms containing such content should already be using age verification technologies in accordance with their obligation to protect minors, as set out in Section 28 (1) of the DSA. The use of such technologies would become necessary on an even greater scale if access to social media and, where applicable, other digital services were generally made conditional upon a specific minimum age.

Article 28 (1) of the DSA itself does not provide any specific legal requirements as to which age verification technologies are to be used, and Section 24a (2) (3) of the JuSchG, which expressly classifies technical means of age verification as precautionary measures within the meaning of Article 28 (1) of the DSA, contains no provisions on this matter either. Section 4 (2), second sentence, of the JMStV does require, for content falling under Section 4 (2), first sentence, of the JMStV, that "the provider ensures that it is made accessible only to adults". However, according to judgments of the Neustadt an der Weinstraße Administrative Court that are not yet final[64], this requirement does not apply to platforms conclusively regulated by the DSA and, furthermore, may be rendered ineffective notwithstanding the provisions of Section 2 (1), sentences 2 and 3 of the JMStV, as it can be circumvented under the country-of-origin principle applicable in the European Union,[65] if the provider registers in another country.

Under the current legal framework, it is therefore largely left to providers of online platforms to decide which age verification method they use and how they apply it. This legal situation is ethically questionable insofar as the various technologies for age verification are not necessarily equivalent. Details of the technical implementation, in particular the question of whether age verification takes place locally on users' devices, is carried out by the platforms themselves or through third parties, can be of great significance for ethical assessment. The differences are not merely technical in nature, but have direct implications for fundamental rights, particularly privacy, non-discrimination and informational self-determination.

In order to assess the opportunities as well as the risks of the respective approaches and their combinations, these must be analysed in terms of their effectiveness on the one hand and their

[64] VG Neustadt, 13.01.2026 – 5 K 475/24.NW, 5 K 476/24.NW, 5 K 1204/24.NW; VG Neustadt, 04.02.2026 – 5 K 1203/24.NW

[65] Regulated in Article 3 (1) and (2) of Directive 2000/31/EC and implemented in Section 3 (1) of the German Digital Services Act (Digitale-Dienste-Gesetz).

side effects on the other. The question of effectiveness encompasses the reliability, accuracy, but also the circumventability of technical solutions. This not only affects the extent to which the respective technologies can actually prevent minors from accessing content deemed harmful, but also the extent to which people may be wrongfully denied access to digital content when the respective technology is applied. The relevant side effects of the respective technologies also include challenges relating to the protection of all users' privacy, as well as potential biases and discrimination, misuse, security or censorship, and dependencies on platforms or operating system providers.[66]

3.3.1 Effectiveness of age assurance technologies

Age verification technologies are used to distinguish between individuals based on their age, to ensure that those who have not yet reached a certain minimum age are denied access to content deemed unsuitable for them. It is important to note, first of all, that no technical age verification system can completely prevent circumvention. As long as age limits apply only in some countries, these restrictions can, for example, be very easily circumvented by using Virtual Private Networks (VPNs), which allow users to pretend they are in a different location where these rules do not apply.

Figures from Australia do indeed show a sharp rise in the use of VPNs following the introduction of mandatory age verification.[67] Such circumvention strategies are therefore to be expected, particularly among tech-savvy minors. Assessments of the effectiveness of age verification technologies must take this fundamental susceptibility to circumvention into account. No system would meet a requirement for perfect effectiveness, but ignoring the possibility of circumvention can create a false sense of security. That said, when examining effectiveness, differences emerge between the various approaches, although their specific effectiveness also depends on the details of their technical implementation.

Verification: Document-based verification technologies offer the highest reliability, as the age of users is verified through existing official documents such as passports or identity cards. This verification can be carried out directly by presenting the document to the service provider, by entering the document's details on the user's device, or via identity providers (IDPs) such as the EUDI Wallet, which is regulated by the European Union's eIDAS Regulation. Differences in effectiveness arise depending on whether the age check takes place once or every time someone attempts to access an age-restricted resource. It is easier with one-off age check, for example when parents or other adults unlock devices for minors using their own documents.

Although the accuracy of document-based verification procedures is highest due to the use of official documents, even these cannot rule out the possibility that children may use adults' documents to register for services, or that their parents or other adults may provide their documents for verification, even if this risk can be reduced, for example, by entering PINs. Conversely, these document-based verification mechanisms raise the issue of unauthorised exclusion from access to digital services for individuals who do not possess the necessary documents or who encounter technical barriers when using the technology.

Parental control and consent: Technical approaches based on parental control and consent, which typically provide for age-appropriate restrictions on content and usage times as well as

[66] See Lueks et al. (2026).
[67] See Kaye (2026); Taylor (2026).

parental consent requirements at the device or service level – such as Apple's "Screen Time", Google's "Family Link" or third-party child protection apps – can achieve a similarly high level of effectiveness to the verification procedures mentioned above. However, this only applies if parents actually activate and configure these tools. Children and adolescents whose parents do not do so, on the other hand, remain unprotected. Furthermore, whilst such tools are built into the operating systems of common mobile devices (e.g. iOS, Android) or into the account settings for minors on some platforms (e.g. Instagram, TikTok, ChatGPT), their functionality could and should certainly be improved.[68] For instance, it should be made significantly easier for parents to enter age information and configure child-friendly settings.[69] Furthermore, sensible, user-centred solutions need to be created to allow for the granular deactivation of specific protection mechanisms, depending on the actual protection needs of the individual child, without completely foregoing protection. For example: if you wish to allow your children access to certain music that contains vulgar language classified by the platform as unsuitable for a child or teen account, this should not only be possible if you opt out of the youth version of the services entirely.

Age estimation and inference: Technologies that estimate age based on biometric data or online behaviour are less reliable and thus carry a high risk of minors bypassing age restrictions, or conversely of wrongfully excluding individuals who are of age from access. As children develop at different rates, both physical appearance and online behaviour can vary so widely within a single age cohort and be so similar across different age cohorts that it seems virtually impossible to reliably distinguish, for example, between 13- and 14-year-olds or 15- and 16-year-olds on the basis of this data. Whilst the consolidation and analysis of a larger volume and greater variety of data could increase this accuracy in the future, this would, come at the cost of highly invasive monitoring of users, particularly if carried out by providers. This leads directly to the side effects of age verification technologies and the associated risks.

3.3.2 Undesirable side effects of age assurance technologies

Privacy protection: Among the key side effects of many age-assurance technologies are the associated risks to privacy. Many approaches require the disclosure of sensitive data and/or the extraction of usage data and content by service providers. Of particular concern here is biometric data, which can range from facial features and voice pitch to bone structure[70] . However, the analysis of behavioural and usage data is also highly invasive and – in addition to calculating probable age – provides very granular and sensitive insights into the lives of the users being analysed. In particular, determining age based on online behaviour creates the risk that digital service providers will use the need to reliably distinguish between different age cohorts as a pretext to engage in even more invasive tracking of all users in the future, with massive implications for their privacy.

[68] Third-party apps already offer advanced functionalities such as more finely adjustable filtering options or AI-based monitoring of the interactions and content a child encounters via social media and communication applications. Depending on the specific design, however, these may present their own challenges for privacy and security. See Maier et al. (2025).
[69] For an overview of the scope and complexity of currently recommended parental settings for comprehensive technical protection of young people's media use, see the youth media protection portal 'Medien kindersicher': https://www.medien-kindersicher.de [21.05.2026].
[70] See Meineck (2026).

