STUDY

Requested by the CULT Committee

European Parliament

The influence of social media on the development of children and young people

Policy Department for Structural and Cohesion Policies
Directorate-General for Internal Policies
PE 733.109 - February 2023

EN

RESEARCH FOR CULT COMMITTEE

The influence of social media on the development of children and young people

Abstract

This study examines research on the impact of pervasive social media use on children's and young people's development. Acknowledging the many benefits children gain from being connected through social media, this study focuses on problematic use and the potential harm that may arise from content, contact, conduct and contract risks. Solutions are considered in light of EU policy and regulatory developments with particular reference to ensuring that children are protected, safe and empowered when they go online.

This document was requested by the European Parliament's Committee on Culture and Education.

AUTHOR

Prof. dr. Brian O'NEILL, Brian O'Neill Research

Research administrator: Kristiina MILT
Project, publication and communication assistance: Anna DEMBEK, Kinga OSTAŃSKA, Stéphanie DUPONT
Policy Department for Structural and Cohesion Policies, European Parliament

LINGUISTIC VERSIONS

Original: EN

ABOUT THE PUBLISHER

To contact the Policy Department or to subscribe to updates on our work for the CULT Committee please write to: Poldep-cohesion@ep.europa.eu

Manuscript completed in January 2023

This document is available on the internet in summary with option to download the full text at: https://bit.ly/3XkgYd8

This document is available on the internet at:
http://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)733109

Further information on research for CULT by the Policy Department is available at:
https://research4committees.blog/cult/
Follow us on Twitter: @PolicyCULT

Please use the following reference to cite this study:
O'Neill, B 2023, Research for CULT Committee – The influence of social media on the development of children and young people, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels
Please use the following reference for in-text citations:
O'Neill (2023)

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

CONTENTS

LIST OF ABBREVIATIONS

AADC	Age Appropriate Design Code
AI	Artificial Intelligence
AVMSD	Audiovisual Media Services Directive
BIK	Better Internet for Kids
COPPA	Children's Online Privacy Protection Act (US)
CO:RE	Children Online: Research and Evidence
DEAP	Digital Education Action Plan
DSA	Digital Services Act
EDAP	European Democracy Action Plan
EDMO	European Digital Media Observatory
EiD	European Digital Identify framework
GDPR	General Data Protection Regulation
HFSS	(Food products) High in fat, sugar or salt
JRC	Joint Research Centre
SIC	Safer Internet Centre
SID	Safer Internet Day
SIF	Safer Internet Forum
SNS	Social Networking Service
UCPD	Unfair Commercial Practices Directive
UNCRC	UN Convention on the Rights of the Child

LIST OF FIGURES

EXECUTIVE SUMMARY

This study examines the influence of social media on the development of children and young people. The study includes a literature review of research on European children's use of social media and a legal and policy analysis of the EU framework to address the negative effects on children's well-being.

Key findings

Social media are pervasive in the lives of European children and young people through which they encounter a diverse range of content, contact, conduct and contract risks. Solutions to the challenges that social media pose for children's development are not easily addressed given the complex way in which risks and opportunities are intertwined. In this study, the focus is on problematic use and the potential harm social media may have for children's development. However, the many benefits children gain from being connected through social media also need to be acknowledged.

Children are routinely exposed to harmful online content on social media platforms such as cyberhate, sexualised content, gory or violent images, content that promotes eating disorders, and disinformation. Harmful effects for children's development include potential increased aggression, problematic sexual behaviours, unhealthy eating habits, body image dissatisfaction and distorted values and attitudes. Some studies have also pointed to regular youth exposure to extremist content on social media though more research is needed on its effects. Media literacy and supportive family or peer environments have been found to be moderating influences.

Harmful online contacts with adults can give rise to risks of sexual exploitation, harassment and threats of extortion. Children generally report confidence in managing the risks of meeting new people online which is an everyday experience for many young people. However, studies highlight gaps in children's awareness of the risks and their coping strategies with unfamiliar situations. In addition, vulnerable children may be more at risk.

Conduct risks on social media platforms arise from aggressive or bullying peer-to-peer behaviour and have been found to have serious adverse effects for younger users. Being a victim of cyberbullying is a persistent risk that children face and is commonplace. Some associations with problematic social media use and bullying others have been found. Social-emotional learning, mentoring, and education on online safety have all played positive roles in countering victimisation risks.

Sexual messaging and sharing of sexual images, known to be increasingly normalised among young people, also gives rise to risks and potential harms. Unwanted requests for sexual information are a cause of distress for young people while the non-consensual sharing of intimate images is a source of severe harm and trauma.

Participation in harmful online communities (promoting self-harm, suicide etc.) is also a potential source of harm though other contributory factors to poor mental health also need to be considered.

Children face wide-ranging *contract risks* through unfair practices, clickbait strategies and hidden marketing practices that contravene their rights and ignore their best interests. Algorithm-based recommendation systems constitute a significant factor in increasing risks to children, with research showing that children have little awareness of how such systems work.

Children's *mental health and well-being* is a vital area to consider concerning social media. This is a complex area which involves many different and interrelated risk manifestations. The evidence for either a positive or negative impact on children's health and well-being is mixed and inconclusive. Probing the outcomes of problematic social media use – reported by only a minority of children – is an important priority for research.

Responses and solutions

Supporting children to be safe, protected and empowered when they go online is a cornerstone of EU digital policies, expressed most clearly in the Better Internet for Kids (BIK+) strategy adopted by the Commission in May 2022.

Significant legal and regulatory developments governing social media and online marketplaces include the Digital Services Act, the revised Audiovisual Media Services Directive, and the General Data Protection Regulation. The Unfair Commercial Practices Directive is also relevant to such areas as social media marketing and the activities of influencers. Legislative proposals under consideration including the Artificial Intelligence Act and the Regulation laying down rules to prevent and combat child sexual abuse also propose solutions with far-reaching consequences for children's online safety.

Internationally, a noteworthy trend in legislative and policy development has been to put an emphasis on children's rights in relation to the digital environment, reinforced by enhanced protection of children's privacy and digital service provider obligations towards safety by design and age appropriate design.

Alongside legal and policy frameworks, support for children's online well-being is recognised as a multistakeholder activity reflected in the many different programmes and initiatives carried out nationally and at the EU level to raise awareness, lessen the chance of children encountering risks and support children if they become victims of online harm.

Recommendations

Based on the findings of this study, the following recommendations are proposed:

- **Recommendation 1: Safety by design is an important concept that should be endorsed and promoted within regulatory discourse.** As the research illustrates, social media is pervasive in the lives of children and young people. In that context, social media environments should be designed to be safe from the outset. Appropriate standards for safety by design can ensure that safety is neither a retrofit nor an afterthought but instead is "baked-in" from the start.

- **Recommendation 2: Age-appropriate design has the potential to mainstream the safe, empowered and rights-respecting participation of young people and should be similarly promoted within the policy sphere.** As referenced in the study, the Commission's support for the development of an EU Code of conduct on age appropriate design is essential to develop this approach further. To ensure its widescale adoption, further work is needed to operationalise the relevant practical processes and monitoring mechanisms associated with such a code.

- **Recommendation 3: Continued development of privacy protections for children's data in the social environment is essential.** One of the distinctive areas of risk that children encounter relates to the data given off in the course of their social media use. Research shows that children often lack awareness of and the skills to manage these highly complex data ecosystems. The General Data Protection Regulation (GDPR) advances the position that children merit a higher bar of protection due to their evolving capacities. Yet, further development of processes, guidance and standards are needed to ensure best practices in supporting children's privacy in social media environments.

- **Recommendation 4: Age assurance and digital identity systems require multistakeholder support if barriers to their implementation are to be overcome and systems to be effective.** Many of the challenges children encounter in using social media arise when they are not appropriately identified as children, thereby meriting higher levels of protection. The lack of adequate and privacy-preserving age assurance mechanisms, as required under GDPR, contributes to this problem. Therefore, all relevant obstacles to developing and rolling out robust age assurance systems should be addressed.

- **Recommendation 5: To future-proof policies and to ensure that existing policies and initiatives are appropriate and effective, there is a need for a strong research observatory function at the European level.** The study called attention in several critical areas to the lack of or uneven evidence in some key areas regarding children's digital activities. The lack of sufficient comparative research at the EU level and longitudinal studies on children's development against the background of digitalisation stand out. Technologies can also quickly outpace policy and regulatory approaches creating new vulnerabilities for children. A greater volume of research on this topic is essential to keep pace with a rapidly evolving digital sphere.

1. INTRODUCTION

KEY FINDINGS

This study examines research on the impact of social media – now a pervasive feature in many children's lives – on their overall development and well-being. While acknowledging the many benefits children gain from using social media, this study focuses on problematic use and the potential negative impact social media may have on children's development.

Social media encompasses a wide range of services with many different functions. They are defined in this study as platforms and services that allow individuals and groups to create user profiles and connect their profiles with other users to share user-generated content.

As used throughout the study, child development refers to the physical, cognitive and social growth through which children mature to adulthood. However, it is important to note that no consensus model of child development exists. For this study, a child is any person under the age of 18.

The study applies the CO:RE classification of online risks (i.e., content, contact, conduct and contract risks) to the review of literature on potential problems children may encounter through their use of social media. The OECD (2021) revised typology of risks is also referenced as a relevant framework. The approach to selecting the most relevant literature is also outlined.

1.1. Background to the study

Social media have a pervasive place in the lives of children and young people today and are central to how they incorporate digital technologies into their everyday lives. While interactivity and sharing content has always been a central feature of the internet, the rise of social media platforms over the last two decades and the easy access provided by smartphones have done more to drive digital adoption among children than almost any other aspect of digitalisation. Constantly evolving and deepening their integration into nearly every facet of daily life, social media and the underlying model of social networking continue to shape and transform the experience of billions of users across the globe.

This study concerns children and young people's engagement with social media. Social media has a unique ability to combine communication, content sharing and the ability to network with friends and peers, making it highly attractive to young people. Children indeed are often early adopters of new social media services and the first to try out the latest apps and services (Hofstra et al., 2016). The popularity of platforms such as YouTube, TikTok, Instagram and Snapchat amongst children and teenagers is confirmed worldwide (Vogels et al., 2022) and in the EU, nearly all adolescents aged 15 to 16 use social media daily (Smahel et al., 2020).

Alongside their popularity and the many benefits young people gain through social media, their pervasiveness also raises concerns as to the potential adverse effects that sustained use may have on children's development. Against the backdrop of issues such as persistent cyberbullying or an apparent mental health crisis among youth, this study seeks to give an overview of research on social media's effects on children and young people's development. While recognising that children have many positive experiences using social media, the central focus here is on evidence for problematic use and harmful outcomes regarding their development and well-being.

1.2. Scope of the study and definitions

The volume of research literature on children and the digital environment, both from the scientific world and the broader policy and practice domains, is large. To narrow its scope, the study is limited to considering social media platforms rather than all digital services and technologies used by young people. Secondly, the study focuses on a review of the impact on children's development and well-being. It does not, for instance, consider other aspects of children's use, such as the use of digital technologies in education or for purely entertainment or leisure purposes, except insofar as these have developmental relevance. These boundaries, of course, are not fixed, nor is social media use always so clearly demarcated in young people's lives.

The term social media, as used throughout the study, refers to *platforms and services that allow individuals and groups to create user profiles and connect their profiles with other users for the purposes of sharing user-generated content*. This general descriptor draws on the synthesis of definitions offered by Obar and Wildman (2015). It also aligns with the definition provided by McCay-Peet & Quan-Haase (2017) in a similar synthesis of the literature:

> Social media are web-based services that allow individuals, communities, and organizations to collaborate, connect, interact, and build community by enabling them to create, co-create, modify, share, and engage with user-generated content that is easily accessible. (McCay-Peet & Quan-Haase, 2017, p. 5)

Given its dynamic and evolving nature, there are challenges to offering a fixed definition of social media. Where previously, social networking service (SNS) was the term more commonly used to describe applications providing the ability to connect and share content, the broader term of social media is more widely used to refer to the many platforms available to consumers, each offering distinct features and types of use, often tailored to different user communities. For example, McCay-Peet & Quan-Haase (2017) identify ten different types of social media that include such diverse types as social networking, microblogging, media sharing, social news, collaborative authoring and web conferencing encompassing well-known diverse services such as Facebook, LinkedIn, Twitter, Tumblr, WordPress, Flickr, Pinterest, Zoom etc.

Social media offer a variety of modes of engagement that allow users to create, share content, and interact with other users in the network in different ways according to the design of the platform or service. Some platforms, such as Twitter or YouTube, may be more one-way in terms of the flow of information and may not need reciprocation in terms of engagement. In contrast, social networking services such as Instagram or TikTok encourage greater user interactivity with others they connect with. Of note here is the role private communication services play within social media. While personal communication is an intrinsic feature of many social media platforms, communication services such as WhatsApp, Viber or WeChat are more properly messaging services rather than social media. Their inclusion here is considered only from the point of view of social connectivity between young people, often in conjunction with other social media platforms.

The other central concept deployed throughout the study is that of child development. Child development refers to the physical, cognitive, and social growth that humans typically follow, beginning at birth and continuing as they grow and mature from infancy through adulthood. Child and adolescent development is a very large field of study with a range of theories regarding the different stages of development through which children mature and which vary according to the degree of emphasis given to various developmental milestones. From classic Piagetian theoretical frameworks of stages of cognitive development to other approaches, such as that of Erikson or Bronfenbrenner, that emphasise the social nature of children's development, there is no single consensus model of development or definitive account of the stages of child and adolescent development. Indeed, a focus of much recent scholarship in childhood studies is the constructed, culturally specific and socially determined basis of childhood which should properly be seen as *"an interpretive frame for contextualising the early years of human life"* (James & Prout, 1997). This, allied with the diverse perspectives on the study of the role of digital culture in childhood, adds further complexity to how such relationships should be contextualised (Coulter, 2021).

Despite this complexity, there exists a vibrant intellectual field for researchers to draw on when studying the relationship between digital technology use and children's development that is widely featured across the range of academic research cited in this study. It remains a constant reminder to assess the assumptions and underlying frameworks for assessing any conclusions drawn within a profoundly complex and multifaceted subject.

Of particular interest in this study is the way in which social media use integrates with – either assisting or hindering – the development tasks associated with adolescence. The World Health Organization defines adolescence as the phase of life between childhood and adulthood, from ages 10 to 19 and which coincides with rapid physical, cognitive and psychosocial growth[1] [2]. Adolescence is a vitally important time in people's lives in which they develop an independent sense of self and identity separate from their families and negotitate increasingly complex social relationships (Ogders et al., 2022). According to Havighurst's classic developmental theory, developmental tasks associated with adolescence include developing new and more mature relationships with peers of both sexes, developing one's own gender identity, accepting one's body image and using the body effectively, achieving emotional independence of other adults, preparing for future relationships, an economic career, acquiring a set of ethical values and achieving socially responsible behaviour (Havighurst, 1972; see also Manning, 2002). Given the pervasiveness of social media use among young people, activities around such developmental tasks take place as much online as offline and indeed the distinction between the physical and the digital for young people is increasingly blurred and irrelevant.

1.3. Approach to the review of literature

To manage the substantial volume of literature in the general field of children's engagement with media and digital culture more effectively, this study draws on two major theoretical constructs that are used to organise the source material.