Age assurance technologies in which sensitive data remains on the end devices and which merely send the signal "old enough" to the platforms and service providers are therefore generally to be preferred over mechanisms in which the service providers themselves carry out age assurance based on collected data. At the device level, this can be achieved either through biometric estimation methods, similar to unlocking a mobile phone with the camera, or through document-based verification procedures.

However, for access to certain content – particularly content that, under the Criminal Code or Section 4 of the JMStV, must not be made available to minors – verification mechanisms may be required whereby providers check that the proof of age actually originates from the person wishing to use the service. Neither parental consent nor purely device-based methods are sufficient for this purpose.

This is where solutions such as the EUDI Wallet come into play. It is based on the EUDI Framework[71] , an EU framework for digital identities which, in accordance with the revised eIDAS Regulation (eIDAS 2.0), obliges all EU Member States to introduce a digital wallet. This digital wallet enables the issuance and verification of identity documents across Europe and could be used for age verification. Using these technologies, the device stores cryptographic proof of a successful age verification and can therefore no longer transmit information that deviates from the result of this verification. Furthermore, it can be ensured – for example by entering a PIN – that the person using the device is indeed the person for whom the proof of age was created.

To ensure such a strong form of verification without such a wallet solution, it would, for example, be necessary to hold up one's passport and, at the same time, one's own face to the camera in order to verify one's identity. However, such an approach poses significant risks to users' security and privacy, as considerably more data than necessary – including sensitive biometric data – would be transmitted.[72] The EUDI wallet, on the other hand, offers a data-efficient and more secure alternative and would clearly be preferable for this very strong form of verification.

In accordance with the eIDAS 2.0 requirements, the EUDI Wallet must fulfil three specific conditions in particular to effectively protect users' privacy:

1. *Selective disclosure:* For age verification, this means that if an ID document also contains a name or date of birth, the service provider may only be shown that the user is of legal age, without any further information – such as the name or date of birth – being disclosed. Selective disclosure helps to prevent the profiling and tracking of users, as it conceals all user-specific information and sends only the cryptographic proof that the user is 'old enough'.[73]
2. *Unlinkability by the issuer of the age verification:* The issuer of the age signal must not be able to identify where an age verification is being used. This prevents identity providers (and age verification services) from creating records of users' online behaviour and thus from tracking them.[74]
3. *Non-linkability of verifiers:* Verifiers or service providers must also not be able to identify users on the basis of the cryptographic proofs received, in order to prevent tracking

[71] https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation [05.05.2026].
[72] For example, in September 2025 there was a data leak involving photos from official identity documents of users of the Discord platform, which they had submitted to a service provider commissioned by Discord for age verification purposes. See https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service [21.05.2026].
[73] Article 5a (4) (a) and Article 5a (5) (a) (iii) of the eIDAS Regulation (eIDAS 2.0).
[74] Article 5a (16) (a) of the eIDAS Regulation (eIDAS 2.0).

and profiling. Furthermore, it must not be possible to link data between different verifiers and service providers.[75]

Technical solutions currently available on the market do not fully meet these three requirements. The EUDI wallet is intended to fulfil these guarantees; however, non-linkability is not currently fully guaranteed.[76] An EU age verification app launched in April 2026[77] , also known as the 'Mini-Wallet' and currently being piloted in various European countries[78] , has further weaknesses in terms of security, data protection and effectiveness.[79] Due to these shortcomings, as well as fundamental criticism of the side effects of these technologies, more than 400 cybersecurity experts, including some who are themselves involved in the development of the EUDI Wallet, spoke out against the use of age verification technologies as recently as March 2026.[80]

Systematic biases and discrimination: Age assurance technologies aim to exclude certain groups, namely children and adolescents, from accessing certain types of content, namely those deemed harmful to their welfare. In particular, systems that estimate age using biometric or behavioural data are susceptible to systematic biases in two ways: On the one hand, particularly in estimation systems, some minors may fall through the cracks because their biometric or tracking data leads to them being estimated as older. Conversely, users who are old enough to use certain services may also be unjustifiably excluded. With biometric methods, this can happen, for example, if they are estimated to be younger than they actually are.

Furthermore, there are additional sources of unjustified exclusion for both data-based and other approaches. These often affect, and for various reasons, user groups that are already marginalised. Firstly, people with limited technical knowledge, including older people, may find it difficult to adapt to an additional step required when using technologies that are already challenging for them. Secondly, age verification techniques may require specific hardware that some people cannot afford, such as mobile phones with cameras to take selfies for age estimation. Thirdly, verification systems require certain types of documents that specific groups may not possess, such as children under a certain age, but also international visitors.

Misuse and censorship: The risk of potential misuse of age verification technologies must also be considered. These technologies are tools for distinguishing between and treating user groups differently. As such, they can also be misused, both to restrict access for further groups and to restrict access to other content, for example to sex education materials or even to content that is politically undesirable. Given this wide range of potential applications, it cannot be ruled out that age verification technologies may be misused as a tool for censorship.

Institutional and technical dependencies: Furthermore, problematic institutional and technical dependencies may arise. The various age verification tools require the cooperation of platform, app and operating system providers. Even if these dependencies cannot be entirely avoided, care should be taken to ensure that legal requirements for age verification do not further increase the market dominance of major providers (such as Google, Apple and Microsoft).[81]

---

[75] Article 5a (5) (b) of the eIDAS Regulation (eIDAS 2.0).
[76] https://eudi.dev/2.4.0/discussion-topics/a-privacy-risks-and-mitigations [05.05.2026].
[77] https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15_en [21.05.2026].
[78] https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint [05.05.2026]; https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications [05.05.2026].
[79] See Steinebach et al. (2026); Marzolf et al. (2026).
[80] See Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance (2026).
[81] See Leisegang (2026).

The end of the open internet: The mandatory use of age verification technologies also raises concerns that this would be a further step towards the end of a freely accessible, open internet. This would be a cause for concern if mechanisms for circumventing age restrictions – such as the use of anonymous browser functions or VPNs, which allow users to pretend to be in a location where age restrictions do not apply – were themselves to be banned. Furthermore, age verification requirements could also pose challenges for open-source software, as smaller providers and open-source projects in particular may not have the capacity to guarantee age verification.

Overall assessment and evaluation

Overall, the various risks arising from technical access restrictions themselves can best be minimised if age-appropriate access to digital content for children and young people is primarily regulated through parental control and consent mechanisms on user devices. This involves two components: Firstly, parents can specify their children's age when setting up their mobile phones or tablets, so that content unsuitable for children is blocked from the outset (parental controls). Secondly, they can also use settings on their children's devices – for example, via Google Family Link on Android-based devices or via Screen Time on Apple devices to specify which apps and websites their children can use and for how long. If a child wishes to access these services, parents must consent to this access, for example by entering a code (parental consent).

Firstly, this approach respects the primacy of parental authority; secondly, it does not tie access to a rigid minimum age. Instead, it enables parents to decide, taking into account their child's individual development, at what age and to what extent access to digital services should be granted, and to gradually expand this access in line with their child's development. In this way, parents can dynamically take into account their children's interests in participation and empowerment. Thirdly, since no further data collection or processing by third parties is required for the use of the aforementioned device-based parental control and consent technologies, many of the problems associated with document- or estimation-based age verification technologies do not arise with this approach.[82] In particular, the additional privacy risks described above do not exist here. Furthermore, fourthly, unlike age verification or estimation procedures, parental control has no impact whatsoever on adult users of digital services, as they are not obliged to undergo age verification themselves.