Firstly, the study adopts the EU Kids Online conceptual framework of children's engagement in the digital environment. Over several iterations, the EU Kids Online project[3] has developed an original theoretical model for studying children's online experiences. The model, as revised in 2015 (Livingstone

[1] https://www.who.int/health-topics/adolescent-health

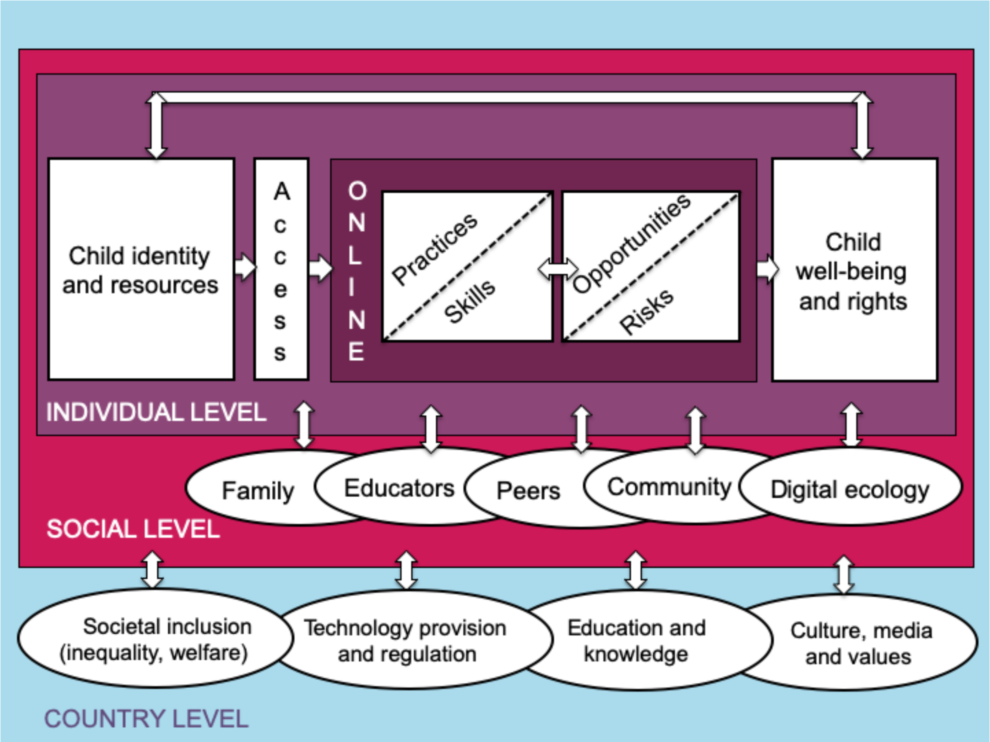
[2] Note, for the purposes of this study, that a 'child' is defined as any person under the age of 18 years as set out in the UN Convention on the Rights of the Child (UNCRC). The term 'young people' is used more generally to refer from approximately 10 years and upwards, coinciding with the WHO definition.

[3] http://www.eukidsonline.net/

et al., 2015) (Figure 1), is focused on the role that digital technology and connectivity play, for better or for worse, in children's well-being.

As outlined in this model, children's engagement in the digital environment and their use of social media for this study is set within a context of nested, interconnected factors that go from the individual to the social and the country level. These shape how children engage with the digital world, the resources available to them, the nature of the practices undertaken, and the associated competences, leading to opportunities availed of or risks experienced, ultimately to a consideration of the outcomes, their well-being and their rights. While the model does not explicitly refer to child development, its connection of children's identity and resources (their age, gender, psychological characteristics, capacities, interests, motivations, life experiences or vulnerabilities) encompass the evolving capacities of the child and allows the overall approach to be applied within a developmental context (Varadan, 2019).

Figure 1: EU Kids Online Conceptual Model

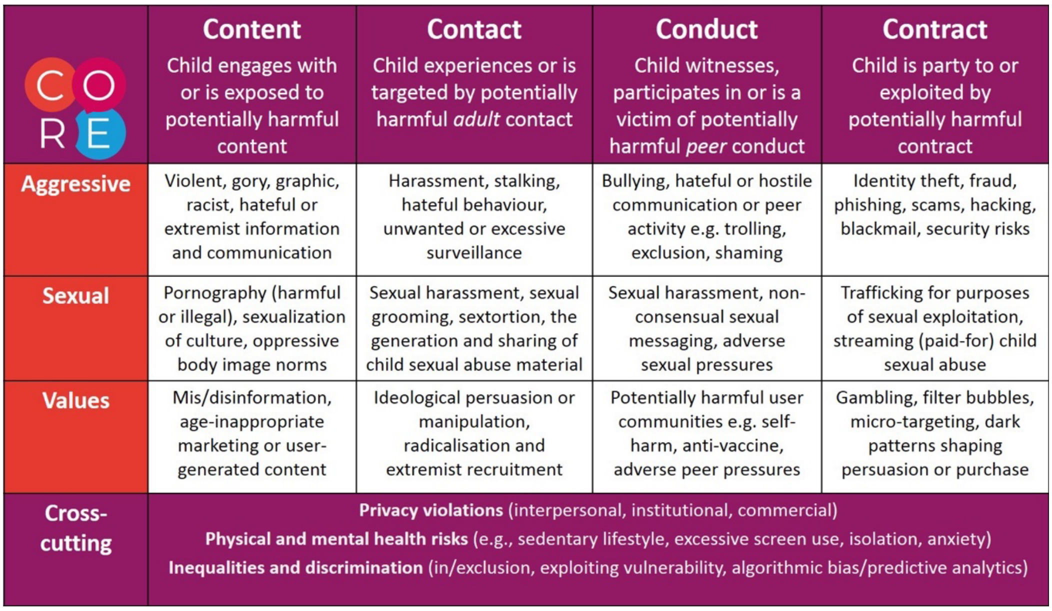

Child identity and resources
Access
ONLINE
Practices
Skills
Opportunities
Risks
Child well-being and rights
INDIVIDUAL LEVEL
Family
Educators
Peers
Community
Digital ecology
SOCIAL LEVEL
Societal inclusion (inequality, welfare)
Technology provision and regulation
Education and knowledge
Culture, media and values
COUNTRY LEVEL

Source: EU Kids Online (Livingstone et al., 2015)

The second theoretical construct that the study draws on is the classification of online risks to children as developed by the EU-funded CO:RE Children Online: Research and Evidence project (Figure 2)[4] as also set out in the revised typology of risks created by the OECD (2021) (Figure 3).

[4] https://core-evidence.eu/

Figure 2: CO:RE Classification of Online Risks



	Content Child engages with or is exposed to potentially harmful content	Contact Child experiences or is targeted by potentially harmful *adult* contact	Conduct Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	Contract Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

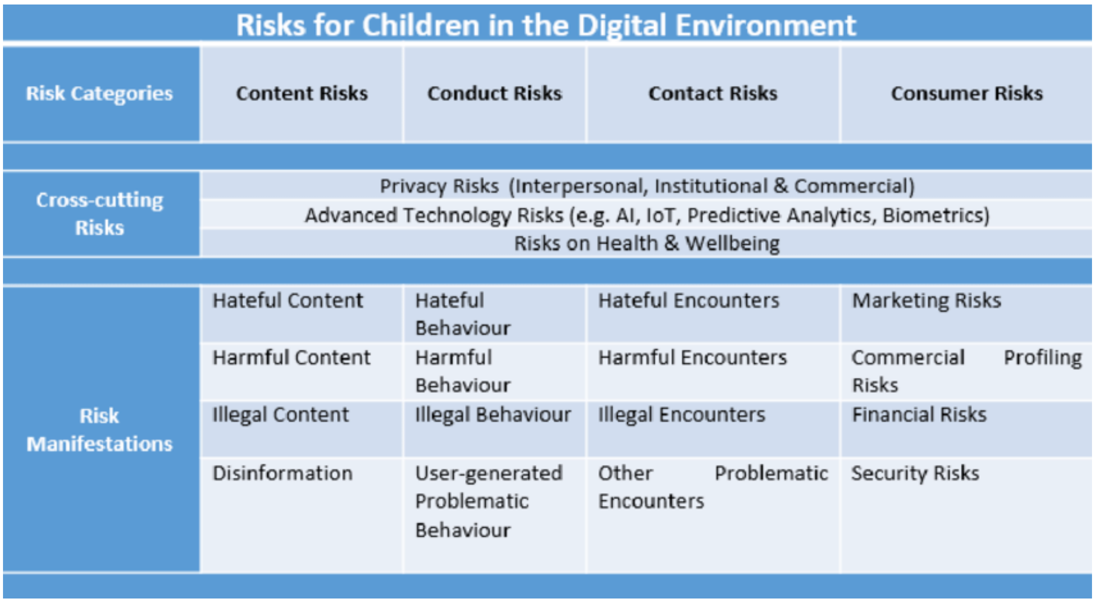
Source: CO:RE Children Online: Research and Evidence

The CO:RE '4Cs' model of content, contact, conduct and contract risks is a comprehensive classification of online risks that is research based and which seeks to disaggregate risks and raise awareness of the wide array of challenges children may face online (Livingstone & Stoilova, 2021).

The model updates the original EU Kids Online classification of risks (Livingstone & Haddon, 2009) which distinguished between *content*, *contact* and *conduct* risks. The approach has been widely used by practitioners and policymakers in framing responses to the most commonly experienced problems children encounter when they go online. In updating the classification, a fourth 'C' of contract risks has been added to reflect the specific issues posed by commercialisation and datafication and to reflect the many profound changes which have taken place in the digital environment since the typology was first created.

The OECD typology (Figure 3) offers a similar approach (OECD, 2021). Contract risks are described as consumer risks in the OECD typology to convey the wide range of contexts in which children are exposed to online commercialised messaging for which they may be ill-prepared. The OECD typology also includes a range of cross-cutting risks such as privacy violations, technology-based risks and risks to health and well-being that are highly relevant to the study of children's social media use.

Figure 3: OECD Revised Typology of Risks



Risks for Children in the Digital Environment

Risk Categories	Content Risks	Conduct Risks	Contact Risks	Consumer Risks
Cross-cutting Risks	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

Source: OECD and Berkman Klein Center for Internet and Society at Harvard University

These high level overviews of the different types of risks that children face in the digital environment are important in guiding policy and prioritising online safety interventions in areas where there is the most compelling evidence of harm. It is also an evolving framework enabling researchers and other stakeholders to track new risk types as they emerge, adjusting the framework as necessary.

For this study, a rapid evidence review was undertaken to search for the most relevant recent research on children and young people's experiences of risks on social media as set out within the CO:RE classification. Keyword searches for associated risks were conducted using the CO:RE Evidence Base[5] as well as standard databases including Web of Science and Google Scholar. An advantage of using the EU-funded CO:RE Evidence Base is that it references scientific research projects and publications specifically from across Europe in the area of children online, thereby facilitating access to research results that may not feature as prominently in international databases. Criteria for the selection of relevant studies included:

- Publications based on primary quantitative or qualitative research with children under 18 years in European countries
- Review articles including systematic reviews of research and evidence on children's online risks
- Published since 2018 to take account of the most recent research within the last 5 years
- High-quality research based on robust methodology and preferably published in a peer-reviewed journal

Some flexibility was adopted to include studies outside these criteria, such as some international studies of a systematic nature, studies before 2018 of European significance and relevant grey literature focused on the topic of children's social media use. Using the above criteria, a total of 207 studies were coded and summarised for the review.

[5] https://base.core-evidence.eu/

Following this Introduction, Section 2 of the study *Impact of Social Media: An Evidence Review* presents the main findings organised around the CO:RE classification of online risks. Here, the main findings related to social media harms are reviewed and summarised from the perspective of impact on children's development, noting where the evidence is most stark and where there remain outstanding research issues. *Section 3* of the study outlines the EU policy and regulatory framework most relevant to promoting children's online safety and well-being, paying particular attention to policy that addresses social media platforms. By way of further context, developments and trends at the international level are also noted. *Section 4, Responses and Solutions,* considers the main programmes and interventions that have evolved at the EU level to mitigate risks to children. Finally, *Section 5, Conclusions and Recommendations,* summarises the main findings of the study and provides a set of policy recommendations for EU policymakers, first and foremost for Members of the European Parliament, on what can be done, especially at the EU level, to better protect children and young people from the harmful effects of social media.

2. IMPACT OF SOCIAL MEDIA: AN EVIDENCE REVIEW

KEY FINDINGS

Content risks include exposure to harmful online content on social media platforms, something that is often reported by European children. Examples include exposure to cyberhate, content on eating disorders, sexual content and disinformation.

- Exposure to sexual content has given rise to much public concern though the evidence for its harm is mixed.
- Poor mental health in adolescents and extreme pornography use may be associated, but other variables must also be considered.
- Social media use in the context of body image dissatisfaction can be particularly problematic though media literacy and supportive family or peer environments have been found to be moderating influences.
- Gaps in children's media literacy skills to combat disinformation are a further content concern.

Contact risks refers to potential harmful contact from adults and includes risks of sexual exploitation, harassment and threats of extortion.

- Meeting new people online is an everyday experience for children and many report confidence in managing the risks of making new online contacts. However, studies highlight gaps in children's awareness of the risks and their coping strategies with unfamiliar situations. In addition, vulnerable children may be more at risk.
- Some studies have also pointed to regular youth exposure to extremist content on social media though more research is needed on its effects.

Conduct risks arise from problematic peer-to-peer behaviour.

- Being a victim of cyberbullying is a persistent risk that children face and is commonplace. Some associations with problematic social media use have been found. Social-emotional learning, mentoring, and education on online safety have all played positive roles in countering victimisation risks.
- Sexual messaging and sharing of sexual images are increasingly normalised among young people but give rise to various risks and potential harms. For example, unwanted requests for sexual information are a cause of distress for young people. At the same time, the non-consensual sharing of intimate images is a source of severe harm and trauma.
- Participation in harmful online communities (promoting self-harm, suicide, etc.) is also a potential source of actual harm though other contributory factors to poor mental health also need to be considered.

Contract risks are also routinely experienced by children.

- These include unfair practices, clickbait strategies and hidden marketing practices that contravene their rights and ignore their best interests.
- Algorithm-based recommendation systems constitute a significant factor in increasing risks to children, with research showing that children have little awareness of how such systems work.

Children's *mental health and well-being* are also vital to the study of social media and children. This complex area involves many different and interrelated risk manifestations. The evidence for either a positive or negative impact is mixed and inconclusive. Probing the outcomes of problematic social media use – reported by only a minority of children – is an important priority for research.

Social media are pervasive in the lives of children and young people and are followed by millions of children worldwide. Children often begin their journey with social media at an early age, sometimes on services that are not designed for their age group. Signing up for a social media service is often an important milestone for many children, sometimes coinciding with significant developmental stages such as adolescence, transitioning to the next stage of schooling and socialising more independently with peers.

This section of the study reviews relevant research on European children's experiences with social media. The available research on children's social media use is large, even if accurate and up-to-date statistics are somewhat uneven. Projects such as the EU-funded CO:RE knowledge base[6] have made research more accessible. However, apart from the occasional series of comparative surveys from EU Kids Online[7], there is still no single, consistent source of data on children's social media or digital technology use across the EU. As outlined in the Introduction, the focus in this section is on those aspects of social media that may negatively impact children's development while acknowledging the many positive benefits and the enjoyment children get from social media.

2.1. Social media in the lives of children

Using digital technologies, going online and connecting through social media is something that research shows is deeply integrated into children's daily lives. For example, the EU Kids Online survey of 19 countries across the EU found that an average of 80% of children aged 9 to 16 go online daily using a smartphone. In 2020, children reported spending between 2 to 3.5 hours on the internet, a finding that has almost doubled since the first EU Kids Online survey in 2010 (Smahel et al., 2020).

As reported in successive EU Kids Online studies, social media use has changed consistently over time, with children migrating from Facebook to other platforms such as Instagram or instant messaging services like WhatsApp (Smahel et al., 2020, p. 28). The number of children aged 9–16 who report using social network sites daily or more often ranges between 38% (Spain) and 73% (Serbia). However, this is likely to be a low estimate given that in many countries, children might use platforms that they do not identify as social network sites.

Social media use is also strongly structured by age, with most 15- to 16-year-olds (77%) reporting doing so daily. At the same time, 28% of 9–11-year-olds and 63% of 12- to 14-year-olds use social media daily despite the minimum age of 13 years for most platforms. Watching video clips, mainly through video-sharing platforms, remains the most popular online activity and is taken up by two-thirds of children in most countries daily (Smahel et al., 2020, p. 26).

While EU Kids Online is the main comparative data source across Europe on children's use of digital technologies, regional and national studies echo many of these findings and provide added insights into children's social media use. Some selected examples include:

- Austria's Youth Internet Monitor[8] found in 2022 that WhatsApp (96%), YouTube (95%) and Instagram (81%) were the most popular online platforms among Austrian young people (aged 11-17) in 2022. TikTok and Snapchat were equally popular with 11–17-year-olds, but in terms of daily use, 77% of Austrian young people say they use TikTok daily.

[6] https://core-evidence.eu/

[7] http://www.eukidsonline.net/

[8] SaferInternet.at (2022). Youth Internet Monitor 2022.