However, restricting access through parental control also has disadvantages. Children and adolescents are only protected by this approach if and to the extent that their parents actually monitor access to digital services. Such monitoring will only take place if parents are aware of the dangers of their children having unrestricted access to digital services and if they have the necessary material and non-material resources to effectively monitor access to these services. Neither of these is a given, and even where resources are available, there are certainly parents who – to save time and, above all, spare their nerves – take the path of least resistance and do not monitor their children's digital activities, or do so only inadequately.

Finally, parental restrictions on access to digital content can also pose a further problem for minors. This becomes particularly evident when children seek protection specifically from their parents, for example in cases of sexual abuse. But even in other circumstances, children may have a legitimate interest in informing themselves about and engaging with certain topics with-

[82] However, if third-party tools are used, privacy issues may also arise in this context.

out their parents' knowledge. However, the problem of parents unjustifiably denying their children access would persist even if a statutory minimum age were introduced, because reaching that age would not oblige parents to grant their children access to digital services.

Depending on the risk, further measures beyond parental control options may be considered. Given the risks outlined above, procedures at the device level should be preferred here, as they have less of a negative impact on users' privacy – even if this may come at the expense of effectiveness and security. Here, both biometric procedures, in which data remains on user devices, and device-based verification mechanisms could be used as a second barrier to accessing content that is harmful to the welfare of children and adolescents. Where age restrictions secured in this way encroach on parents' discretion because they do not avert a clear risk to the child's welfare, parents should have the option to override these age restrictions or make individual configurations.

Should even stricter verification mechanisms be required, whereby providers must verify that proof of age actually originates from the person wishing to use the service, the EUDI wallet would be the method of choice. Its implementation would need to comply with the requirements of the eIDAS 2.0 Regulation and also be sufficiently scalable. Alternatives such as showing a passport and one's face to a mobile phone camera should be rejected on grounds of security and privacy protection.

4 Conclusions and recommendations

4.1 Conclusions from the ethical analysis

Children and adolescents are exposed to numerous risks in digital contexts – through harmful content, through actions that endanger themselves or others, through harmful contacts in the digital space, through consumer risks and through cross-cutting risks arising, for example, from the use of AI chatbots or the excessive use of online platforms[83] Effective protection of minors in digital spaces is therefore essential. At the same time, digital technologies play an important role in meeting the fundamental information, communication and other social needs of children and adolescents. Furthermore, it is of great importance for their future lives that they acquire the skills to deal competently with the diverse opportunities and risks presented by these technologies.

This creates a triangle of interests relating to protection, participation and empowerment, all of which must be taken into account in order to ensure and promote the well-being of children and adolescents to the greatest possible extent. Measures should primarily aim to make risks in digital environments manageable without unnecessarily restricting participation and empowerment. More restrictive measures are only justified if an adequate level of protection cannot otherwise be achieved or if there are particularly serious risks.

In public and political debate, the focus is on protection against the risks that social media pose to minors. However, other digital services and applications, such as messaging services, unmoderated gaming platforms or, above all, generative AI applications – particularly chatbots and image and video generators – carry risks comparable to those of social media. Consequently, a sole focus of political and societal discourse on social media falls significantly short. If access to social media were restricted for children and teenagers alone, they might shift their communicative and emotional needs towards chatbots, for example, with potentially even more problematic consequences for their psychological, social and health development. However, there is a significant regulatory gap regarding applications of generative AI, as these do not necessarily fall under the Digital Services Act, and the State Treaty on the Protection of Minors in the Media has so far contained only insufficient provisions on AI. The AI Act itself, in turn, contains no explicit and easily implementable provisions for the protection of minors.

If we are to effectively address the diverse risks to children and adolescents in digital environments, potential measures must therefore not be limited to social media alone. Rather, the various digital technologies must be considered collectively, taking into account their overlaps and interactions. This requires a nuanced understanding of the socio–technical foundations of an increasingly complex and dynamic, digitally interconnected world. Measures for the protection of minors in the digital world must take this complexity and dynamism into account in order to be appropriate and effective, but also to avoid undesirable side-effects and negative interactions.

In addition to the complexity and dynamism of the digital world, any regulation of minors' access to digital services must also take into account the diversity of the stakeholders involved, each with very different interests and capabilities. On the one hand, the rights of all parties must be safeguarded; on the other hand, duties and responsibilities must be clearly defined and delineated from one another to avoid a diffusion of responsibility. The German Ethics Council

[83] See the five risk categories in the European Commission's guidelines on the protection of minors under the Digital Services Act: http://data.europa.eu/eli/C/2025/5519/oj [05.05.2026].

proposes the concept of multi-actor responsibility for the allocation of duties and responsibilities in complex situations. Our recommendations are based on this concept and thus address specific stakeholders in each case.

The primary parties responsible for improving the protection of children in the digital world are the providers of platforms and other digital technologies, as it is often their products and the underlying business models that can harm not only minors, but also other user groups. Digital environments should therefore be made better and safer for everyone. This primarily involves the effective implementation of the Digital Services Act. This would also reduce the need for barriers to keep minors away from digital services.

Nevertheless, a certain degree of control over minors' access to digital services will remain necessary. This requires technical solutions that are effective yet have minimal side effects.

The German Ethics Council proposes a three-tier, risk-based model for the technical protection of children and adolescents[84] , with the aim of shaping the socio–technical framework for digital technologies through a combination of diverse measures that ensure protection, participation and empowerment in the best possible (see Recommendation 7.b-d).

Level 1: The first level of protection should be provided by parents, who, by virtue of their primary role in child-rearing, are primarily responsible for protecting their children from the risks of the digital world, empowering them to navigate it safely, and ensuring their participation in digital spaces. Technically, this control would be achieved by entering the children's ages when configuring the devices, as well as by regulating usage times or access to apps on the devices.

Level 2: In order to protect the welfare of children whose parents do not use these tools, or use them inadequately, and to ensure that the responsibility for protecting children and adolescents is not placed solely on parents, additional age controls at the device level can form a second level of protection. One option here is biometric age estimation methods; however, due to their limited effectiveness, these are only recommended as a supplementary measure and, given the sensitivity of the data, are only permissible if this data remains on the device. Methods whereby platforms estimate the age of users on the basis of biometric or behavioural data, on the other hand, should not be permitted, as these methods are, on the one hand, not sufficiently accurate or secure and, on the other hand, highly invasive. A second option is device-based verification methods, in which the devices verify the age of users by means of official documents.

Level 3: For access to certain content—particularly content that must not be made available to minors under the Criminal Code or Section 4 of the JMStV, mechanisms are required whereby providers verify that the proof of age actually originates from the person wishing to use the service. To ensure that *only* the signal "old enough" is transmitted, whilst other data remains protected, the EUDI wallet is to be preferred in these cases, as it would offer strong guarantees for the protection of privacy, provided it complies with the requirements of the eIDAS Regulation regarding selective data transfer and non-linkability. However, in addition to implementing these requirements, it is also necessary for the technologies used to be sufficiently scalable for widespread deployment.

[84] This model is based on the analysis by Lueks et al. (2026).