- A 2016 nationally representative study in Bulgaria of children aged 9-16 years for Global Kids Online[9] found social networks to be the second most popular online activity after watching videos. 86% of young people had a profile on social media, with Facebook, Messenger, Viber, Instagram and Snapchat as the most used services.
- A 2019 national study in Croatia on social media and young people's mental health[10] reported that a third of adolescents use social media for 3-5 hours daily. One in five spends more than 5 hours daily on social media. Almost one in four adolescents created their first profile on a social network at age 12. Approximately one-third (30%) of adolescents created their first profile on a social network at age ten or younger.
- Denmark's media development monitoring report, Internet Use and Social Media 2021[11], reported that 99% of 12–18-year-olds have a profile on at least one social media. In addition, 46% of this age group have between 2 and 5 profiles, while 41% have profiles on 6-8 social media platforms.
- In Flanders, the top 5 platforms used by children (6-12) are YouTube (86%), Netflix (68%), TikTok (56%), Spotify (52%) and WhatsApp (45%). Among young people (12-18), YouTube (96%), WhatsApp (91%), Snapchat (91%), TikTok (86%) and Instagram (83%) are the most popular platforms[12]. The same research found that around a fifth of children and a quarter of young people spend one to two hours daily (on schooldays) using social media.
- In Germany, the Southwest Media Education Research Association has regularly conducted a nationally representative study on children aged 6 to 12 on the role of media in their daily lives. The KIM study is a long-term project that maps children's constantly changing media environment. The KIM Study 2018[13] found that at age 9, three out of five children are online, rising to four out of five among 10–11-year-olds and 94% of 12–13-year-olds. 73% of 10- to 11-year-olds and 83% of 12- to 13-year-olds use WhatsApp daily (6-7 years: 17 %, 8-9 years: 36 %). Overall, one in every three children reports using a messenger service every or almost every day.
- Research carried out by the Greek Safer Internet Centre in 2018 found that 86% of Greek children aged 10 to 17 had a profile on social media[14]. 70% created a profile before the age of 13. 34% of children with social media profiles created them on their own without the consent of their parents.
- Ireland's National Advisory Council for Online Safety reported in 2021 that 62% of children aged 9-17 have at least one profile on a social media or gaming site[15]. A quarter (26%) of 9–10-year-olds reported having a social media profile; this rose to just under half, or 45% of 11–12-year-olds; three-quarters or 73% of 13–14-year-olds and 87% of 15–17-year-olds. Findings for 9–10-year-olds with their own social media profile rose from 14% in 2010 to 26% in 2020. Among 11–12-year-olds, this rose from 39% in 2014 to 45% in 2020.

[9] SaferNet.bg Online Experiences of Children in Bulgaria.

[10] Polyclinic for the Protection of Children (2019). Social online experiences and mental health of young people.

[11] Kulturministeriet (2021). Internet and Social Media 2021. (Summary in English).

[12] Apestaartjaren (2022) Report – Digital Lives of Children and Young People (in Dutch).

[13] Medienpädagogische Forschungsverbund Südwest (mpfs). KIM Study 2018. (In German).

[14] Greek Safer Internet Center (2018). Online Behaviour of Students Aged 10-17 Years Old In Greece. (In English).

[15] National Advisory Council for Online Safety (2021). Report of a National Survey of Children, their Parents and Adults regarding Online Safety.

- In Norway, the Norwegian Media Authority found that 90% of 9–18-year-olds use social media in 2022. 48% of 9-year-olds, 56% of 10-year-olds and 85% use one or more social media in 2022. Of the 9–11-year-olds, 40% are on TikTok; 24% are on Snapchat, and 7% are on Instagram. YouTube is used by 9 out of 10 of all 9–18-year-olds[16].

Research carried out by Ofcom, the United Kingdom's communications regulator, found that a majority of children under 13 had their own profile on at least one social media app or site; 33% of parents of 5-7-year-olds said their child had a profile, and 60% of 8-11-year-olds said they had one (Ofcom, 2022). Four in ten parents of 8-11-year-olds also said they would allow their child to use social media (38%)[17].

Internationally, the Pew Research Centre in the United States – which has some of the most comprehensive research on social media trends among teenagers – similarly found in 2022 that YouTube was used by 95% of teens, followed by TikTok (67%), Instagram (62%), and Snapchat (59%). Facebook (32%) is the next most popular platform, having previously been the most popular in 2015. Other platforms with smaller shares of this demographic group are Twitter, Twitch, WhatsApp, Reddit and Tumblr[18].

All such monitoring studies show some similarity in trends observed, such as more intensive use over time which is also strongly associated with age. For example, there is widespread evidence of children being active on social media from an early age, with significant numbers under the minimum age set by most social media platforms and increasing trends towards a diversity of services, incorporating various forms of video, photo-sharing and communications functionality. Accordingly, social media provides access and opportunity on an unprecedented scale for children to explore, communicate and participate in online communities. As the most popular and interactive online experience that children are likely to experience, it is also the most likely context in which children will engage in or be exposed to risks related to potentially harmful content, contact with others, conduct among peers or exploitative contracts or consumer risks.

2.2. Risks of harm through exposure to harmful content

Through social media, children may engage with or be exposed to potentially harmful content of different forms and of varying degrees of severity. The CO:RE classification of online risks distinguishes between the *aggressive*, *sexual* and *values-based* nature of online risks (Livingstone & Stoilova, 2021). The OECD Typology recognises four risk manifestations under content risks: i) hateful content; ii) harmful content; iii) illegal content, and iv) disinformation (OECD, 2021, p. 7). The primary purpose of such classifications is to provide common terminology to report findings and to map the available evidence. The classification of risks is also intended to be flexible so that new and emerging risks can be highlighted and positioned according to a diverse array of children's problematic online experiences.

2.2.1. Hateful and aggressive content

There are many different types of content that may be harmful to children's physical, emotional, cognitive or social development. Here the focus is on types of harmful content a child may encounter

[16] Medietilsynet (2022). Available in Norwegian at Children and young people's use of social media 2022.

[17] Ofcom (2022). Children and parents: media use and attitudes report 2022

[18] Vogels, E., Gelles-Watnick, R., & Massarat, N. (2022). Teens, Social Media and Technology 2022.

on social media platforms, i.e., user-generated content and some harmful content that may be professionally produced. For example, violent, gory, graphics, racist, hateful or extremist information and communication are among the forms of hateful and aggressive content that research has shown that children have experienced online.

The EU Kids Online 2020 survey examined six different types of harmful online content children may encounter (Smahel et al., 2020, p. 61). In summary:

- Hate messages were the most widely reported, experienced by an average of 17% of 12–16-year-olds at least monthly. This ranged from 4% in Germany to 48% in Poland.
- Seeing gory or violent images at least monthly was reported by 13% of 12-to-16-year-olds. This ranged from 6% in Slovakia and Germany to 28% in Poland.
- 12% reported encountering pro-anorexic content that promoted ways to be very thin.
- 11% reported seeing content of others sharing their experiences of taking drugs.
- 10% reported seeing self-harm content that depicted ways for young people to physically hurt or harm themselves.
- 8% reported seeing content that demonstrated ways of committing suicide.

When asked, children also report that experiencing, and witnessing hateful, vulgar, or nasty messages are among the top problematic experiences they encounter. Although less covered in the risk literature, some of these messages involve being killed, cursed, excluded, and verbally assaulted in online games (Smahel & Wright, 2014).

Recent evidence shows that young people encounter numerous instances of **hateful online content**. National and cross-national studies have shown that exposure to hate speech is common among young people, experienced more often by older teenagers than younger children (Blaya et al., 2022; Reichelmann et al., 2021). 28% of children reported an increase in witnessing cyberhate during COVID-19 lockdown periods (Joint Research Centre, 2021, p. 26). Cyberhate exposure is the experience of encountering hateful content online but not necessarily feeling victimised by it. Cyberhate victimisation is when people are targeted by malicious content online and is much less prevalent than exposure to cyberhate content (Machackova et al., 2020).

While EU Kids Online has found daily or weekly victimisation to be less than 2%, the UK Safer Internet Centre (SIC) has reported that 24% of 13–18-year-olds experienced being targeted with online hate because of their gender, sexual orientation, race, religion, disability or transgender identity (UK SIC, 2016). One in twenty-five (4%) say this happens all or most of the time. Being a victim of cyberhate is positively associated with risky activities (contact with unknown people, witnessing cyberhate, excessive internet use, lack of parental oversight etc.) (Wachs et al., 2021). However, cyber hate and racist stereotyping have also been found to be routinised on many social media platforms, including those likely to be used by children such as TikTok, and where there is a lack of clear and transparent community standards or moderation processes (Matamoros-Fernández et al., 2022; O'Connor, 2021; Weimann & Masri, 2020). Measures of harm from exposure to hateful content, such as being disturbed by the content, vary and indicate that those already vulnerable are the most strongly impacted (Savimäki et al., 2020).

Content related to **problematic eating habits and eating disorders**, such as anorexia or bulimia, has raised concerns about their harmful developmental impact, significantly affecting teenage girls.

According to EU Kids Online, the number of children who see ways to be very thin on the internet varies across countries, ranging between 3% (Germany) and 32% (Poland), with an average of 12% across European countries reporting seeing this type of content at least every month or more often (Smahel et al., 2020, p. 64). The literature makes several connections between exposure and feelings of negative body image:

- Systematic reviews of social media in the context of body image have indicated some correlational connection between social media use, body dissatisfaction and disordered eating among adolescents. Activities such as viewing and uploading photos and seeking negative feedback via status updates were identified as particularly problematic (Holland & Tiggemann, 2016) though the need for more longitudinal and experimental studies was noted.
- A systematic review of studies of social media and food choices in healthy young adults (Rounsefell et al., 2020) identified that social media engagement or exposure to image-related content negatively impacted body satisfaction and healthy eating. Five themes were highlighted in the literature as follows: (i) social media encourages comparison between users, (ii) comparisons heighten feelings about the body, (iii) young adults modify their appearance to portray a perceived ideal image, (iv) young adults are aware of social media's impact on body image and food choices, however, (v) external validation via social media is pursued.
- Self-presentation on social media is frequently central to young people's developing identity. Many people post photographs of their bodies in ways that conform to particular body ideals, such as through selfies and filters (Burnette et al., 2017). Some evidence exists, however, for the protective role that media literacy might afford (Paxton et al., 2022).
- A study of teenage girls in Ireland (mean age 15.16 years) found a significant relationship between appearance-related activity (e.g., looking at photos of friends) on social media and body dissatisfaction among adolescent girls (Scully et al., 2020). Body dissatisfaction was significantly related to the time spent in social comparisons while evaluating oneself less favourably than the target group of close friends was most strongly associated with poorer body image appraisals.

Research on exposure to cyberhate and body image-distorting content highlights the important moderating role of supportive family and peer environments. Görzig et al. (2023) observe in their analysis of EU Kids Online data that family and peer support can act as a buffer against the effects of perceived discrimination and low life satisfaction due to cyberhate victimisation. Social media literacy has also been an important protective factor, particularly for young people's consumption of idealised image representations on social media (Paxton et al., 2022).

2.2.2. Online sexual content

Children's exposure to **online sexual content** has been the topic of much debate, with concerns raised about children's consumption of pornography and their inappropriate messages about body image, gender norms and sexual behaviour. The easy access to adult content and its potentially harmful impact on children's development has given rise to calls for better access controls and age verification.

EU Kids Online reported in 2020 that, on average, 33% of children aged 9 to 16 had seen sexual images either on- or offline (Smahel et al., 2020, p. 89). In some countries, e.g., Croatia, the Czech Republic, Spain, Malta and Serbia, more than 40% of children had viewed sexual content. Research shows that the older children are, the more likely they are to see sexual content, with 61% of 15–16-year-olds reporting exposure to sexual images compared to 15% of 9–11-year-olds.

How children respond to exposure to sexual content and how its impact may be assessed is a challenging area for research. For one, what constitutes sexual content is in part culturally dependent. The intentionality of the child is also a factor, and the response will differ between sexual content that is sought out and that which is unexpected and unwanted. As such, the emotional response is also connected to the developmental stage and needs of the children, reflected by age.

Findings from EU Kids Online regarding children's reactions to exposure showed that in most countries, the majority of children who viewed sexual content were neutral about it and just under half (an average of 44%) were neither upset nor happy in response to viewing pornography. Reactions of being somewhat or very upset after seeing sexual images were reported by more than a quarter of children who saw them. In some countries, however, e.g., Finland, Italy, Lithuania, and Portugal, being somewhat or very upset was reported by less than 15% (Smahel et al., 2020, p. 91). Overall, the results suggest that exposure may not be as distressing to youth as prevalent risk-focused narratives suggest (Lebedíková et al., 2022).

Most studies of children's consumption of online sexual content from European sources use cross-sectional designs and convenience samples, leading to wide variation in reports of incidence and outcomes (Peter & Valkenburg, 2016; Stoilova, Livingstone, et al., 2021).

Some relevant key findings include the following:

- Boys report greater exposure than girls to sexual content online and at a younger age compared to girls (Ballester-Arnal et al., 2016; Smahel et al., 2020). How children feel after seeing online sexual content shows a differentiated pattern, with younger children and girls more likely to feel upset than older boys (Staksrud, 2020).
- The nature or mode of exposure to sexual content is, however, not always easy to define (Nash et al., 2015). UK research carried out against the background of legislative proposals for more robust age verification checks found that it is more likely for 16- and 17-year-olds in the United Kingdom to have been exposed, at least once, to sexually explicit porn videos or pictures via social media platforms (63%) or internet search engines (51%) than via dedicated pornographic websites (47%). More young people (63%) had seen pornography on social media than on pornographic websites (47%). However, pornography was much more frequently viewed on pornographic websites than on social media (Thurman & Obster, 2021), suggesting priority for stricter controls on the former may be more urgent.
- A study of 10,900 adolescents in six European countries found exposure among male adolescents to be ubiquitous and more pronounced among heavy internet users and those who displayed dysfunctional internet behaviour (Andrie et al., 2021). Gender differences were similar in each country. Exposure was associated with positive qualities and competences and externalising behavioural problems.
- Concerns for possible developmental outcomes for children from viewing pornography for younger children under 12 years include the development of problematic sexualised behaviours arising from exposure to sexual knowledge beyond what would be expected for the child's age and developmental level while noting other contributory factors to such problem behaviour (Hornor, 2020). Other potential negative consequences of adolescent viewing include excessive internet use, promotion of sexual aggression, risky sexual practices,

objectification of women and highly gendered male and female stereotypes (Peter & Valkenburg, 2016).

- The associations between viewing pornography and adverse outcomes for young people are mixed. Reviews of the literature suggest that accessing pornography affects young people's sexual attitudes and behaviours (Massey et al., 2021) and may also be a factor in sexual coercion. While studies have shown some relationship between watching more extreme forms of pornography and poor mental health in adolescents, other background variables also have to be taken into account (Svedin et al., 2022). The emotional effects of viewing online sexual content may not always be harmful, however. For example, an over-emphasis on risk may ignore its more positive uses by young people in the absence of more reliable information or education resources (Dawson et al., 2022; Harvey, 2020) and understood in the context of healthy sexual development (Green et al., 2020).

2.2.3. Disinformation

Going online to access information for learning and discovery and using the internet for schoolwork are the main daily activities for nearly all children across Europe. Over 30% of children said they do this daily, according to EU Kids Online (Smahel et al., 2020, p. 26). However, against increased concerns about the prevalence of mis/disinformation online, children encountering false and misleading content during their use of social media presents another key content related risk. According to a Eurobarometer survey on fake news and disinformation in Europe, in every country, at least half of respondents say they come across fake news at least once a week. More than a third of respondents (37%) say they come across fake news daily or almost every day (European Commission, 2018). However, children's experiences of encountering such disinformation remain relatively under-researched, with few cross-national studies available. As a result, young people may be considered more at risk than adults and more likely to be influenced by disinformation due to their predominant online news consumption and the fact that their cognitive capacities are still evolving.

The European Commission's Joint Research Centre found that during the COVID-19 pandemic, when the need for accurate information was most pronounced, across the 11 countries surveyed, nearly three-quarters of children aged 10 to 18 years (69%) reported coming across information they believed to be untrue. Over one-third of children (37%) believed this happened more frequently during the COVID-19 pandemic (Joint Research Centre, 2021).

Internationally, a UNICEF survey in 10 countries highlighted shortcomings in how young people evaluate online information: up to three-quarters of children reported feeling unable to judge the veracity of the information they encounter online (Howard et al., 2021). In the UK, the Commission on Fake News and Critical Literacy in Schools found that only 2% of children and young people in the UK had the critical literacy skills they need to tell whether a news story is real or fake (National Literacy Trust, 2018).

Similar gaps in critical media literacy were identified in other recent European studies, such as:

- A study for Safer Internet Day in 2017 by the Austrian Safer Internet Centre reported that 59% of 14–18-year-olds got their news from social media. However, 86% of those surveyed were unsure whether the information they found online was correct. Few believed (just 10%) that social media was a credible source. While many stated that they would look to check the sources of information given, in practice, many admitted that they tended to skim the headlines and rarely consulted more than one source (SaferInternet.at, 2017).