4.2 Recommendations

1. To better protect children and adolescents, a risk-based protection framework with age-appropriate restrictions on specific content and functions should be implemented more effectively.

The German Ethics Council recommends a risk-based approach to age-appropriate restrictions on content and functions that are harmful to the welfare of minors. This approach is already established in the Digital Services Act and in German legislation on the protection of minors but should be implemented more effectively, and the available investigative and sanctioning measures be utilised consistently. Measures to protect children and adolescents should primarily aim to reduce risks in digital environments and keep them under control, rather than comprehensively prohibiting use. Risk-based approaches generally allow for a higher degree of participation and promote the development of media literacy. They therefore create less tension with participation and empowerment as further central dimensions of the child's best interests.

A risk-based protection framework still allows for far-reaching access restrictions in contexts involving serious risks. However, it is necessarily complex and therefore carries the risk of overwhelming stakeholders and inadvertently creating loopholes, particularly for platforms. To counter this, its regulations must be as detailed and granular as necessary, yet as simple and clear as possible. To implement the approach, recourse could be made, among other things, to already established regulations, practices and institutions such as the Federal Agency for Child and Youth Protection in the Media (BzKJ), the Commission for the Protection of Minors in the Media (KJM) and voluntary self-regulation organisations.

Primary addressees: platforms, service providers, policymakers (federal government, European Commission)

2. Specific measures to improve digital environments must hold providers accountable and should be implemented at European level.

The primary parties responsible for the design of platforms and other digital services are the providers, who must ensure that their offerings do not harm children and adolescents. Due to the fully harmonising effect of the Digital Services Act, regulations addressing platform providers can only be implemented at European level. For this reason, and to prevent the foreseeable impairment of law enforcement that would result from fragmented regulations, the German Ethics Council recommends that efforts to implement further measures be concentrated at the European level from the outset. Key points from the "Guidelines on measures to ensure a high level of privacy, security and protection of minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065" should be integrated into the Digital Services Act and thus made legally binding. This could also include binding requirements regarding age limits and methods for verifying them.

Primary addressees: platforms, service providers, policymakers (federal government, European Commission)

2.a Features of digital services that encourage excessive use should generally be prohibited.

A key risk that has recently attracted the most attention, particularly in connection with social media, is that certain design features can lead to excessive consumption and addiction-like behaviour, as well as causing or exacerbating mental and physical harm. Minors are particularly vulnerable in this regard, but these mechanisms are also harmful to other users. The German

Ethics Council therefore recommends that Articles 34 and 35 of the DSA be applied consistently to generally prohibit features that encourage excessive use.

Primary addressees: policymakers (European Commission), platforms, service providers

2.b Providers must design digital spaces accessible to minors in such a way that children and adolescents are protected more effectively than has been the case to date.

In services freely accessible to children and adolescents, all features and mechanisms harmful to them should be consistently avoided in accordance with the European Commission's guidelines under Article 28 (4) of the DSA. In addition to avoiding addictive features, this also encompasses numerous other measures, such as refraining from profiling, tracking, and algorithmically driven feeds or recommendation systems; secure default settings that restrict both contact options and the ability to comment on, tag and share usercreated content to verified contacts; as well as better ways to block and report problematic content and interactions.

Furthermore, the identification of content that is harmful to children and young people should be improved. Given the volume of content (including user-generated content) that users may encounter on platforms, we consider the use of appropriate AI tools for content classification and the identification of harmful content to support human moderation to be justified. However, these tools must meet sufficiently specific quality metrics to minimise misclassifications. In addition to the problem of so-called underblocking (harmful content is not identified), it is also important to minimise overblocking (content is wrongly classified as harmful). Users should have the option to configure filters individually, and in doing so be able to utilise third-party services or locally installed AI systems. This would further reduce the risks posed by under- and overblocking.

Primary addressees: policymakers (European Commission), platforms, service providers

3. The risks to children's welfare associated with generative AI applications must be given greater consideration in the protection of minors in the media.

Generative AI applications pose the same, and in some cases greater, risks to minors' welfare as social media. In particular, chatbots – with their versatile applications and design possibilities accessible via natural language – are increasingly becoming the first port of call for the questions, interests and needs of children and adolescents in the digital world. As a result, they not only gain in significance as a source of relevant digital risks, but also pose additional dangers for the best interests of children and adolescents.

In particular, participation and empowerment may be compromised if the use of AI hinders or damages learning and educational processes, social and emotional development, or interpersonal relationships. Image generators also pose risks, for example with regard to the creation of pornographic material, but also in relation to sexual coercion and blackmail. Given the rapidly increasing prevalence of both standalone AI applications and the deep integration of AI into many digital services, the risks to children's welfare associated with these services must therefore be given greater attention in all efforts to improve the protection of minors in the media. As the Digital Services Act does not apply to most generative AI services, the German Ethics Council recommends that youth protection requirements for generative AI at European level, structurally follow the risk-based approach set out in Article 28 of the DSA. At national level, the State Treaty on the Protection of Minors in the Media would need to be expanded to regulate AI applications even where their output is based exclusively on the user's input – which is not currently the case.

Primary addressees: policymakers (European Commission), platforms, service providers

4. Access to digital services should initially be regulated by parents, who should receive significantly better support in this regard than has been the case to date.

Balancing the interests of protection, participation and empowerment of children and adolescents is primarily the responsibility of their parents, to whom the Basic Law entrusts the care and upbringing of their children. Parents have a degree of discretion in this regard, which is only exceeded when the child's welfare is specifically endangered. Only under this condition is the state entitled and obliged to intervene on the basis of its constitutional duty to protect. Accordingly, the German Ethics Council recommends that access to digital services which do not yet pose an unquestionable threat to the child's welfare should be regulated by parents. Parents should be comprehensively informed about the risks posed to their children by digital services, with the involvement of paediatricians, and should be better supported in various ways in fulfilling their responsibilities.

Firstly, there is a need to improve the technical options available to parents and guardians to restrict access to apps, functions and content, as well as total usage time, in a simple, secure and tailored manner. Such tools already exist for the most common mobile operating systems, but they are generally not easy to use and have limited functionality. To enable parents to make decisions that suit their child's individual development with a manageable amount of effort, devices should be configured so that, simply by entering an age, all digital content not intended for the age is initially reliably blocked. However, provided there are no mandatory restrictions, parents should then be able to unblock this content individually and as granularly as possible.

Secondly, every effort must be made to ensure that parents actually make use of these technical options. This requires clear guidance on how parents can effectively protect their children from digital dangers by using the relevant technical options. Furthermore, these tools must be designed and explained in such a way that even parents with little technical expertise can use them without difficulty. Where parents nevertheless require technical support, it must be ensured that they actually receive it. This could, for example, be provided through digital mentors arranged via family support services.

Thirdly, when deciding which digital services are suitable for their children, parents should be able to rely not only on the age guidelines provided by the providers themselves, but also on those from neutral institutions. To make this possible, an extension of the voluntary self-regulation system is particularly worth considering. Although recognised voluntary self-regulation organisations could not, due to the fast-paced nature of the internet, provide age ratings for every single service, they could certainly issue such ratings upon request for larger providers and platforms, which app marketplaces would then adopt.

Primary addressees: policymakers, operating system providers, service providers

5. Children and adolescents should be appropriately involved in the design of protection frameworks.

To ensure that decisions are not made solely *on behalf of* their children, but that their wishes and interests are also taken into account appropriately, parents should involve their children in decisions regarding access to digital services in a manner appropriate to their age.