- A national survey of Romanian 17–18-year-old students found strong third-person effects in their ability to detect fake news, i.e., they consider themselves more capable of identifying false information than peers in their inner and outer circles (Corbu et al., 2022), raising concerns about their ability to be well-informed participants in the democratic process.
- A qualitative study involving 214 Flemish young people aged 15-19 years highlighted young people's awareness of which type of news is likely to be less credible. Most were able to distinguish between topics that are more likely to be fake news than others, particularly from social media sources. However, their ability to critically evaluate sources depended on their proximity to their environment, thus leaving significant areas of online information to be of uncertain validity (Vissenberg & d'Haenens, 2020).

2.3. Risks of harm through potentially harmful adult contact

Contact risks occur in the digital environment when a child experiences or is targeted by potentially harmful *adult* contact (Livingstone & Stoilova, 2021). Given the highly interactive nature of social media, it is in this context that children may be vulnerable to harmful contact from strangers in the form of stalking, excessive surveillance or harassment, leading to significant harms such as so-called "sextortion", ideological persuasion or manipulation or extremist recruitment. The OECD revised typology of risks distinguishes between contact risks where: *i)* children are exposed to hateful encounters in the digital environment, *ii)* the encounter takes place with the intention to harm the child, and *iii)* where the encounter involves illegal contact. Other potential problematic encounters that may be difficult to classify are also incorporated into the framework (OECD, 2021).

While research shows that the incidence of harmful contact from predatory strangers is rare, its potential impact is severe. It is also the source of much anxiety and distress for young people, their parents, and carers. Despite the efforts made by social media platforms to restrict the ability of adults who are not among their existing list of friends to contact minors, young people report unwanted communications as a persistent negative feature in their use of social media (O'Neill et al., 2021). For this review, three manifestations of contact risks are considered in relation to young people's social media use – hateful encounters which may lead to experiences of harassment, stalking and excessive surveillance; sexual harassment, potential sexual grooming and threats of extortion; and forms of ideological persuasion and manipulation.

2.3.1. Stranger contacts and harmful encounters

Meeting new people online, mainly through social media, is increasingly commonplace among young people despite its association with potential risks of harm from strangers. EU Kids Online includes two aspects of interactions with new people – whether the child has had contact with someone previously not met face-to-face and whether they have also met such a person face-to-face in the physical world. As reported in the 2020 survey, 37% of children aged 9 to 16 have communicated online with someone not previously known to them (Smahel et al., 2020, p. 95). 16% said they subsequently met the person face-to-face. Having contact with previously unknown persons online is strongly associated with age: just 16% of 9–11-year-olds say they did this, while 47% of 12–14-year-olds and 63% of 15–16-year-olds report making new online contacts. Meeting new online contacts in this way is not necessarily harmful. In fact, according to EU Kids Online data, just 10%, on average, reported negative feelings because of the encounter.

Survey findings indicate that meeting previously unknown people is an everyday experience for many children. Even though harm is infrequent, young people also report repeated unwanted contacts from others outside their friends list as a negative aspect of their online experience. Negotiating the risks and benefits of making online contacts forms part of the digital literacy young people require in managing their e-presence and is a focus of many mediation strategies (Symons et al., 2020). In addition, qualitative research with children in nine European countries found that most children reported awareness and confidence in how to deal with any potential adverse outcomes and develop coping strategies such as assessing non-verbal aspects of stranger contacts, deciding when to initiate in, participate or continue communication with a stranger (Cernikova et al., 2018).

Nonetheless, research has highlighted cases of harm arising from contact with strangers, including the study mentioned above of nine European countries as part of the EU Kids Online project, which reported situations where an unknown person stole their account, contacted them, sent inappropriate content, and communicated with them inappropriately (Cernikova et al., 2018, p. 106).

2.3.2. Harmful and illegal encounters (sexual)

Risks regarding **sexual solicitation and online 'grooming'** are among those that have raised the most concerns about children's use of social media. Adult perpetrators take advantage of the relative anonymity that the online world affords and the ready access that some platforms may provide to contact and connect with young people for sexual abuse. Sexual solicitation arises when a child is asked to provide sexual information or engage in sexual talk or sexual activities either online or offline. Whether another peer or adolescent initiates that contact or is an adult targeting a child for sexual purposes (i.e., 'grooming' or illegal contact) may not always be clear.

While the terms solicitation and grooming are often used interchangeably and have the same general meaning, grooming is the term more commonly used to refer to interactions on social media platforms that may be interpreted as "preparing" a child for potential sexual exploitation. Solicitation is used more frequently in a legal context, drawing on the definition in Directive 2011/93/EU [19], to refer to an "offline meeting" for sexual purposes. The Luxembourg Terminology Guidelines (ECPAT International, 2016) regard the terms as interchangeable but raise the important point that a legal definition should not be restricted to a physical meeting and that in technological terms, abuse can happen online without any offline meeting taking place.

Strategies used by offenders to solicit or groom children online for sexual purposes have been widely researched, frequently forming the basis for online safety education interventions. Stages of potential sexual solicitation may typically involve: selecting a potential victim – often those in already conditions of vulnerability; engaging in one-to-one conversation to foster isolation from others; developing trust with a potential victim; desensitisation to sexual content; and maintaining a position of power over the victim through threats and blackmail (ICMEC, 2022).

- Reliable data on the incidence of experiences of sexual solicitation among European children is not readily available. An evidence review undertaken for UNICEF found that among available studies, 12% to 17% of those surveyed had experienced sexual solicitations by adults (Stoilova, Livingstone, et al., 2021). Girls and older teenagers are more likely to be victims of online sexual solicitation, according to most studies. Research also points to a connection between online sexual solicitation and other online risk behaviours as well as a connection between being vulnerable offline and online.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32011L0093

- A retrospective study in the United States of young adults showed that a quarter of participants interacted with adult strangers online as minors. 65% of participants who chatted with adult strangers as children experienced sexual solicitation from an adult stranger, and 23% engaged in conversations that followed a pattern of online sexual grooming (Greene-Colozzi et al., 2020).
- A study of 2731 Spanish students aged 12 to 15 years found that 7% had experienced one of several factors related to online grooming: talking about sexual things with an adult on the internet, having sent adult photos or videos with sexual content of his or herself, having maintained a flirtatious relationship with an adult online, having met in person an adult previously met on the internet and proceeding to meet offline for the purposes of sexual contact (Gámez-Guadix et al., 2018).Girls more often reported that they were the target of persuasion strategies and nonsexual involvement, indicating a higher risk for females of online sexual exploitation.
- A study of German adolescents' online sexual experiences aged 14-17 years found that adolescents (51.3%) frequently engage in sexual interactions on the Internet (i.e., sexual conversation, exchanging pictures, and cybersex). This mainly involved peers and did not result in negative responses. However, 23.2% reported negative responses to online sexual interactions with peers. 22.2% reported online sexual interactions with adults, 10.4% of which were perceived as negative (Sklenarova et al., 2018).
- An experimental study in the Netherlands of adolescent girls' ability to assess the age of an online stranger found that only 43% were able to make a correct assessment. Most adolescents adopted passive strategies to reduce uncertainty, such as scanning the stranger's profile page and checking contact information and the profile picture (Groenestein et al., 2018). Cues that caused alarm but about which participants were uncertain included danger signals such as ignoring personal questions, showing an exaggerated interest, acting as a friend, and being sexually oriented.
- Research with adolescent victims who had offline meetings with adult perpetrators shows that the adolescents' misplaced trust often masked the subtleties of online grooming as they pursued opportunities for online friendships or sexual activities, pointing to the need to clearly define the risks for adolescents (Chiu & Quayle, 2022).

Sexual extortion, also known as 'sextortion', involves the threat of exposing sexual images of a victim to coerce them to provide additional pictures, sex, or other favours (Wolak et al., 2018). Sextortion has been identified as an emerging threat, though the evidence to date is scarce. One of the few studies based on a nationally representative sample is from the United States, which found that 5% of those surveyed had been the target of sextortion, while 3% admit they had done it to others. As a result, males were significantly more likely to have participated in sextortion both as a victim (5.8% vs 4.1%) and as an offender (4.1% vs 1.9%) than females (Patchin & Hinduja, 2020).

Europol (2017) has distinguished between two primary motivations for online sexual coercion and extortion of children: sexual and financial. According to a review of open cases, minors can be the victims of both, though the sexual gratification of a perpetrator appears to be the primary motivating factor. However, the recent rise in the detection of self-generated child sexual abuse images reported by law enforcement agencies worldwide (Internet Watch Foundation, 2021) has been linked to an increase in instances of sextortion carried out by organised offenders based outside of the EU (European Union Agency for Law Enforcement Cooperation, 2021).

A 2022 study conducted by the Canadian Centre for Child Protection (C3P, 2022) of victims' accounts of final sextortion found that the main targets are predominantly boys and young adult males. Extorters were reported as using similar strategies across popular platforms such as Snapchat and Instagram. When posing as a female, they entice the victim to send nude images, following which the extorter blackmails the victim demanding money and threatening to expose the photos to their friends and family.

2.3.3. Ideological persuasion and manipulation

Content risks related to disinformation, user-generated content designed to mislead, and extremist hate messages have been widely reported by young people. Adults may also directly target children for ideological persuasion, manipulation or recruitment to extremist causes. While there has been increased attention to extremism online and children being drawn in as victims, the available evidence of children's experiences of this type of harmful contact is relatively scarce.

The notion of 'radicalisation' refers to being persuaded, manipulated or adopting content of an extremist, far-right or fringe nature. A review of the relatively limited research on extremist radicalisation highlights the challenge that there are few if any discernible patterns (Marwick et al., 2022). No specific type of person is vulnerable to radicalisation; there is no single way in which people are radicalised and viewing extremist media does not necessarily lead to adopting extremist beliefs.

Notwithstanding that exposure of children and young people to online hate material – some of which may be extremist– raises particular concerns, little research on children as a target population is available.

- A comparative study which included a mix of Finnish youth and young adults (aged 15 to 30 years) found that a majority of the sample had experienced online hate material, the purpose of which was to affect the subjective well-being of the targeted group or individual (Keipi et al., 2018).
- EU Kids Online likewise found that, on average, 17% of children in 19 European countries had encountered similar online hate messages (Smahel et al., 2020). However, there is no data on the response to such messages.
- Exposure to cyberhate during the COVID-19 pandemic among children aged 10 to 18 ranges between one-half, with 52% in Austria and over two-thirds in Romania (71%). In France, 45% reported this experience. However, between one-quarter and one-third of young people said this happened more often during periods of lockdown (Joint Research Centre, 2021).

Empirical research specifically concentrating on violent extremism is scarce and tends to focus on young adults 18 years and older rather than children and deals with interventions to develop resilience and resistance to extremist messaging (Frissen, 2021).

One of the few available large-scale studies from Germany showed that exposure to extremist messages among young Germans was commonplace (Reinemann et al., 2019). Almost half of young people encounter extremist messages and attitudes at least sometimes - be it in public, in everyday encounters or through the media. Social networks, online news sites and video platforms (YouTube) are places where young people often encounter extremism. However, the most frequent contact with extremism occurs through journalistic media reporting. Based on the findings of this survey, the authors put forward a typology of the different ways and different degrees of contact with extremism experienced by young people. These include the "Unaware" (the largest group), the "Informed", the

"Reflective", and the "Vulnerable" (Reinemann et al. 2019, p. 219). Education and media literacy measures should be targeted and prioritised accordingly.

Extremist exploitation of social media platforms is an important question for policymakers, and developing effective regulatory solutions to counter its impact is vital for all internet users, including children (Ganesh & Bright, 2020). However, in the absence of further empirical research specifically on the topic, such routes to potential ideological manipulation should be considered within the more general context of pathways to anti-social and criminal behaviour to which children may be victims.

2.4. Peer conduct risks on social media

Peer conduct risks arise on social media when a child witnesses, participates in and is a victim of potentially harmful conduct or behaviour (Livingstone & Stoilova, 2021). In contrast to the various risks which harmful content and contact pose on social media platforms, conduct risks are associated with peer behaviour. In its original typology of online risks, the OECD excluded activities whereby children created risks for other children. However, the reported prevalence of problematic peer-to-peer behaviour and interaction mediated by digital technologies have made conduct risks among the most persistent and complex issues for children's online safety.

A further distinction may be made between "aggressive" conduct risks, such as online bullying and hostile communication or peer activity; "sexual" conduct risks, including sexual harassment between peers and non-consensual sexual messaging; and "values-based" conduct risks, including participation and interaction in potentially harmful user communities such as self-harm groups or other groups exerting negative peer pressures. As with content and contact risks, boundaries between such risk categories can overlap and become blurred, meaning that different manifestations of such risk patterns often occur together. For this study, the focus is on evidence regarding experiences of bullying on social media, problems associated with sexual conduct risks and participation in peer communities that are problematic for children's development.

2.4.1. Bullying and aggressive behaviour in social media

Bullying and online aggression are among the most discussed topics regarding children's use of social media and issues affecting their development. The adverse impact on children's social, psychological and educational development are well-established (Smith & Steffgen, 2013), and the negative consequences for children's well-being more generally have made this a policy priority of the highest order (Office of the SRSG on Violence against Children, 2016).

Cyberbullying has been defined as *"willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices"* (Hinduja & Patchin, 2021) and involves incidents where young people use technology and platforms to harass, threaten, humiliate or otherwise behave aggressively towards their peers. Sending hurtful messages, spreading rumours online, and posting nasty comments on social media are all patterns that young people report as harmful and problematic experiences. Reports of incidence while varying according to the methods and definitions employed emphasise its prevalence and persistence as an issue impacting children's participation in the digital environment.

The EU Kids Online 2020 survey of 19 European countries found that an average of 23% of children aged 9 to 16 experienced aggression or was a victim of bullying, on- or offline, in the past year. This ranged between 7% (Slovakia) and 40% (Poland). In most countries, more than 20% of children experience victimisation. There are no substantial gender differences in being a victim of bullying though in some countries (France, Malta), more girls are victimised than boys. Bullying affects all age groups but is particularly pronounced for early teenagers aged 12 to 14 years.

The Joint Research Centre (2021) found that 49% of children aged 10 to 18 years had experienced at least one form of online aggression or bullying (nasty or hurtful messages being sent to them or circulated to others about them, being excluded from an online activity, being threatened online). 24% had experienced all four forms of cyberbullying asked about. Countries with the highest percentage of children reported to have encountered all four cyberbullying situations are Germany at 36%, Italy at 31%, Romania at 29% and Switzerland at 28% of children. Notably, 44% of children reported that experiences of aggression or bullying online had increased during the COVID-19 pandemic (though 22% also reported that it happened less). A third of children (34%) also said they had been a perpetrator of cyberbullying and had treated someone else in a hurtful or nasty way online.

The dynamic and changing nature of the environment in which online bullying can occur requires continued monitoring, e.g., bullying risks in the metaverse (see Hinduja, 2022), with constantly updated research needed to reinforce effective policy and educational interventions. Relevant recent European findings have highlighted the following aspects:

- Comparative international studies such as the Health Behaviour in School-aged Children (HBSC) survey show that problematic social media use (showing addiction-like symptoms) is strongly and consistently related to cyber-victimisation (Craig et al., 2020). Social media use as such exposes young people to risks for involvement in cyberbullying and more aggressive online behaviours, particularly for boys. In addition, intense and problematic use may also expose adolescents to peers and social norms that validate and reinforce forms of aggression, including cyberbullying.

- One of the problems of social media interaction is that the communication cues that exist in face-to-face interaction are no longer present, leading to misunderstanding and more rapid escalation of exchanges into cases of cyberbullying behaviour. Online banter or teasing can easily be misinterpreted as aggressive behaviour, causing harm to victims and creating additional challenges for detection and intervention (Steer et al., 2020).

- Research has long emphasised the continuity between offline (e.g., school-based) bullying and online experiences. As young people conduct more of their social life online and through social media platforms and messaging services, increased levels of online aggression and bullying are in evidence with a consequent impact on the quality of the educational setting. Victims of cyberbullying can feel isolated in school, lose their sense of belonging, and withdraw from school activities (Kashy-Rosenbaum & Aizenkot, 2020; Mancheva, 2020).

- Teachers are often the first to deal with concrete instances of cyberbullying, many of whom report that with appropriate and timely intervention, three out of five cases of cyberbullying could have been prevented (Gold, 2021).