Furthermore, children and adolescents should be appropriately involved in the design of general regulations on the protection of minors. Therefore, institutionalised participation of the affected

age groups is recommended in political decision-making on the protection of children and adolescents in the digital world. Structured participation – for example through youth councils, public hearings or participatory formats within parliamentary procedures – helps to better assess the proportionality and practicality of regulatory interventions. At the same time, it strengthens trust in state institutions and promotes political maturity.

Primary addressees: parents/guardians, policymakers (federal and state governments)

6. Blanket bans on the use of social media and other digital services based on new statutory minimum age limits should be avoided.

The German Ethics Council opposes the introduction of blanket minimum age limits for access to social media and similar services for four reasons. Firstly, a blanket age limit for digital technologies does not do justice to the fact that the risks associated with them do not arise generally for categories of service, but rather due to specific features such as infinite feeds, which could be disabled in youth-friendly versions. Secondly, children differ significantly in their level of maturity both within and between age cohorts. Thirdly, an exclusive focus on social media ignores risks posed by other digital services or those that may arise from children and adolescents circumventing a ban. And fourthly, a universally applicable minimum age would impair both the participation and the development of media literacy among minors, and would disproportionately interfere with parents' rights to individually balance their child's protection, participation and empowerment needs when it comes to access to digital services.

If, nevertheless, there was political support for a statutory minimum age for access to social media, a uniform solution at European level should be sought. National bans with potentially differing age limits could result in a regulatory patchwork across Europe, which would stand in the way of effective implementation and enforcement of the law.

Primary addressees: policymakers (European Commission, federal government, federal states)

7. Age assurance technologies should be more clearly regulated.

Where age-based access restrictions to services or content are applied, the decision on which age assurance methods to use should no longer be left to providers, but should be determined by legally binding requirements. Solutions must, firstly, be sufficiently reliable and tamper-proof, and secondly, have minimal side effects. If these two requirements cannot be met simultaneously, measures run the risk of either being ineffective or disproportionately infringing on fundamental rights. The choice of suitable age verification technology must also be proportionate to the risks posed to children and adolescents by the respective services or content. This leads to the following recommendations:

7.a Age assurance should primarily take place at the device level.

Age assurance carried out by providers can involve significant intrusions into users' privacy. Data-based estimation methods are particularly problematic, as they require either biometric data (age estimation) or invasive tracking (age inference), whereby comprehensive data from various sources is collated to create detailed profiles. The German Ethics Council therefore opposes the use of technologies for age inference or age estimation where data leaves the user's device. Instead, proof of age should primarily be stored at the device level in order to protect users' privacy.

Primary addressees: policymakers (European Commission), operating system providers

7.b Parental control systems should be the standard method of age assurance.

To protect children and adolescents from the various risks in digital contexts, access restrictions should primarily be implemented through parental control and consent mechanisms on user's devices (see Recommendation 4). This approach combines sufficient effectiveness with comparatively few side effects and also respects the primacy of parental freedom of education.

Primary addressees: policymakers (European Commission), parents/guardians, operating system providers

7.c Age assurance procedures at device level can be used as a supplementary measure.

As parental control mechanisms are only effective if parents use these functions, mandatory age assurance technologies on user's devices may be used as a second measure, depending on the area of application or the specific service. This involves checking whether users are of the required age to use a service, for example through age estimation via the camera or verification using official documents. However, given the sensitivity of biometric data in particular, it is important here that this data remains on the device and is used solely for age assurance. Even in the case of document-based verification, it is important that only the relevant age signal is transmitted.

Primary addressees: policymakers (European Commission), operating system providers

7.d Where there are heightened legal requirements for age verification, the EUDI Wallet is recommended, provided that non-linkability and selective disclosure of data are guaranteed.

To access certain content, particularly that which may not be made available to minors under the Criminal Code or Section 4 of the JMStV, providers must not only verify users' ages using official documents, but also ensure that the proof of age actually belongs to the person seeking to access the service. In such cases, the German Ethics Council recommends the use of the EUDI Wallet, provided that the requirements of the eIDAS 2.0 Regulation are fully met and the technical and infrastructural conditions for this purpose are in place. Under these conditions, the EUDI Wallet offers strong guarantees for the protection of users' privacy. Alternatives such as the Mini-Wallet or even showing a passport and one's face to a mobile phone camera should be rejected on grounds of security and privacy protection.

Primary addressees: policymakers (European Commission), research and development

7.e Specific technical requirements for age assurance technologies must be laid down by law.

When defining age assurance technologies or their characteristics, legislators should not limit themselves to general principles such as "privacy by design", as these are too abstract to prevent widely divergent implementations, some of which merely demonstrate formal compliance with data protection regulations despite deeply intruding on users' privacy.

Instead, legislators should, similar to the requirements in the eIDAS 2.0 Regulation, also establish the following minimum standards for age verification technologies as a whole: requirements regarding the separation of issuer and verifier roles and selective disclosure; the processing of biometric and identity data on the user's device or under the user's control; a ban on data storage beyond the purpose of age assurance; and compliance with publicly audited, disclosed cryptographic protocols.

Primary addressees: policymakers (in particular the European Commission)

8. Gatekeeping and market dominance should be actively countered.

Large platform operators might exploit regulations on the protection of minors to consolidate their market power or gatekeeper positions and expand data collection. Firstly, platform providers such as Google, Apple or Meta, which already possess verified identity data, could position themselves as trusted providers of age assurance and thus become identity and compliance brokers who tacitly centralise control once again. Secondly, age assurance technologies generate new data signals (age limits, time of verification, device information) that platforms can use for profiling and advertising. Legislators should ensure that requirements for age verification technologies do not inadvertently create new advantages for gatekeepers that undermine the objectives of the Digital Markets Act.

To counteract dominant positions, promote competition and, overall, create incentives for age-appropriate digital spaces, alternative digital platforms, services and offerings that comply with European values, standards and laws should be promoted. Policymakers can provide incentives here through research and innovation funding.

Primary addressees: policymakers as regulators and research funders, public administration as users, research, industry

9. Children and adolescents, but also the democratic process as a whole, must be better protected against forms of manipulative influence.

Digital spaces offer various actors opportunities for coordinated influence and manipulation. The spectrum ranges from covert advertising to propaganda and cognitive warfare, with the aim of undermining trust in democratic processes and institutions. Whilst these dangers affect everyone, young people are particularly vulnerable to them. Appropriate measures are therefore needed to minimise these risks, in order to protect minors, as well as the democratic community. Such measures include, for example, obligations on service providers to detect and contain botnets and other manipulative communication tactics, as well as crisis protocols for large-scale disinformation or hate campaigns.

Primary target groups: policymakers, public authorities, service providers

10. Scientific research into digital technologies, their consequences and risks should be expanded and strengthened.

In order to better understand and address the risks of digital technologies, access to platforms for scientific research should be improved. Given the great significance of digital technologies for children and adolescents, as well as the complexity and dynamism of developments, the German Ethics Council further recommends, in addition to fundamental ethical, legal and social science research, dedicated programmes for educational, psychological and medical research to monitor future developments in this highly dynamic field and respond to them on an empirically sound basis.