- Whole school education programmes which emphasise social-emotional learning, mentoring and education on online safety, respectful communications and resilience effectively reduce experiencing or engaging in bullying behaviour (see ENABLE, 2015). In particular, social-emotional learning with peer mentors is recommended as a key design component of such programmes (Hajnal, 2021).

2.4.2. Sexual harassment

Experiences of sexual harassment and other forms of peer-to-peer conduct involving negative sexual pressures on social media platforms, including the non-consensual sharing of intimate images, is an increasing concern for many young people and online safety professionals. Underpinning this concern is the rise of so-called youth "sexting" or the sending and receiving of sexually explicit messages using digital technologies and online platforms. A meta-analysis of 39 international studies of youth sexting shows this to be a growing practice (Mori et al., 2022). Sexual communication, while a normalised and widespread communicative practice among young people, is also highly complex. The sending or receiving of sexual messages may be intentional within the context of a consensual relationship. However, there are concerns that sexual content may fall into the wrong hands, be exploited for other purposes or, in extreme cases, be considered child sexual abuse material. Accordingly, there are often complex safety messages and sometimes contradictory legal provisions surrounding the practice of peer-to-peer sexual communication using digital technologies and social media platforms (Quayle, 2022). Here, the focus is on experiences of sexual harassment arising from the misuse of online communication.

In its research on sexting – the practice of sending sexually explicit messages via electronic devices – EU Kids Online reported that an average of 16% of 12- to 14-year-olds rising to one in three (32%) 15- to 16-year-olds across 19 European had received sexual messages in the past year (Smahel et al., 2020, p. 84). This ranged between 8% (Italy) and 39% (Flanders). In eight countries (Switzerland, Czech Republic, Germany, Spain, Malta, Norway, Serbia and Flanders), 40% to 50% of children in the oldest age category received sexual messages. Sending sexual messages is less prevalent than receiving such messages, with an average of 6% reporting this - ranging from 1% (France) to 18% (Germany).

Noting that sexual communication can be either intentional or unwanted, children were also asked if they had received any unsolicited requests for sexual information about themselves. For example, 17% of children 12 to 16 said they had received unsolicited requests for sexual information. More girls than boys (19% vs 14%) experience such unwanted sexual requests.

As noted by EU Kids Online, defining sexual messaging only as a negative experience without further data about the harms that may ensue risks rendering policy or safety advice irrelevant to young people's lives. More research is needed to investigate the harm to children's development from receiving sexual messages and unwanted pressure to exchange sexual information.

Drawing on some of the themes of recent research regarding children and sexual communication, the following offers some further insights into these experiences:

- National and regional studies have found that the sharing of intimate images is pervasive and an increasingly normalised feature among many young people (Van Ouytsel, Punyanunt-Carter, et al., 2020).
- A study of 3300 young people in Spain, aged between 12 and 16 years, found that 8% of teenagers send or forward sexual content, while more than 1 in 5 receive it directly from the creator, and more than 1 in 4 teenagers receive it via an intermediary (Ojeda et al., 2020). The study highlights that "*the Snapchat platform is used more to exchange consensual sexual content between romantic/sexual partners. However, a study of whether factors, including pressure and coercion, exert an influence is needed. In contrast, Facebook and Instagram are more frequently used for generally non-consensual forms of sexting*" (Ojeda et al. 2020: 16).
- Sexual messaging and sharing of sexual images have also been researched more generally within the context of adolescent risk-taking. For example, in a German study of students aged

14 to 17 years, intimate photo-sharing was discussed as a form of self-disclosure in the development of adolescent relationships, serving the purpose of "proving friendship" and deemed an acceptable risk related to "friendly intimacy" (Thorhauge & Bonitz, 2020).

- A systematic review of studies of empirical evidence of outcomes of sexting practices shows a wide spectrum of consequences, both positive and negative, spanning benefits for adolescents' well-being and relationships through to severe harm and trauma (Doyle et al., 2021) with implications for targeting of educational supports.
- Qualitative research on youth sexting practices points to greater nuance in the gender imbalance in sexual communication, for instance, when girls also instigate sexting and pressure boys to send pictures (York et al., 2021). However, gender stereotyping and objectification of girls remains a key finding.
- Much concern is centred on the negative impact of a highly sexualised digital culture and the formation of healthy relationships in real life. For example, there is a tendency to attribute online unwanted sexual requests to stereotyped gender norms creating further barriers to negotiating consent in the context of relationships and sexuality education (Setty, 2021).
- Gender minority adolescents (transgender, gender diverse and non-binary gender) may be especially vulnerable to sexting-related risks. For example, an exploratory study in Flanders found that young gender minority people are more like to experience online harassment and pressure to engage in sexual communication. They also face unique challenges with regard to safety and anonymity in online spaces and may be especially vulnerable to online pressure and abuse (Van Ouytsel, Walrave, et al., 2020).

2.4.3. Potential harmful online peer communities

In the highly interactive world of social media, children actively seek out online peer communities to learn, discover and share interests. One of the many benefits of social media to young people is the ability to connect with others, participate in groups beyond geographic boundaries and seek advice and support from peers. However, there may also be potentially harmful user communities that manipulate vulnerable children, causing them to disconnect from family and social ties and rely on online community supports that are harmful to their development. The CO:RE classification of online risks (Livingstone & Stoilova, 2021) gives examples of self-harm and self-injury groups, anti-vaccine groups, or others that may apply negative peer pressure on the young person. Conduct risks are an extension of risks of exposure to harmful content and behaviours but may have more severe outcomes once a child engages or actively participates in such communities. Identifying and responding to such pressure and manipulation online is one of the main themes of online safety and media literacy education in this area[20].

Recalling the EU Kids Online finding of exposure to various forms of harmful content (Smahel et al., 2020, p. 61), approximately one in ten children aged 9 to 16 years reported seeing at least monthly content such as the following:

- Ways of physically harming or hurting themselves – 10%
- Ways of committing suicide – 8%
- Ways to be very thin – 12%

[20] For example, the Danish Centre for Digital Youth Care has developed a resource responding to the challenge of young men engaging in right-wing or anti-women communities online https://www.betterinternetforkids.eu/en/resources/resource?id=26775

- Their experiences of taking drugs – 11%

However, exposure to content does not imply active engagement or participation in harmful online peer communities for which evidence is scarce, and more targeted and detailed analysis is needed. Some of the salient points for policy making from available studies include:

- A systematic review of studies of self-harm and suicidal content online from 2015 to 2021 examined such content from the perspective of whether it was intended to be helpful or harmful. Very little content online was found to be easily classifiable as explicitly harmful or definitively helpful, with responses varying by the individual and immediate context. Accordingly, the authors recommend that blanket approaches to regulation should be avoided in favour of user-focused supports (Brennan et al., 2022).
- A systematic review of studies of suicide attempts in young people under the age of 19 years found some evidence for an association between problematic heavy social media/internet use and increased suicide attempts. However, the direction of causation is unclear (Sedgwick et al., 2019). Research also highlights that vulnerable self-harming young people use social media for help-seeking and support. In addition, increased exposure may lead to increased psychological distress due to users receiving negative messages promoting self-harm if the appropriate supports are unavailable (Memon et al., 2018).
- Concerns have also been raised about the susceptibility of adolescents to so-called online challenges spread virally through social media platforms, some of which may have a self-harming dimension (Deslandes & Coutinho, 2020). Although such games (for example, the Blue Whale & Momo challenges) might promote self-harm and suicidal behaviour, they cannot be considered the sole cause of suicide even if they have a serious "precipitant effect". Other factors such as depression, emotional difficulties, social isolation, or peer problems are substantial risk factors for problematic internet use (Fındık & Çeri, 2019, p. 558). The concern is also expressed in the literature that media, social media and warnings issued by authorities serve to spread the challenge culture and exaggerate fears regarding this type of online risk (Bada & Clayton, 2020; Phippen & Bond, 2020).

A further area of concern regarding children's vulnerability to harmful manipulation and adverse peer pressure is inducement through online participation into **cyber criminality**. Cybercrime is a general term encompassing a wide range of illicit conduct perpetrated by both individuals or groups against computers and networks. It also encompasses traditional crimes that are computer-mediated. Phillips et al. (2022) put forward a new classification framework that distinguishes between crimes against technology (e.g. hacking, data interference); crimes using technology (e.g. computer fraud, digital piracy, identity theft); crimes within a technology context (e.g. interpersonal violence, sexual violence, violence against groups); and cyber-assisted (e.g. illegal gambling, drug trade, laundering).

EU Kids Online (2020) did not study cybercrime as such. However, in its study of data misuse, an average of 7% of children aged 9-16 years reported that somebody had used their personal information in a way they didn't like; a similar number reported being victims of identity theft; and 4% reported being the victim of fraud online (Smahel et al., 2020, p. 69). The Joint Research Centre similarly found that, on average, a quarter of 10-18-year-olds experienced someone using their personal information in a way they didn't like (Joint Research Centre, 2021, p. 30) including having their password stolen or misused to impersonate them (23%) or having a page created that was hostile to them (22%).

A survey undertaken by the EU-funded CC-Driver project[21] found that 69% of European young people aged 16-19 years had participated in at least one form of cyber-deviant behaviour (CC-Driver, 2022). This includes a spectrum of behaviours, including activities that may be antisocial or harmful to the individual or others, and those that violate established norms as delinquent and criminal acts (Cioban et al., 2021). Two-thirds of the sample, 67.2% (N=5359) report having multiple accounts on at least one platform, the most common reason being "*to post content that I only want some of my friends to see*" (CC-Driver, 2022, p. 4). 3% of the sample reported having used social media for catfishing, the practice of setting up a fake online profile, particularly in the context of cyber-dating (Paat & Markham, 2021).

2.5. Contract and consumer risks

Including a fourth "C" of "contract risk" that children may encounter is the most significant change introduced in the CO:RE classification of online risks (Livingstone & Stoilova, 2021). The CO:RE classification reflects evolutionary changes in the digital environment, particularly concerning the commercialisation and datafication in the diverse platforms and services likely to be used by children. Labelling this as a "contract" risk is intended to highlight how children as users are connected directly or indirectly to digital providers through their registration for a service and through that service's data collection practices. The OECD revised typology of risks (OECD, 2021) also includes a category of "consumer" risks intended to reflect the additional risks posed to children by evolving marketing, targeted advertising and personalised profiling (Lombana-Bermudez et al., 2020).

Addressing contract and consumer risks faced by children is a relatively new area of research for which consistent data has yet to be available. In the BIK+ strategy[22], the European Commission recognises that children are now more active and independent digital consumers than in 2012 when the first European Strategy for a Better Internet for Children was launched[23]. Children, according to the BIK+ strategy, are exposed to or targeted by a range of online marketing techniques: "*Through social media recommendation systems, and other algorithms, targeted advertising, influencer marketing and gamification of marketing, harmful or inappropriate content is proposed to young users, exploiting their inexperience and lack of self-control*" (2022, p.7). A key proposed action of the BIK+ strategy is that the Commission will "*map research into the impact of neuro-marketing on children in order to assist national consumer authorities to better assess how commercial influencing techniques may be unfair on children"* (p.11).

Contract risks arise for children in numerous ways across the social media environment. One obvious way this happens is when the child registers as a user on a social media platform and "accepts" the Terms of Service of the commercial provider of a digital product or service. As noted by Livingstone and Stoilova, such terms "*can bind the child in ways that may be unfair or exploitative, or which pose security or safety or privacy risks of which they be unaware or over which they have little control of means of escape*" (Livingstone & Stoilova, 2021, p. 7). The following are examples drawn from the literature on available research regarding such **unfair practices**:

- Profiling and automated decision-making, commercialisation of play, and digital child labour are examples of exploitative practices that may significantly impact the well-being and rights of children (Hof et al., 2020). Algorithmic recommendation systems can increase the phenomenon of encountering inappropriate content through the use of auto-feed features

[21] https://www.ccdriver-h2020.com/

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

[23] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196

displaying similar content under “recommended” content. Such systems and clickbait strategies can be pernicious and detrimental, undermining children’s opportunities to build self-control and balance digital and real-world activities.

- Children are often exposed to technological designs and algorithms that are repurposed for them, but which were initially developed for adults (for example, YouTube for Kids, Messenger for Kids, Instagram for Kids etc.). These services apply adult-centred processes (e.g., social comparison, image obsession etc.) which can be detrimental to children’s well-being and are not designed in their best interests. The intensification of content that children are exposed to via algorithmically driven recommendations is a common feature of children’s online experience. Video-sharing platforms are one of the most popular activities for children and are used by two-thirds of the children in most European countries daily (Smahel et al., 2020). Yet, as the Pew Research Centre reported, videos suggested by YouTube’s recommendation engine constantly direct children toward progressively longer, more intense and more popular content (Pew Research Centre, 2018).

- Although research has shown that children display some awareness of the importance of data privacy (Stoilova, Nandagiri, et al., 2021), there is still little awareness of the complexities of the data processing underpinning in social media, how algorithmic profiling happens, or how AI agents use data.

- Children also face significant consumer risks in their general online use and in social media environments (Verdoodt, 2020). Risks include embedded advertisements, privacy-invasive practices, and the exploitation of their incredulity and inexperience, resulting in overspending or fraudulent online transactions. Behind the fun and playful activities available for children online lie complex revenue models, creating value for companies by feeding children’s data into algorithms and self-learning models to profile them and offer personalised advertising or by nudging children to buy or try to win in-app items to advance in the games they play.

- Teenagers are often unaware of the commercial use of their personal information and are susceptible to the persuasive effects of personalised advertising. Children’s coping strategies are often inadequate (Holvoet et al., 2022). For example, serving advertisements on mobile formats (smartphones and tablets) is even more difficult for children to identify with low recognition of the persuasive intent of commercial messages that are not explicitly identified as such, particularly on social networks (Feijoo & Sádaba, 2022).

- Research conducted among 374 adolescents between 12 and 17 years in Flanders found that advertising literacy increases progressively throughout adolescence and reaches adult-like levels only by age 16. In addition, adolescents may lack adequate awareness of commercial data collection practices and take little action to cope with targeted advertisements using privacy protection strategies (Zarouali et al., 2020).

- Advertising literacy may be particularly important for younger children for whom video-sharing platforms such as YouTube are a key part of their media consumption. In contrast to linear television, the boundaries between entertainment and advertising content on such platforms are not always clear. A study of preschool children aged 4 to 5 years showed that while most children were able to identify when advertising was presented, they displayed no critical advertising literacy, treating the advertisement in the same way as the entertainment content (Vanwesenbeeck et al., 2020).

Consumer risks such as marketing **products high in fat, sugar or salt (HFSS products**), which can encourage inappropriate dietary behaviour, can adversely affect children's physical health at any age.

- A European Commission study found that 64% of the food and drink advertisements to which children were exposed online were for HFSS products. Most HFSS advertisements promoted sweet snacks. Just 4% were for healthier food options. The vast majority (81%) of the HFSS advertisements children were exposed to were served on YouTube (European Commission. Directorate General for Health and Food Safety. et al., 2021, p. 194).
- Youth-targeted food marketing is highly appealing to young people (Meléndez-Illanes et al., 2022). A 2019 study found that a sample of 27 fast food, snack, and beverage brands collectively maintained 6.2 million adolescent followers on Twitter and Instagram. In "following" brands on social media platforms, young people opt in to greater exposure to food and beverage advertisements with adverse consequences for their dietary behaviour (Rummo et al., 2020).

Social media influencer marketing and **gamification of marketing** are further examples of commercialised practices on social media which pose risks to children who may lack the knowledge and critical literacy to be fully aware of its potential influence. Contemporary advertising has been described as less about persuading children through persuasive messages and increasingly about influencing them through implicit tactics (De Pauw, De Wolf, et al., 2018).