Primary target groups: research, industry, politics as regulator and research funder, public administration as user

11. The conditions for the acquisition of digital competence must be fundamentally improved.

To ensure the protection, participation and empowerment of children and adolescents in the digital world, effective measures are needed to strengthen the digital literacy of minors, but also

of teachers, specialists and, in particular, parents and guardians. Media education programmes, including those for these target groups, should therefore be promoted more strongly. For schools in particular, however, the aim cannot be to overload curricula even further. Rather, on the one hand, space must be created to engage with digital technologies themselves, but also with the new questions arising from them. On the other hand, pupils, teachers, parents and other stakeholders must be supported in developing their skills through tailored and flexible initiatives. This also includes safe and secure digital and analogue spaces where children and adolescents can learn, interact and experiment.

Primary target audience: policymakers (particularly at the regional level)

12. The private use of digital devices in schools should be largely restricted.

Compulsory schooling places a special responsibility on the state to design schools as protected spaces for learning, personal development and direct personal interaction. Given the manifold risks that the private use of digital technologies can pose to the concentration, learning processes and social interaction of pupils and teachers alike, it seems sensible to strengthen the school as a safe space by extensively restricting the private use of digital devices, as has already been implemented in some federal states. Such regulations could, for example, include implementation models in which private devices are handed in whilst pupils are at school. The use of digital technologies in the classroom should preferably take place on devices with youth-friendly settings. Breaks should once again provide more scope for non-digital social interaction.

Primary addressees: policymakers, in particular the federal states

13. Screen-free spaces and time should be strengthened.

For their mental and physical wellbeing, children and adolescents need screen-free time outside school to make room for analogue activities such as sport and exercise, time in nature, musical or other creative pursuits, and social interaction in physical spaces. Therefore, open spaces and leisure time for these activities should be promoted – for example, through schools that favour physical activity with active breaks and sports programmes, attractive youth and community centres, accessible club and cultural activities, and nature-based educational leisure programmes. Individual and family customs also play a central role here, for example family-friendly routines such as screen-free meals, shared offline time or digital downtime before bed.

Primary addressees: policymakers (particularly regional and local authorities), but also schools, clubs and parents

References

Age Check Certification Scheme (ed.) (2025): Age Assurance Technology Trial. Part A: Main Report. Available at https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_A_DIGITAL.pdf, accessed on 20 May 2026.

Agyapong-Opoku, Nadine; Agyapong-Opoku, Felix; Greenshaw, Andrew J. (2025): Effects of social media use on youth and adolescent mental health: a scoping review of reviews. In: *Behavioral Sciences*, 15 (5), 574. DOI: https://doi.org/10.3390/bs15050574.

Behre, Julia; Hölig, Sascha; Stöwing, Ezra; Möller, Judith (2025): Reuters Institute Digital News Report 2025. Findings for Germany. Leibniz Institute for Media Research | Hans Bredow Institute (Working Papers of the Hans Bredow Institute | Project Results). DOI: https://doi.org/10.21241/ssoar.102887.

Block, Hans; Riesewieck, Moritz (Dir.) (2018): The Cleaners. Farbfilm Verleih. Available at https://www.bpb.de/mediathek/video/273199/the-cleaners, accessed on 20 May 2026.

Brailovskaia, Julia; Buchmann, Johannes; Hertwig, Ralph; Metzinger, Thomas; Montag, Christian; Sadeghi, Ahmad-Reza; Schneider, Silvia; Spiecker gen. Döhmann, Indra; Waldherr, Annie (2025): Social media and the mental health of children and young people. Halle (Saale): German Academy of Sciences Leopoldina (Discussion). DOI: https://doi.org/10.26164/leopoldina_03_01307.

Brand, Alexander (2026): Mobile phone ban in schools – yes or no? The majority of young people are against it. *German School Portal*. Available at https://deutsches-schulportal.de/schulkultur/handyverbot-an-schulen-ja-oder-nein-was-sagen-die-studien, accessed on 21 May 2026.

Brüggen, Niels; Dreyer, Stephan; Gebel, Christa; Lauber, Achim; Materna, Georg; Müller, Raphaela; Schober, Maximilian; Stecher, Sina (2022): Risk Atlas. Growing up in the digital age. Thinking from the child's perspective. Acting with a view to the future. (2nd ed.). Bonn: Federal Agency for Child and Youth Protection in the Media. Available at https://www.bzkj.de/bzkj/service/publikationen/gefaehrdungsatlas-digitales-aufwachsen-vom-kind-aus-denken-zukunftssicher-handeln-aktualisierte-und-erweiterte-2-auflage--197812, accessed on 14 April 2026.

Bundestag parliamentary group Bündnis 90/Die Grünen (ed.) (2026): Better platforms for everyone – protecting and empowering young people. Available at https://www.gruene-bundestag.de/fileadmin/dateien/downloads/Beschluesse/Fraktionsbeschluss_Social_Media_04-2026.pdf, accessed on 20 May 2026.

Burns, Mary; Winthrop, Rebecca; Luther, Natasha; Venetis, Emma; Karim, Rida (2026): A new direction for students in an AI world: Prosper, prepare, protect. The Brookings Institution. Available at https://www.brookings.edu/wp-content/uploads/2026/01/A-New-Direction-for-Students-in-an-AI-World-FULL-REPORT.pdf, accessed on 29 May 2026.

CDU Germany (ed.) (2026): Motions and initiatives adopted at the 38th Party Conference of the CDU Germany. Available at https://www.cdu.de/app/uploads/2026/02/2026_02_26_Angenommene-Sach_und-Initiativantraege.pdf, accessed on 5 May 2026.

Common Sense Media (ed.) (2025): Social AI Companions. Common Sense Media. Available at https://www.commonsensemedia.org/sites/default/files/pug/csm-ai-risk-assessment-social-ai-companions_final.pdf, accessed on 05/05/2026.

Davis, Christopher G.; Goldfield, Gary S. (2025): Limiting social media use decreases depression, anxiety, and fear of missing out in youth with emotional distress: A randomised controlled trial. In: *Psychology of Popular Media*, 14 (1), 1–11. DOI: https://doi.org/10.1037/ppm0000536.

German Ethics Council (ed.) (2017): Big Data and Health – Data Sovereignty as a Means of Shaping Informational Freedom. German Ethics Council (Statement). Available at https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf, accessed on 21 May 2026.

German Ethics Council (ed.) (2023): Man and Machine – Challenges posed by Artificial Intelligence. German Ethics Council (Statement). Available at https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf, accessed on 20 May 2026.

Dreyer, Stephan (2025): The AI Regulation, its relationship to children's rights in the digital sphere and options for advocacy approaches. German Children's Fund (Series). Available at https://www.dkhw.de/filestorage/1_Informieren/1.1_Unsere_Themen/Kinder_und_Medien/Kinderrechte_und_KI/DKHW_Schriftenreihe_Kinderrechte_und_KI.pdf, accessed on 20 May 2026.

Eder, Maximilian; Sjøvaag, Helle (2024): Artificial intelligence and the dawn of an algorithmic divide. In: *Frontiers in Communication*, 9 (September), 1453251. DOI: https://doi.org/10.3389/fcomm.2024.1453251.

Eickelmann, Birgit; Fröhlich, Nadine; Bos, Wilfried; Gerick, Julia; Goldhammer, Frank; Schaumburg, Heike; Schwippert, Knut; Senkbeil, Martin; Vahrenhold, Jan (eds.) (2024): ICILS 2023 #Germany. Computer and information-related skills and computational thinking skills of school pupils in an international comparison. Münster: Waxmann. DOI: https://doi.org/10.31244/9783830999492.