- A study of influencer practices on social media platforms such as Instagram, YouTube and Snapchat found that influencers frequently ignore requirements to disclose or label the commercial nature of messages. However, there is often a lack of clarity as to how such conditions should be fulfilled, for example, in the case of "unboxing" videos where there is no specific payment involved (Österreichisches Institut für angewandte Telekommunikation, 2018).
- Vlogs or video blogs are a particularly popular way for social media influencers to build a following, promoting products and brands that appeal to children. Children's bonding with the vlogger is a key factor in how much time they spend viewing vlogs, many of which endorse food and beverages that may be considered unhealthy (Folkvord et al., 2019).
- There is often a need for more transparency in the relationship between digital influencers, brands and social media platforms. Even where there is a disclosure of the underlying commercial purpose of embedded advertisements, these provide particular challenges for children who may lack the skills needed to fully appreciate its persuasive intent (Balaban et al., 2022). For example, a study of Portuguese children aged 10 to 17 found that while most were aware of the relationship between influencers and brands, many lacked detailed awareness of the commercial nature of the relationship with social media platforms (Dias et al., 2022).
- The method of displaying a clear disclosure regarding advertising has also been found to be important in raising levels of critical awareness (De Pauw, Hudders, et al., 2018; Van Reijmersdal et al., 2020). In addition, appropriately structured, school-based education interventions are important but not always sufficient to empower young people to use advertising coping strategies (Rozendaal & Figner, 2020). Awareness of selling intent does not always lead to critical processing (Daems et al., 2019). Moreover, novel forms of marketing and brand integration within highly interactive social media environments require new approaches to effective education and awareness raising.

2.6. Mental health and well-being

The potentially harmful effects of social media use on children's mental health and well-being have become a prominent and urgent topic of concern. Against an apparent mental health crisis among children and youth, exacerbated by the COVID-19 pandemic, wide-ranging concerns have been expressed about the adverse effects of social media (OECD, 2018). Various manifestations of mental health issues, such as increased levels of depression and anxiety, excessive digital technology dependency, and increased rates of youth self-harm, are cited in the literature as potentially related to patterns of social media use. Research on these interrelated topics has been referred to in previous sections. Here, a more general overview of the negative impact of social media on children's mental health and well-being is reviewed.

Both the CO:RE classification of online risks and the OECD's revised typology of risks include mental health as a cross-cutting form of risk that children may face through their engagement in the digital environment. By identifying this as a transversal risk, both typologies point to the fact that some experiences of risks are not always easily distinguished and, in one way or another, combine aspects of the "4Cs" of content, contact, conduct, and contract risks (Livingstone & Stoilova, 2021, p. 10). For example, addressing mental health and well-being as a cross-cutting risk recognises that being a victim of cyberbullying or exposure to hateful content can have mental health outcomes. Other cross-cutting risks within the classification (physical health, privacy violations, experiences of inequalities and discrimination) similarly attest to the interrelated nature of children's online experiences, and that adverse effects may touch on many different parts of their lives.

2.6.1. Mental health and social media use

Research on how social media use impacts children's mental health is diverse and uses varying methods with often conflicting conclusions. The subject area is also contested, with differing opinions on the best indicators and outcome measures. Many researchers further argue that to understand better how adolescents' mental health relates to the digital environment, it is essential to consider *offline* as well as *online* factors and to consider both *harm* and *benefits* as far as mental health is concerned (Stoilova, Edwards, et al., 2021)

A meta-analysis undertaken on behalf of UNICEF of research regarding the effects of digital technology on children's mental health and well-being (Stoilova, Livingstone, et al., 2021, p. 59) summarised key findings as follows:

- The evidence for either a positive or negative impact on children's health and well-being is mixed and inconclusive. Some studies show a positive association with poor mental health, but others find no association or point to positive benefits.
- Most studies focus on correlations between digital technology use and mental health rather than causation. As such, it is not possible to say that problematic social media use is a cause of poor mental health outcomes. Turning to social media may also be a way of coping with mental health problems.
- Long-term outcomes related to children's mental health and well-being are rarely explored in the literature.
- What matters for children's mental health is less the time spent using the internet and social media and more about how children use their time online and the consequences of that use.

A meta-analysis for the Swedish Media Council of 26 longitudinal and five experimental studies found that a small association between time spent on social media and mental health issues was replicated in most studies (Nutley & Thorell, 2022). Its review concluded *"that there is evidence of associations between digital media and mental health problems. However, effects vary between individuals, with some being at much higher risk than others"* (p.28).

This is similar to an analysis of the UK Millennium Cohort Study, which concluded that different types of screen time might have contrasting associations with depressive symptoms during adolescence, some positive, and some negative (Kandola et al., 2021).

Focussing predominantly or exclusively on the amount of time spent using social media platforms, however, has been criticised as ignoring the nature of the activities themselves or the contexts of use. For example, in a review undertaken for UNICEF, it was found that the evidence suggests that "*moderate use of digital technology tends to be beneficial for children's mental well-being, while no use or too much use can have a small negative impact*" noting that these impacts very small and not as relevant as other factors known to be of importance to children's mental well-being (Kardefelt-Winther, 2017, p. 6).

2.6.2. Problematic social media use

Probing the nature of problematic online use, or perceived negative effects of high levels of use of digital technologies and social media, has been argued as a way to understand the role that social media may play in adverse outcomes over time.

Excessive internet use is the term used by EU Kids Online (Smahel et al., 2020, p. 77) to refer to problematic internet use that is associated with children's emotional problems, lower self-efficacy, higher sensation-seeking, poor sleeping habits, poor nutrition, physical inactivity and other health problems (Helsper & Smahel, 2020).

Children aged 12 to 16 years in 19 European countries were asked how often they had experienced any of five indicators related to problematic internet use. Findings for individual indicators included the following:

- 4% reported that they had gone without eating or sleeping because of the internet;
- 10% reported that they had felt bothered when they could be online;
- 11% reported that they found themselves using the internet even when not really interested;
- 13% said that they had spent less time with family, friends or schoolwork because of the time they spent online; and
- 10% had tried unsuccessfully to spend less time online.

However, children may only be said to experience excessive or problematic internet use only if all five criteria or present. Here, only a small minority reported experiencing all five criteria ranging between 0% (Italy and Slovakia) and 2.1% (Croatia and Malta). Between 2% (Italy, Lithuania and Slovakia) and 8% (Switzerland, Croatia and Romania) were found to experience three or four excessive internet use criteria.

Noting that the overall findings for excessive internet use among European children are low, other related research findings address the following aspects:

- National and regional studies similarly report low levels of severe problematic internet use (less than 2%) while noting that together with moderately problematic internet users, this still represents a significant number of children (Kapus et al., 2021; Lukács, 2021).
- Further analysis of EU Kids Online data has shown that whether intense internet use is related to adverse outcomes depends on the child's psychological characteristics. Here, digital literacy can be helpful (Helsper & Smahel, 2020). Moreover, a study of social relational factors in four European countries, drawing on the most recent EU Kids Online data, found that positive family relationships and positive school relationships were associated with lower levels of excessive internet use and thereby provided a protective factor against its adverse effects (Mikuška et al., 2020).
- A meta-analysis of 19 international studies (Europe, Euro-Asia, America and Asia) of problematic internet use and depression in adolescents highlighted that problematic use and depressive symptoms are interrelated so that one problem promotes the other. Age and culture were not significant, and education interventions are needed for all groups to prevent it from being maintained into adulthood (Lozano-Blasco & Cortés-Pascual, 2020).
- A longitudinal study of social media use and sleep patterns in The Netherlands found that problematic social media use predicted poorer quality of sleep among adolescents. Moreover, among adolescents who used social media more frequently or reported more problematic social media use, strict parental rules did not predict better quality of sleep and, therefore, did not prevent negative media influences on sleep (van den Eijnden et al., 2021).
- A three-wave longitudinal study of adolescent students also in The Netherlands found that problematic social media use rather than intensity or the amount of time spent online was a factor in predicting decreases in mental health over time (Boer et al., 2021). Problematic social media use indicates addiction-like features such as loss of control over social media use or neglecting hobbies or other activities due to social media. The researchers found this was a one-way direction: increased depressive symptoms were not predictors of problematic social media use.

The available research on the relationship between social media use, especially use that may be defined as problematic, and mental health outcomes reveal a complex picture. There are both positive and negative features in how social media may contribute to or alleviate aspects of children's behavioural patterns. What stands out from this research and from research more generally on risks and harms experienced by children is the role played by the design attributes of the social media environment and the extent to which such design supports or undermines better outcomes for young people. Regulations governing this dimension and the responsibility of social media platforms to provide safer environments are considered in the following sections.

3. THE EU POLICY AND REGULATORY FRAMEWORK

KEY FINDINGS

Supporting children to be safe, protected and empowered when they go online is a cornerstone of EU digital policies, expressed most explicitly in the Better Internet for Kids (BIK+) strategy adopted by the Commission in May 2022.

EU policies to protect children online are underpinned by respect for children's rights and comprise a range of policies, strategies, laws and regulations to create a safer online environment in which children are supported in attaining digital skills and competences, including media literacy.

Legal and policy developments with significant implications for the regulation of social media and online marketplaces include the Digital Services Act, the Audiovisual Media Services Directive, the General Data Protection Regulation and the Unfair Commercial Practices Directive. These provide the foundation for a resetting of rules that apply to children's online safety.

Legislative proposals under consideration such as the Artificial Intelligence Act, the European Digital Identity framework and the Regulation laying down rules to prevent and combat child sexual abuse also propose solutions with far-reaching consequences.

Several significant developments at the international level have also emphasised the application of children's rights to the digital environment, as reflected in the EU policy framework.

Measures reinforcing children's privacy and obligations towards safety by design and age appropriate design are noted.

Supporting children to be safe and empowered when they go online has been a cornerstone of European Union policies for over two decades. Successive policy initiatives such as the Safer Internet Programme begun in 1999, the European Strategy for a Better Internet for Children adopted in 2012 and most recently, the Better Internet for Kids (BIK+) strategy adopted in May 2022, have sought to prioritise children's safety and well-being online. Such policies to keep children safe online and to empower them in the digital environment also lie within a broader policy context that seeks to secure the opportunities and benefits of digitalisation for all as set out in European Commission's vision for 2030, the Digital Compass: the European way for the Digital Decade[24].

This section of the report gives an outline of the main elements of the EU policy and regulatory framework for children's online safety in the digital environment. Firstly, EU policies specifically focused on children's online safety and well-being are briefly reviewed. This is followed by an overview of laws and regulations governing social media, particularly concerning provisions that address minors' protection in the digital environment. Finally, to place these frameworks in a broader context, developments and trends at the international level are outlined.

[24] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118

3.1. EU policies to promote children's online safety and well-being

3.1.1. The European strategy for a better internet for kids (BIK+)

The need to protect and empower children and young people in the online space has most recently been confirmed in the European Declaration on Digital Rights and Principles for the Digital Decade[25], signed in December 2022 by the Presidents of the European Parliament, the Council and the Commission. This reflects the shared political commitment of the EU and its Member States to:

- provide opportunities to all children and young people to acquire the necessary skills and competences, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices;
- promote positive experiences for children and young people in an age-appropriate and safe digital environment;
- protect all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes;
- protect all children and young people against illegal tracking, profiling and targeting, in particular for commercial purposes;
- involve children and young people in the development of digital policies that concern them.

The European Commission set out in May 2022 the new European strategy for a better internet for kids (BIK+)[26].

The BIK+ strategy provides an ambitious vision for age-appropriate digital services, with no one left behind and every European child protected, empowered and respected online. It aims for accessible, age-appropriate and informative online content and services that are in children's best interests, building on three key pillars:

1. *Safe digital experiences* to protect children from harmful and illegal content, conduct, contact and consumer risks and to improve their well-being online through a safe, age-appropriate digital environment, created in a way that respects children's best interests.
2. *Digital empowerment* so children acquire the necessary skills and competences to make sound choices and express themselves in the online environment safely and responsibly.
3. *Active participation*, respecting children by giving them a say in the digital environment, with more child-led activities to foster innovative and creative safe digital experiences.

The BIK+ strategy forms part of a new phase in European policy to protect and empower children and young people in the digital environment. In the decade since the adoption of the original BIK strategy, EU citizens have become ever more reliant on digital technologies, something that became particularly evident during the COVID-19 pandemic. To address the risks and harms of an increasingly digitalised society, including for children, the Commission outlined in December 2020[27] an ambitious reform of the digital space with a comprehensive set of new rules for all digital services, including social media, online marketplaces, and other online platforms that operate in the European Union. Thus, the updated

[25] https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

[26] https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik

[27] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

BIK+ strategy contributes to and forms part of a wider policy framework to ensure European values are at the heart of digital policies and that people are at the centre of the digital transformation in the European Union, as set out in the European Declaration on Digital Rights and Principles for the Digital Decade[28].

Additional strategies and action plans that have been adopted at the Commission level and which further support the goals of the BIK+ strategy to ensure that every child is protected, empowered and respected online are briefly described below.

3.1.2. EU Strategy on the Rights of the Child

Most notably, in March 2021, the Commission adopted its first-ever comprehensive EU Strategy on the Rights of the Child[29] in which an update of the 2012 BIK strategy was first announced. In this context, the updated BIK+ strategy can be regarded as "*the digital arm of the rights of the child strategy*" (BIK+, p.2), reflecting the recently adopted digital principle that "Children and young people should be protected and empowered online"[30]. The new comprehensive EU Strategy on the Rights of the Child and the European Child Guarantee are major policy initiatives put forward by the European Commission to better protect all children, to help them fulfil their rights and to place them right at the centre of EU policy making. The strategy brings all existing and future EU actions and policies on children's rights under one single umbrella, including children's rights in the digital world and the commitment that children and young people should be empowered and protected in the digital environment[31].

Thematic area 5 of the EU strategy on the Rights of the Child includes actions to ensure that children can safely navigate the digital environment and harness its opportunities[32]. As well as the commitment to adopt an updated Better Internet for Kids Strategy in 2022, under this thematic area the Commission commits to:

- Create and facilitate a child-led process aimed at developing a set of principles to be promoted and adhered to by the industry.
- Promote the development and use of accessible ICT and assistive technologies for children with disabilities such as speech recognition, closed captioning and others, including in Commission's conferences and events.
- Ensure the full implementation of the European Accessibility Act.
- Step up the fight against all forms of online child sexual abuse, such as by proposing the necessary legislation including obligations for relevant online services providers to detect and report known child sexual abuse material online.

EU policy towards children's participation in the digital transformation is thereby framed within a children's rights framework, reflecting a wider trend to consider online safety as a child rights issue and that offline and online need to be seen as a continuum. As signalled in the BIK+ strategy reference to international outreach and cooperation, the Commission's approach aligns with, for example, the

[28] https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

[29] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_en#the-eu-strategy-on-the-rights-of-the-child

[30] https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

[31] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12454-Delivering-for-children-an-EU-strategy-on-the-rights-of-the-child

[32] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/digital-and-information-society_en

Council of Europe Strategy for the rights of the child (2016-2021)[33] which includes children's rights on the internet as one of its five priority areas, later reinforced in the Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers (2018).[34] Similarly, the United Nations Committee on the Rights of the Child adopted in February 2021 General Comment No. 25 on children's rights in relation to the digital environment[35] setting out guidance on interpreting and implementing the UNCRC for the digital age.

3.1.3. Other relevant strategies and actions

Examples of other strategies and policies that have been initiated at the European level in recent years and which have contributed to overall EU policy on protecting and promoting children's digital participation include:

- In June 2020, the Commission adopted its first-ever EU strategy on victims' rights[36]. This strategy is comprised of a two-stranded approach focussing on the empowerment of victims of crime and collaboration among relevant actors. The strategy complements the EU Strategy for a more effective fight against child sexual abuse[37] and commits to strengthening the cooperation between law enforcement, INHOPE, and industry.
- In September 2020, the Commission launched its Digital Education Action Plan (DEAP) 2021-2027 which aims among other things to enhance digital skills and competences for the digital transformation. As set out in the action plan: "*Digital literacy has become essential for everyday life. A sound understanding of digital information, including personal data, is vital to navigate a world increasingly infused with algorithms. Education should more actively help learners to develop the ability to critically approach, filter and assess information, notably to identify disinformation and to manage overload of information as well as develop financial literacy. Education and training institutions can help build resilience to information overload and disinformation, which becomes more widespread in times of crisis and major societal upheaval. Countering disinformation and harmful speech through education and training is crucial for effective participation in society and democratic processes, especially by young people. More than 40% of young people consider that critical thinking, media and democracy are not "taught sufficiently" in school. The challenge is particularly relevant for younger students, nearly all of whom are online every day*" (p. 13)[38].
- In November 2020, the Commission launched the New Consumer Agenda 2020-2025 to empower European consumers to play an active role in the green and digital transition[39]. In the wake of the COVID-19 pandemic during which EU citizens became more reliant on digital technologies, the European Commission has set out its plans to take this agenda forward by empowering European consumers in the digital environment and by increasing consumer protection[40]. Recognising that digital transformation has radically changed consumers' lives, the agenda includes actions to tackle online commercial practices that disregard consumers' right to make an informed choice, abuse their behavioural biases or distort their decision-making processes, such as dark patterns and hidden advertising. The Commission has also

[33] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8

[34] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[35] https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0258

[37] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0607

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0624&from=EN

[39] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2069

[40] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0696

signalled its intention to look at specific safeguards and to strengthen protections for children as a specific vulnerable group, when setting rules governing the digital economy and requirements for Artificial Intelligence (AI).