Feierabend, Sabine; Rathgeb, Thomas (eds.) (2005): JIM Study 2005: Youth, Information, (Multi-)Media. Baseline study on media use among 12- to 19-year-olds in Germany. Media Education Research Network Southwest. Available at https://mpfs.de/app/uploads/2024/11/JIM_Studie_2005.pdf, accessed on 21 May 2026.

Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan (2025a): JIM Study 2025: Youth, Information, Media. Baseline study on media use among 12- to 19-year-olds. Media Education Research Network South-West. Available at https://mpfs.de/app/uploads/2025/11/JIM_2025_PDF_barrierearm.pdf.

Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan (2025b): KIM Study 2024: Childhood, Internet, Media. Baseline study on media use among 6- to 13-year-olds. Media Education Research Network Southwest. Available at https://mpfs.de/app/uploads/2025/05/KIM-Studie-2024.pdf, accessed on 05/05/2026.

Society for Innovative Market Research (ed.) (2022): Social Media as an Information Channel. Weighting study on the relevance of media for opinion formation in Germany, 2022–

Hunt, Melissa G.; Marx, Rachel; Lipson, Courtney; Young, Jordyn (2018): No more FOMO: limiting social media decreases loneliness and depression. In: *Journal of Social and Clinical Psychology*, 37 (10), 751–68. DOI: https://doi.org/10.1521/jscp.2018.37.10.751.

Institute for Youth Culture Research and Cultural Education (ed.) (2024): Beauty ideals on the internet. Saferinternet.at. Available at https://www.saferinternet.at/news-detail/neue-studie-schoenheitsideale-im-internet, accessed on 21 May 2026.

Institute for Youth Culture Research and Cultural Mediation (ed.) (2026): AI chatbots as everyday companions for young people. Saferinternet.at. Available at https://www.saferinternet.at/news-detail/neue-studie-ki-chatbots-als-alltagsbegleiter-fuer-jugendliche, accessed on 21 May 2026.

Joint Statement of Security and Privacy Scientists and Researchers on Age Assurance (2026):, 2 March 2026. Available at https://csa-scientist-open-letter.org/ageverif-Feb2026, accessed on 5 May 2026.

Kang, Cecilia; Mac, Ryan; Tan, Eli (2026): Meta and YouTube found negligent in landmark social media addiction case. In: *The New York Times*, 25 March 2026. Available at https://www.nytimes.com/2026/03/25/technology/social-media-trial-verdict.html, accessed on 21 May 2026.

Kang, Cecilia; Tan, Eli (2026): Meta ordered to pay $375 million over child safety violations. In: *The New York Times*, 24 March 2026. Available at https://www.nytimes.com/2026/03/24/technology/meta-new-mexico-child-safety-violations.html, accessed on 21 May 2026.

Kaye, Byron (2026): Australians reach for VPNs, find porn sites blocked as online age restrictions take effect. In: *Reuters*, 9 March 2026. Available at https://www.reuters.com/world/asia-pacific/vpns-up-porn-websites-down-australia-brings-new-online-age-restrictions-2026-03-09, accessed on 21 May 2026.

Kelly, Dominique (2025): Youth Perspectives on Privacy Dark Patterns. Western University. Available at https://hdl.handle.net/20.500.14721/37637, accessed on 5 May 2026.

Kieninger, Julia; Feierabend, Sabine; Rathgeb, Thomas; Gerigk, Yvonne; Glöckler, Stephan; Spang, Emil (2024): miniKIM Study 2023: Young Children and Media. Baseline study on media use among 2- to 5-year-olds in Germany. Media Education Research Network Southwest. Available at https://mpfs.de/app/uploads/2025/01/miniKIM-2023_PDF_barrierearm.pdf, accessed on 05/05/2026.

Kops, Maxime; Schittenhelm, Catherine; Wachs, Sebastian (2025): Young people and false information: A scoping review of responses, influential factors, consequences, and prevention programmes. In: *Computers in Human Behavior*, 169 (August), 108650. DOI: https://doi.org/10.1016/j.chb.2025.108650.

Kosmyna, Nataliya; Hauptmann, Eugene; Yuan, Ye Tong; Situ, Jessica; Liao, Xian-Hao; Beresnitzky, Ashly Vivian; Braunstein, Iris; Maes, Pattie (2025): Your brain on ChatGPT:

accumulation of cognitive debt when using an AI assistant for essay writing tasks. arXiv. DOI: https://doi.org/10.48550/arXiv.2506.08872.

Leisegang, Daniel (2026): A Google heart beats within the age verification app. In: *netzpolitik.org*, 7 May 2026. Available at https://netzpolitik.org/2026/europaeische-kommission-in-der-alterskontroll-app-schlaegt-ein-herz-von-google, accessed on 21 May 2026.

Livingstone, Sonia; Stoilova, Mariya (2021): The 4Cs: classifying online risk to children. CO:RE short report series: key topics. Hamburg: Leibniz Institute for Media Research | Hans Bredow Institute (CO:RE Children Online: Research and Evidence). DOI: https://doi.org/10.21241/SSOAR.71817.

Lueks, Wouter; Dreyer, Stephan; Federrath, Hannes; Simon, Judith (2026): Assessing age assurance technologies: effectiveness, side-effects, and acceptance. arXiv. DOI: https://doi.org/10.48550/arXiv.2603.25695.

Ma, Ili; Sultan, Mubashir; Kozyreva, Anastasia; Bos, Wouter van den (2026): Understanding the impact of misinformation on adolescents. In: *Nature Human Behaviour*, 10 (1), 18–28. DOI: https://doi.org/10.1038/s41562-025-02338-8.

Maier, Eva-Maria; Tanczer, Leonie Maria; Klausner, Lukas Daniel (2025): Surveillance disguised as protection: a comparative analysis of sideloaded and in-store parental control apps. In: *Proceedings on Privacy Enhancing Technologies* (2), 107–24. DOI: https://doi.org/10.56553/popets-2025-0052.

Marzolf, Émile; O'Regan, Ellen; Gkritsi, Eliza (2026): Brussels launched an age checking app. Hackers say it takes 2 minutes to break it. In: *Politico*, 17 April 2026. Available at https://www.politico.eu/article/eu-brussels-launched-age-checking-app-hackers-say-took-them-2-minutes-break-it, accessed on 05/05/2026.

Meineck, Sebastian (2026): Meta wants to monitor us down to the bone. In: *netzpolitik.org*, 7 May 2026. Available at https://netzpolitik.org/2026/du-siehst-aber-jung-aus-meta-will-uns-bis-auf-die-knochen-ueberwachen, accessed on 21 May 2026.

Molly Rose Foundation (ed.) (2026): Australia's social media ban – is it working? Molly Rose Foundation. Available at https://mollyrosefoundation.org/wp-content/uploads/2026/04/MRF_Australia-Social-Media-Ban-Research_Briefing-April-26.pdf.

Nuñez, Tania R.; Radtke, Theda (2024): Is socially disruptive smartphone use detrimental to well-being? A systematic meta-analytic review on being phubbed. In: *Behaviour & Information Technology*, 43 (7), 1283–1311. DOI: https://doi.org/10.1080/0144929X.2023.2209213.