- Particular attention is given to children as a vulnerable group of consumers who need to be both empowered and protected. As stated in the New Consumer Agenda: "*Children and minors are particularly exposed to misleading or aggressive commercial practices online. It is important to invest more in lifelong consumer education and awareness raising, for people at all stages of life from school onwards. This should also include the promotion of financial literacy as an essential skill for empowering consumers to make good decisions about their personal finances. Better coordination of actions among key actors at national and EU level covering issues such as access to online educational material and capacity building could help achieve synergies, constant innovation, adaptation and uptake of new online and pedagogical approaches, including through the creation of online platforms and other tools*" (p. 17)[41].
- An Action Plan for Europe's Media in the Digital Decade to support their recovery and transformation following the COVID-19 pandemic was adopted by the European Commission in December 2020[42]. The news media and audiovisual sectors are regarded as essential for democracy, Europe's cultural diversity, and digital autonomy. Again, media literacy is regarded as critical to empowering citizens in today's media environment and should be supported across various programmes and initiatives, as outlined in the European Democracy Action Plan (EDAP). Media literacy, the action plan states, should also be included in school curricula to enable children to use media services responsibly. In particular, the role of media literacy in combating disinformation is highlighted.
- In December 2020, the Commission presented its European Democracy Action Plan (EDAP)[43] to empower citizens and build more resilient democracies across the EU. This highlights, among other things, the importance of empowering young citizens to make informed decisions. Media literacy, including critical thinking, it is argued, "*is an effective capacity helping citizens of all ages to navigate the news environment, identify different types of media and how they work, have a critical understanding of social networks and make informed decisions. Media literacy skills help citizens check information before sharing it, understand who is behind it, why it was distributed to them and whether it is credible. Digital literacy enables people to participate in the online environment wisely, safely and ethically*" (p.24).
- In support of this strategic goal, the Commission has increased efforts to strengthen media literacy including further support for national media literacy campaigns, in cooperation with the European Digital Media Observatory (EDMO), the Media Literacy Expert Group, and in line with the measures carried out under the revised AVMSD. At the same time, in its aim to counter disinformation, the EDAP calls for more obligations and accountability for social media platforms which "*can be used by malicious operators for disseminating and amplifying false and misleading content and have been criticised for the lack of transparency in the use of algorithms to distribute content online and for targeting users on the basis of the vast amount of personal data generated from online activity*" (p. 22)[44].

[41] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0696&from=EN

[42] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0784

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:790:FIN

[44] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

3.2. EU laws and regulations relevant to social media

The EU policy framework underpinning children and the digital environment includes significant legal and regulatory arrangements which form a comprehensive set of rules for digital services, including social media, online marketplaces, and other online platforms that operate in the European Union.

The main components of this legal and regulatory framework may be said to comprise the following:

- The Digital Services Act (DSA)[45]
- The revised Audiovisual Media Services Directive (AVMSD)[46]
- The General Data Protection Regulation (GDPR)[47]
- The Unfair Commercial Practices Directive[48]

Each may be said to contain important measures that contribute to children's online safety and well-being in the digital environment. This evolving framework is also complemented by proposed legislative acts such as:

- The Artificial Intelligence (AI) Act[49]
- The proposal for a European Digital Identify framework (eID)[50], and
- The proposal for a Regulation laying down rules to prevent and combat child sexual abuse[51]

3.2.1. Digital Services Act (DSA)

In December 2020, the European Commission proposed a major legislative reform of the rules governing digital services in the EU: the Digital Markets Act (DMA) and the Digital Services Act (DSA)[52]. Political agreement on both proposals was reached in March and April 2022 respectively.

The DSA package is a horizontal initiative – building on the e-Commerce Directive to better address new challenges online – with a focus on issues such as liability of online intermediaries for third-party content, safety of users online, and due diligence obligations. The Digital Services Package was adopted by the European Parliament in July 2022 and, following adoption by the Council, entered into force in November 2022. The DSA is directly applicable across the EU and will apply to all regulated entities from 2024 onwards. For very large online platforms (VLOPS) and very large online search engines, the DSA will apply from an earlier date, that is four months after their designation.

The main goals of the DSA are to better protect consumers and their fundamental rights online, establish clear accountability frameworks for online platforms, and to foster innovation, growth and competitiveness within the single market. In this sense, explicit reference is made to the fact that citizens in the European Union are exposed to ever-increasing risks and harms online. Among other things, the DSA will make a significant difference by making it easier to report illegal online content and services, raising due diligence obligations for online platforms (with stronger obligations for very large ones), and equipping authorities across the Union to better supervise platforms and enforce rules.

[45] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

[46] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1808

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

[48] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32005L0029

[49] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

[51] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN

[52] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

The DSA will also require more transparency regarding content moderation and why some content is recommended to users while making it possible for users to opt out of content recommendations based on profiling.

The DSA contains rules for various online intermediary services in accordance with their role, size and impact. For the very largest platforms (i.e., those reaching more than 10 per cent of 450 million consumers in Europe), specific rules will apply covering areas such as countering illegal content, safeguards for users, obligations for transparency, risk assessment, codes of conduct and technical standards. An oversight structure will apply, primarily in EU Member States, with supervision and enforcement of the very largest online platforms undertaken by the Commission[53].

The DSA contains a range of provisions for greater protection of children online including a ban on targeted advertising aimed at children and obligations to assess and limit the risks that platforms may pose for minors. Moreover, the DSA's overall provisions regarding risk assessment and mitigation, transparency and accountability are aimed at enhancing safeguards for all users. More specifically, a key action under the BIK+ strategy is the development of a comprehensive EU Code of conduct on age-appropriate design[54]. Building on the framework of the DSA and aligned with the rules of AVMSD and GDPR, the Code, once developed, aims to reinforce the involvement of industry in protecting children when using digital products, with the ultimate goal of ensuring their privacy, safety and security online.

3.2.2. Audiovisual Media Services Directive (AVMSD)

On 2 October 2018, a revised AVMSD was approved, paving the way for "*a regulatory environment that is fairer for all players in the audiovisual sector, including more flexibility to broadcasters in terms of advertising, protecting minors and tackling hate speech in all audiovisual content, better promoting European audiovisual productions and ensuring the independence of audiovisual regulators*"[55].

Notably, under the newly introduced Article 6(a), Member States are required to enact measures for the protection of minors and to ensure that children are shielded from content that may be harmful for their development. Under Article 28b, these provisions are extended to video-sharing and video-on-demand (VOD) platforms, thus bringing services frequently used by children such as YouTube, Vimeo and TikTok within its remit.

New rules are laid out to enhance protection for children and minors from harmful content. Content that may impair the physical, mental or moral development of minors (harmful content) should only be made available in such a way as to ensure that minors will not normally hear or see them, regardless of whether such content is broadcast by TV broadcasters or provided by on-demand providers. As a result, video-sharing platforms and services are required to put in place the appropriate measures, such as tools for users to report and flag harmful content, age verification, or parental control systems. The most harmful content, such as gratuitous violence and pornography, should be subject to the strictest measures providing a high degree of control (such as encryption and effective parental controls). Meanwhile, EU co-regulation is encouraged on content descriptors (words, symbols or acoustic means of warning of bad language, sex, violence, drugs, and discrimination) which provide sufficient information to viewers about the possible harmful nature of the content. This should empower parents to make decisions for their children or for children to make decisions for themselves.

[53] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en

[54] https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design

[55] http://europa.eu/rapid/press-release_MEMO-18-4093_en.htm

The AVMSD also introduces important legal obligations regarding media literacy. Member States are required to promote and take measures for the development of media literacy skills (Art. 33a) while video-sharing platforms are also required to put in place effective media literacy measures and tools and to raise users' awareness of those measures and tools (Art.28b (3) (j)). In the text of AVMSD, it is also stated that:

> *in order to enable citizens to access information and to use, critically assess and create media content responsibly and safely, citizens need to possess advanced media literacy skills. Media literacy should not be limited to learning about tools and technologies but should aim to equip citizens with the critical thinking skills required to exercise judgment, analyse complex realities and recognise the difference between opinion and fact. It is therefore necessary that both media service providers and video-sharing platforms providers, in cooperation with all relevant stakeholders, promote the development of media literacy in all sections of society, for citizens of all ages, and for all media and that progress in that regard is followed closely* (Introduction, para 59)[56].

September 2020 was set as the deadline for the transposition of the AVMSD into national legislation. With the enactment of Ireland's Online Safety and Media Regulation Act[57] in December 2022, the last Member State to do so, all Member States have now completed the incorporation of the AVMSD into national law. A study on the implementation of the AVMSD provisions in February 2021 found that the larger platforms provide a wide array of measures to protect minors online, with a pivotal role for automated systems based on Artificial Intelligence (AI) and machine learning (ML)[58]. However, in other areas like age verification, for instance, there remains much room for improvement as the current approaches are little more sophisticated than requiring the user to input their birth date.

3.2.3. General Data Protection Regulation (GDPR)

The GDPR entered into force in May 2016 and has applied since May 2018[59]. The GDPR contains explicit recognition that children's personal data merits specific protection and outlines the required conditions of consent and transparency for processing children's data. Article 6(1)(f), for example, provides that processing of data based on legitimate interests can be outweighed by the interests or fundamental rights and freedoms of data subjects, "*in particular where the data subject is a child*". Article 8 deals with the processing of children's data on the basis of consent and sets out that such processing is only lawful if the child is over 16 years – or the applicable digital age of consent – or if consent has been received by a person with parental responsibility. Article 12 GDPR also addresses requirements for transparency and states that children, as much as adults, are entitled to receive information about the processing of the data in clear and plain language.

The GDPR has had wide-ranging implications for children's participation in the digital environment. This includes the much-discussed issue of the minimum age a user must be before a social media or internet company can collect, process and store their data, the consent to some data processing practices to be given by parents, the obligation for companies processing children's personal data to provide information in child-friendly language, or the duty for data protection authorities to put in place activities promoting public awareness of these issues among children[60]. However, the GDPR has also raised a number of questions about the possible (unintended) consequences that may arise in

[56] https://eur-lex.europa.eu/eli/dir/2018/1808/oj

[57] https://www.oireachtas.ie/en/bills/bill/2022/6/

[58] https://ec.europa.eu/digital-single-market/en/news/study-implementation-new-provisions-revised-audiovisual-media-services-directive-avmsd

[59] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[60] See also https://www.betterinternetforkids.eu/practice/awareness/article?id=694148

limiting children's rights to communicate with their peers, engage online with educational, health and other valuable resources, or participate in online civic and public spheres[61]. Data protection authorities have moved to provide more detailed guidance on the application of GDPR provisions to children's data processing, for example, in the Irish Data Protection Commission's *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*[62].

3.2.4. The Unfair Commercial Practices Directive

The Unfair Commercial Practices Directive (UCPD)[63] from 2005 is the overarching EU legislation regulating unfair commercial practices in business-to-consumer transactions and specifically protects children as vulnerable consumers[64]. Unfair commercial practices under UCPD are defined as either *distorting* or contrary to professional diligence; *misleading* in the sense of containing false information or which is likely to deceive the average consumer, for example, by hiding the commercial intent of the commercial practice; or *aggressive* by impairing or limiting the consumer's freedom of choice or decision to make a purchase that might not otherwise be made. The UCPD is a principles-based instrument designed to keep pace with fast-evolving circumstances. As such, it remains highly relevant to the digital environment and to children as a vulnerable group of consumers. Under the UCPD, therefore, encouraging children directly to buy things or persuade their parents or other adults to buy advertised products for them ("pester power") is an unfair commercial practice that is expressly prohibited. Guidance on the application of the UCPD published by the European Commission in 2021[65] contains further relevant sections on protecting children from unfair practices in such areas as social media marketing and the activities of influencers. For example, influencers must state clearly if they are paid to promote items. The guidelines also address such areas as misleading prizes or in-app purchases presented as upgrades.

3.3. Legislative proposals

There are also a number of important legislative proposals under consideration and yet to be enacted that are significant for the wider digital ecosystem and for children's social media use. These include the Artificial Intelligence (AI) Act, the proposal for a European Digital Identify framework (eID)[66] and the proposal for a Regulation laying down rules to prevent and combat child sexual abuse[67].

3.3.1. The Artificial Intelligence (AI) Act

The proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)[53] was presented by the Commission in April 2021. It contains new rules to make sure that AI systems used in the EU are safe, transparent, ethical, unbiased and under human control. A risk-based approach is presented differentiating between AI uses that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. The legal text considers children as a specific vulnerable group in several parts. Prohibited practices include AI systems that have a significant potential to manipulate or exploit by subliminal means vulnerable groups such as children (p.12). Under Article 9, specific consideration

[61] https://www.betterinternetforkids.eu/practice/awareness/article?id=687352

[62] https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

[63] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32005L0029

[64] https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en

[65] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)&from=EN

[66] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

[67] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN

must be given in implementing the risk management system where the service is likely to be accessed by or have an impact on children.

Prior to the AI Act, the Commission first put forward its Strategy on Artificial Intelligence in April 2018[68] with the aims of placing Europe at the forefront of technological developments, preparing for the socio-economic changes brought about by AI and laying out an appropriate ethical and legal framework to ensure that AI is human-centric and trustworthy.

The work of the High-Level Expert Group on Artificial Intelligence (AI HLEG)[69] is relevant in this regard. The AI HLEG Ethics Guidelines for Trustworthy AI included among its key ethical principles the need to:

> *pay particular attention to situations involving more vulnerable groups such as children, persons with disabilities and others that have historically been disadvantaged or are at risk of exclusion*" (p. 2).[70] Elsewhere, the AI HLEG recommends to "*establish a European Strategy for Better and Safer AI for Children, in line with the European Strategy for a Better Internet for Children, designed to empower children, while also protecting them from risks and potential harm. The integrity and agency of future generations should be ensured by providing Europe's children with a childhood where they can grow and learn untouched by unsolicited monitoring, profiling and interest-invested habitualisation and manipulation* (p. 14)[71].

This aligns with the views expressed in the original BIK strategy to ensure children and young people have access to "online playgrounds" where they can experiment, play, develop and learn in a free and unmonitored manner. However, children should also enjoy the "right to be forgotten" or right to erasure so that when they move into adulthood, they should be able to start afresh without any permanent consequences of their youthful digital technology use or have unnecessary data stored about them.

3.3.2. European Digital Identity framework (eID)

In June 2021, the Commission proposed a framework for a European digital identity (eID)[72] that would be available to all EU citizens, residents and businesses via a European digital identity wallet. The proposal would require Member States to issue a digital wallet under a notified eID scheme, built on common technical standards with a common standard defining the technical specifications of the wallet, thereby providing citizens with a harmonised European digital identity. Alongside its other attributes and benefits, access to a common European digital identity would provide a simple and safe way to confirm online and offline identity, enable cross-border authentication, and give users control over how much information they wish to share with third-party services and keep track of such sharing. As noted in the BIK+ strategy, such a framework "*will enable minors, on the basis of national laws, to use the Digital Identity Wallet, for example, to prove their age without disclosing other personal data"* (p.4).

The proposed framework builds on the eIDAS Regulation of 2014[73] which is currently the only cross-border framework for trusted electronic identification (eID) of natural and legal persons, and trust services, such as electronic signatures. The eIDAS Regulation does not harmonise national eIDs but instead enables their mutual recognition through a notification process. Member States notify eID schemes on a voluntary basis and there is, at present, no obligation on Member States to provide

[68] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

[69] https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[70] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[71] https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence

[72] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910

citizens with secure electronic identification services. Given the many changes in technology since its adoption and increased demand for secure and trusted services, a new European eID framework would provide a further crucial building block in the overall digital ecosystem. However, many challenges remain to the implementation of common EU standards in this area. Not all Member States use eIDAS and, of those that do, very few make digital identities available for children. Accordingly, the Commission has also funded complementary initiatives such as euCONSENT[74] to examine practical interim methods and approaches to robust age verification and age assurance which could meet the technical requirements of the planned European standard, once approved.

3.3.3. Regulation laying down rules to prevent and combat child sexual abuse

In May 2022, the European Commission proposed a new EU Regulation laying down rules to prevent and combat child sexual abuse[75]. The proposal builds on longstanding initiatives at the European level including Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (CSA/CSE), the aim of which is to ensure that what is illegal offline is illegal online. In 2017, the Commission published a Communication on tackling illegal content online[76] followed by a Recommendation on measures to effectively tackle illegal content online[77]. Both echoed the original BIK strategy in their call for smooth, effective and appropriate cooperation on the protection side between competent authorities and hosting service providers.