OECD (ed.) (2026): OECD Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education. Paris: OECD Publishing. DOI: https://doi.org/10.1787/062a7394-en.

Orben, Amy; Meier, Adrian; Dalgleish, Tim; Blakemore, Sarah-Jayne (2024): Mechanisms linking social media use to adolescent mental health vulnerability. In: *Nature Reviews Psychology*, 3 (6), 407–23. DOI: https://doi.org/10.1038/s44159-024-00307-y.

Raffoul, Amanda; Ward, Zachary J.; Santoso, Monique; Kavanaugh, Jill R.; Austin, S. Bryn (2023): Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model. In: *PLOS ONE*, 18 (12), e0295337. DOI: https://doi.org/10.1371/journal.pone.0295337.

Rohleder, Bernhard (2023): How Germans use social media. Bitkom. Available at https://www.bitkom.org/sites/main/files/2023-02/BitkomChartsSocialMedia2023.pdf, accessed on 21 May 2026.

Salehi, Nasim; Marshall, Georgia Rose; Maziarfar, Mohammad Hossein; Zubrinich, Alice; Madani, Nazanin; Nickbakht, Mansoureh; Moustafa, Ahmed A. (2025): A double-edged sword perspective on young Australians' use of social media: a structured narrative review. In: *Health Promotion Journal of Australia*, 36 (4), e70093. DOI: https://doi.org/10.1002/hpja.70093.

Scheiter, Katharina; Bauer, Elisabeth; Omarchevska, Yoana; Schumacher, Clara; Sailer, Michael (2025): Artificial intelligence in schools. A guide to the current state of research and practice. Framework Programme for Empirical Educational Research. Available at https://www.empirische-bildungsforschung-bmbfsfj.de/img/KI_Review.pdf, accessed on 29 May 2026.

SPD Parliamentary Group (ed.) (2026): Safe Social Media. Strengthening the protection of children and young people in the digital space. Available at https://www.spdfraktion.de/system/files/documents/impulspapier-sichere-soziale-medien.pdf, accessed on 5 May 2026.

Stadler, Matthias; Bannert, Maria; Sailer, Michael (2024): Cognitive ease at a cost: LLMs reduce mental effort but compromise depth in student scientific inquiry. In: *Computers in Human Behavior*, 160 (November), 108386. DOI: https://doi.org/10.1016/j.chb.2024.108386.

Staksrud, Elisabeth; Livingstone, Sonia; Ólafsson, Kjartan (2026): Use, views and worries on age bans on social media: responses from 29,169 children in 19 European countries. LSE Research Online (EU Kids Online). DOI: https://doi.org/10.21953/researchonline.lse.ac.uk.00138705.

Steinebach, Martin; Jager, Tibor; Simon, Judith; Lehmann, Anja (2026): EU app for age verification. In: *Science Media Center Germany*, 17 April 2026. Available at https://www.sciencemediacenter.de/angebote/eu-app-zur-altersverifikation-26083, accessed on 05/05/2026.

Taylor, Josh (2026): VPN apps rocket up download charts in Australia as porn websites begin blocking users. In: *The Guardian*, 9 March 2026. Available at https://www.theguardian.com/australia-news/2026/mar/09/vpn-downloads-australia-porn-sites-blocking-users, accessed on 21 May 2026.

Ukrow, Jörg (2024): Child and Youth Media Protection and Artificial Intelligence – A Challenge for the State Treaty on the Protection of Minors in the Media (JMStV)? Current status and reform considerations with particular regard to generative AI and taking into account the EU's planned Artificial Intelligence Act. Commission for the Protection of Minors in the Media. Available at https://www.kjm-online.de/fileadmin/user_upload/KJM/Service/Publikationen/Studien_Gutachten/KI_Gutachten_2024.pdf, accessed on 20 May 2026.

Independent Expert Commission on ‘Child and Youth Protection in the Digital World’ (ed.) (2026): Stocktaking. Federal Ministry of Education, Family Affairs, Senior Citizens, Women and Youth. Available at https://www.bmbfsfj.bund.de/resource/blob/284628/c22a5e3075220368a8591bca19ff288b/20260420-exertenkommission-kinder-und-jugendmedienschutz-bestandsaufnahme-data.pdf, accessed on 21 May 2026.

Wiedemann, Hanna; Busch, Katharina; Schlichter, Nele; Gebhardt, Lucie; Paschke, Kerstin (2026): Between Fortnite, TikTok and ChatGPT: Media use, risks and new usage trends among children and young people in Germany. Results Report 2025/2026. DAK-Gesundheit. Available at https://www.dak.de/dak/unternehmen/reporte-forschung/dak-studie-mediensucht-2026_164552, accessed on 5 May 2026.

Wiedemann, Hanna; Thomasius, Rainer; Paschke, Kerstin (2025): Problematic media use among children and young people in Germany. Report on findings 2024/2025. DAK-Gesundheit. Available at https://www.dak.de/dak/unternehmen/reporte-forschung/dak-studie-mediensucht-2024_91442, accessed on 06/05/2026.

Scientific Services of the German Bundestag (ed.) (2006): The UN Convention on the Rights of the Child and its binding effect in the German legal system. German Bundestag (WD 2-160/06). Available at https://www.bundestag.de/resource/blob/414972/WD-2-160-06-pdf.pdf, accessed on 21 May 2026.

Scientific Services of the German Bundestag (ed.) (2026): On the restriction and prohibition of social media platforms. German Bundestag (WD 7-004/26). Available at https://www.bundestag.de/resource/blob/1158560/WD-7-004-26.pdf.

Yu, Yaman; Liu, Yiren; Zhang, Jacky; Huang, Yun; Wang, Yang (2025): Understanding generative AI risks for youth: a taxonomy based on empirical data. arXiv. DOI: https://doi.org/10.48550/arXiv.2502.16383.

PRELIMINARY VERSION

Members of the German Ethics Council

at the time of the adoption of the statement on 21 May 2026

Prof. Dr. iur. Helmut Frister (Chair)
Prof. Dr. rer. nat. Susanne Schreiber (Vice-Chair)
Prof. Dr. phil. Judith Simon (Vice-Chair)
Prof. Dr. med. Dr. phil. Eva Winkler (Vice-Chair)

Prof. Dr. Dr. h.c. Jutta Allmendinger
Prof. Dr. Rana Alsoufi
Prof. Dr. phil. Cornelia Betsch
Prof. Dr. iur. Hans-Georg Dederer
Dr. rer. nat. Uta Eser
Prof. Dr. Aldo Faisal
Military Bishop Dr. theol. Bernhard Felmberg
Prof. Dr. rer. pol. Nils Goldschmidt
Prof. Dr. theol. Elisabeth Gräb-Schmidt
Prof. Dr. med. Winfried Hardinghaus
Dr. phil. Ute Kalender
Hedy Kerek-Bodden
Prof. Dr. phil. Armin Nassehi
Prof. Dr. phil. habil. Annette Riedel
Prof. Dr. iur. Dr. phil. Frauke Rostalski
Prof. Dr. rer. soc. Dr. theol. Jochen Sautermeister
Prof. Dr. theol. Kerstin Schlögl-Flierl
Dr. med. Dr. h.c. Josef Schuster
Prof. Dr. phil. Mark Schweda
Prof. Dr. iur. Gregor Thüsing
Prof. Dr. Achim Wambach