In July 2020, the Commission launched its EU Strategy for a more effective fight against child sexual abuse[78]. The strategy presented a comprehensive response to the increasing threat of child sexual abuse, both in its online and offline form and outlined a range of initiatives, both legislative and non-legislative, covering prevention, law enforcement, and assistance to victims. The legislative proposal on child sexual abuse which followed in May 2022 forms part of this overall approach and is integral to a framework to making the fight against child sexual abuse more effective in the EU. Of note is the support and contribution of INHOPE and member hotlines to the respective initiatives as it directly pertains to the work of the INHOPE network. INHOPE actively contributed to the public consultation and continues to contribute to and enhance the evidence base underpinning the initiative.

The new proposal for a CSA Regulation updates this approach and is designed to complement the DSA with a specific focus on combating online child sexual abuse and exploitation. The proposed legislation makes it mandatory for service providers to report child sexual abuse online on their platforms and to alert the authorities. Providers will also be required to report cases of grooming – where sexual predators seek to manipulate, exploit and abuse children through online contacts. The proposed legislation lays out plans for an EU Centre to be established to coordinate actions to fight against child sexual abuse, from detection and reporting to prevention and assistance to victims. The centre will work with companies, research institutes, and law enforcement to help them exchange information and best practices, providing oversight, transparency and accountability. The EU Centre will also directly support law enforcement in acting on reports, working closely with similar centres internationally while also providing companies with indicators to find and report online child sexual abuse. Currently, under a temporary derogation from the e-Privacy Directive 2002/58/EC[79], providers voluntarily scan communications and process personal and other data for the purpose of combating

[74] https://euconsent.eu/euconsent-and-the-better-internet-for-kids-strategy/

[75] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN

[76] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=47383

[77] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50095

[78] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0607

[79] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568

online child abuse. The proposed Regulation will replace this arrangement and place mandatory obligations on providers to detect and report child sexual abuse material.

3.4. Developments and trends at the international level

The range of EU policy and legislative developments addressing children's online safety and well-being come at a time when internationally, a noticeable shift towards stricter regulation and enhanced online safety is in evidence. While headline legislative developments such as the coming into effect of the GDPR may be said to be at the forefront of such actions, stricter rules regarding basic online safety requirements, content moderation and transparency now feature in several international regions. This is further underpinned by a more fundamental turn towards recognising and implementing children's rights in the digital environment.

3.4.1. The rights of the child in the digital environment

With respect to keeping children safe online, there has been an evident shift in the discourse away from protection and online safety for its own sake towards situating online safety concerns within the framework of children's rights. The shift from *safer* to *better* internet policies, as set out in the European Strategy for a Better Internet for Children (the original BIK strategy), is a forerunner to this development which sought to balance children's online safety with considerations of positive opportunities, empowerment and well-being. More directly, the recognition that the fundamental rights of children that apply offline also have an equivalent application online, has provided new impetus for policy development.

The adoption by the UN Committee on the Rights of the Child of General Comment No. 25 (2021) on children's rights in relation to the digital environment[80] is an important milestone in this regard. The UN Convention on the Rights of the Child (or UNCRC)[81] sets a global standard for assessing the treatment of children and the fulfilment of their fundamental human rights. Drafted before the rise of the internet, the UNCRC does however recognise the importance of media for children's development. Article 17 of the UNCRC states that children and young people should be able to access information, particularly from the media and should be able to get information from many places— from their country and beyond.

General Comment 25 identifies the digital environment as an important dimension in which children's rights should be promoted and realised. It explains how States parties should implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment. Among its recommendations, General Comment 25 highlights the obligations of States Parties to:

- Ensure that businesses meet their responsibilities to respect children's rights and remedy abuse (p.6, para 35)

[80] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[81] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

- Monitor compliance of businesses in preventing their services from contributing to the violation or abuse of children's rights (p.7, para 36)
- Require the business sector to undertake child rights due diligence, including the use of child rights impact assessments and to disclose them to the public (p.7, para 38)
- Require business enterprises to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety (p.7, para 39)
- Consider appropriate measures to enable the detection and reporting of child sexual exploitation and abuse or child sexual abuse material in the case of encrypted networks, noting that such measures must be strictly limited according to the principles of legality, necessity and proportionality (p.12, para 70).

A further articulation of this agenda is contained in the Council of Europe's Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment[82]. Adopted in July 2018, this far-reaching recommendation sets out detailed guidelines regarding the right to be heard, access to the digital environment, rights to freedom of expression and information, and empowerment through digital literacy while considering the importance of safety, security and data protection and privacy. It recommends that governments review their legislation, policies and practice to ensure children's rights are promoted within a digital context, that appropriate oversight is developed to ensure that business enterprises meet their responsibilities and that all relevant stakeholders ensure concerted action and cooperation at the national and international level to uphold and respect children's rights.

This is further supported by the Handbook for policymakers on the rights of the child in the digital environment[83], which elaborates on guidance to policymakers in dealing concretely with the online rights and protection of children with a focus on national frameworks and policies that ensure the respect of children's rights online. A Declaration by the Committee of Ministers adopted in April 2021[84] further calls on Member States to intensify their efforts to protect children's privacy in the digital environment, with particular reference to education settings.

3.4.2. Age appropriate design

A further noteworthy trend in policy to promote children's online safety has been a focus on age appropriate design which emphasises both guidelines as design requirements for digital services that are used by children as well as obligations on digital providers to ensure that children's best interests are to the fore when offering such services. A safe, *age appropriate* digital environment is a fundamental principle of the BIK+ strategy within which the European Commission undertakes to "*facilitate a comprehensive EU code of conduct on age-appropriate design, building on the new rules in the DSA and in line with the AVMSD and GDPR*" (2020, p.9)[85].

There is no single definition of what is constituted by age appropriate design. However, in the context of children's participation in the digital environment, age appropriate design may be said to refer to digital products and services that are suitable for children given their age or stage of development, in line with the evolving capacities of children as set out in Article 5 UNCRC (see Van Der Hof, 2021). A

[82] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[83] https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8

[84] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a2436a

[85] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

diverse range of international initiatives now advocate that to make children's online experiences safer, key principles of safety, security, and privacy should be incorporated into the design process from the very start and should shape and inform all further stages of the product life cycle rather than seek to retrofit child safety into products that were designed for adults (Pothong & Livingstone, 2021).

In June 2028, Australia's Office of the eSafety Commissioner outlined Safety by Design Principles[86] to help guide organisations to embed the rights of users and user safety into the design and functionality of digital products and services. Drawing on a number of models of online risks and harms, including the 4Cs classification of content, contact, conduct and contract risks (Livingstone & Stoilova, 2021), the Principles address three main priorities:

- *Service provider responsibility*: the burden of safety should not fall solely on the user, and every attempt needs to be made that online harms are understood, assessed and addressed in the design and delivery of online platforms and services.
- *User empowerment and autonomy*: products and services should align with the best interests of users.
- *Transparency and accountability*: a robust approach to safety needs to be underpinned by assurances that platforms and services are operating according to their published safety objectives.

The United Kingdom's Age Appropriate Design Code[87] (AADC, also known as the Children's Code) is one of the first statutory codes of practice on a national level that builds on the GDPR's requirement that children's data be afforded special protection. The Children's Code is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. It outlines 15 standards that online services need to follow in prioritising the best interests of the child. These include mapping the personal data of children that may be collected, carrying out age checks, turning off geolocation services that track users, avoiding nudge techniques, and providing a high level of privacy by default. The Code came into force in September 2020 with a transition period with organisations required to conform by 2 September 2021.

Privacy by design and age appropriate design principles have also featured in recent legislative proposals originating in the United States.

- The Californian Age-Appropriate Design Code Act[88] was enacted by the Californian Legislature in August 2022 and will come into effect in July 2024. Based on the United Kingdom's AADC, the Act requires platforms to proactively assess the privacy and protection of children in the design of any digital product or service that they offer. In a significant departure from US federal law, the Act defines a child as anyone under 18 in contrast to age 13 which has been the standard set for data privacy purposes.
- The Children and Teens' Online Privacy Protection Act[89] (COPPA 2.0) is a federal legislative proposal to amend the Children's Online Privacy Protection Act (COPPA) of 1998[90] to strengthen protections related to the online collection, use, and disclosure of personal information of children and minors up to age 16. The provisions of the 1998 COPPA have had

[86] https://www.esafety.gov.au/industry/safety-by-design/principles-and-background

[87] https://ico.org.uk/for-organisations/childrens-code-hub/

[88] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

[89] https://www.congress.gov/bill/117th-congress/senate-bill/1628/text

[90] http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

global influence arising from the fact that the majority of social media platforms have set 13 as the minimum age for registering a profile on the service. Below this age, verifiable parental consent is required to comply with COPPA. With COPPA 2.0, internet companies would be prohibited from collecting data from13-16-year-olds without the child's consent. COPPA 2.0 also proposes to prohibit behavioural and targeted marketing to children. The proposal also allows for an online eraser mechanism that would enable users to delete information from a child or teenage account. COPPA 2.0 also provides for the creation of a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC), which would be responsible for addressing concerns regarding youth privacy and marketing practices.

- The Kids Online Safety Act (KOSA)[91] is a proposal for federal legislation directed at platform design and operations used by children. The Bill contains provisions whereby social media platforms are required to prevent and mitigate harmful content for minors; default privacy levels for minors set to the highest level; providing privacy controls such as the ability to opt out of recommendation systems, or to limit features that seek to extend use; and user controls that would limit the time a child may spend on a service.
- The Children and Media Research Advancement (CAMRA) Act[92] was passed by the US Congress in December 2022 as part of a package of spending measures. CAMRA directs the National Institutes of Health to fund research regarding the effects of media on infants, children, and adolescents. Such research must examine the impact of media (e.g., social media, television, video games) on cognitive, physical, and social-emotional development. The director of the National Institutes of Health must deliver a report to Congress on its work within two years of the law's enactment.

As a number of legislative proposals are still under consideration, many of the above remain subject to significant amendment and may be enacted, if at all, in a different form. However, for the purposes of this study, they illustrate how children's safety when using social media has been adopted within policy discourse and the extent to which the concept of age appropriate design has been embedded within proposed solutions to online risks considered in the next section.

[91] https://www.congress.gov/bill/117th-congress/senate-bill/3663/text

[92] https://www.congress.gov/bill/117th-congress/senate-bill/971?s=1&r=64

4. RESPONSES AND SOLUTIONS

KEY FINDINGS

Supporting children's online well-being is a multistakeholder activity reflected in the many different programmes and initiatives carried out nationally and at the EU level to raise awareness, lessen the chance of children encountering risks and to support children if they become victims of online harm.

Research highlights the importance of awareness raising and digital literacy to empower children to have the necessary skills to safely and responsibly manage their use of digital services. The Insafe network of Safer Internet Centres plays a vital role in this regard.

Risk mitigation is a key focus of current policy, illustrated by the shift from self-regulatory initiatives to more direct forms of regulation and co-regulation. The proposed development of a comprehensive EU code of conduct on age-appropriate design within the framework of the Digital Services Act and support for effective age verification techniques are important examples.

Technology can also play a key role in mitigating risks and creating a safer online environment for children.

Alongside awareness raising and risk mitigation, extensive supports exist for victims for which the Model National Response (WeProtect Global Alliance, 2016) provides a valuable template.

Supporting children to be safe, protected and empowered when they go online encompasses many different programmes, actions, and interventions involving diverse stakeholders at EU, national and regional levels. Responsibility for children's online safety is often considered to be a shared one both due to the complexity of the topic and the need to support parents and educators in the task of guiding children's growing autonomy in the digital environment. Responses and solutions to keeping children safe online take a number of different forms from education about the risks, measures to prevent risks happening through to supporting victims of online harm. In this section, illustrative examples are briefly reviewed under the headings of raising awareness, risk mitigation and assistance to victims.

4.1. Raising awareness

Raising awareness of the risks that children may face when using social media is central to online safety education. The aim of awareness raising is to increase people's understanding and knowledge of an issue, often with the goal of making them alter their behaviour. Such efforts have long been promoted to make users, parents, guardians and children more aware of the potential benefits of the internet as well as its downsides. Raising awareness was one of the three pillars of the original Safer Internet Programme alongside combating illegal content online and content classification for potentially age inappropriate content.

4.1.1. Safer Internet Centres

Raising awareness is central to the role of Safer Internet Centres (SICs). SICs operate in all EU Member States as well as in Iceland, Norway and the United Kingdom and are co-funded under the Digital

Europe Programme (and previously, the Connecting Europe Facility programme)[93]. Safer Internet Centres exist to inform, advise and assist children, parents, teachers and carers on issues related to the digital environment to fight against online child sexual abuse and other illegal content online. The Better Internet for Kids core service platform and related activities is managed on behalf of the European Commission by European Schoolnet (EUN)[94], which coordinates the Insafe network of awareness centres, helplines and youth panels, in partnership with INHOPE[95] (the International Association of Internet Hotlines), dedicated to the removal of illegal online content.

SICs typically comprise an awareness centre, helpline, hotline and youth panel which cooperate as follows:

- Awareness centres focus on raising awareness and understanding of safer internet issues and emerging trends, and are organised within the context of the Insafe network[96].
- Helplines provide information, advice and assistance to children, youth and parents on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct such as (cyberbullying or sexting).
- Hotlines allow members of the public to report illegal content anonymously. Reports are then passed on to the appropriate body for action (internet service provider, Law Enforcement Agency in the country or corresponding INHOPE Association Hotline).
- Youth panels represent the voices of young people regarding their use of online technologies. They also advise on online safety and empowerment strategy, contribute to the development of resources and disseminate eSafety messages to their peers.

Operating as a network, SICs co-operate and exchange resources and best practices at EU level through the betterinternetforkids.eu portal, the EU hub for child online safety.

4.1.2. Awareness nodes

The Awareness Centre within each SIC specialises as a point of contact at the country level on safer and better internet policies and issues. Awareness Centres undertake the following indicative activities:

- Raise awareness of online safety and of potential risks that young people may encounter online;
- Observe emerging trends;
- Run campaigns and develop information material for parents, children and teachers;
- Organise information sessions and events such as the annual Safer Internet Day campaign;
- Contribute to the SIC's work in empowering children and people, their parents and carers and educators to equip with the necessary knowledge and skills for online safety.

The Insafe network of awareness centres leverages the collective expertise and resources of individual awareness nodes as illustrated in the extensive range of resources made available on the Better Internet for Kids portal[97]. Awareness centres work extensively with other stakeholders, such as the research community, industry and other NGOs, to extend the reach of key messages and awareness raising

[93] https://digital-strategy.ec.europa.eu/en/policies/safer-internet-centres

[94] http://www.eun.org/

[95] https://www.inhope.org/EN

[96] https://www.betterinternetforkids.eu/en/policy/insafe-inhope

[97] https://www.betterinternetforkids.eu/en/

actions. Key actions include the annual Safety Internet Day (SID) campaign and Safer Internet Forum (SIF) event as well as individual campaigns and initiatives.

In February 2020, the Youth Pledge for a Better Internet was launched as part of the SID campaign[98]. This initiative of the (BIK) Youth Ambassadors consisted of a pledge on how to make information on the apps and services used by young people more age appropriate. After an initial mapping of research and youth consultation work carried out by Safer Internet Centres in the Insafe network, the BIK Youth Ambassadors collated a range of issues that should be prioritised to ensure that online platforms and services are designed in an age-appropriate way to meet children and young people's developmental needs. These were subsequently presented to members of the Alliance to better protect minors online[99] – a self-regulatory initiative, overseen by the European Commission, designed to improve the online environment for children and young people – at the SID 2020 event. It was agreed that an ongoing dialogue would take place between youth and industry representatives to progress the aims of the pledge.

Following its launch, a number of co-design workshops have been initiated within the framework of the Youth Pledge in partnership with six member companies of the Alliance (Meta, Lego, Samsung, Sulake, Super RTL and Twitter). The Youth Pledge continues as an initiative of the Better Internet for Kids programme and includes a best practice guide on age appropriate design with youth[100]. The March 2021 BIK Bulletin was dedicated to the Youth Pledge.

The annual Safer Internet Forum held in the autumn of each year is another central awareness raising event. This international conference brings together young people, parent and teacher representatives, industry and government policy makers, technology and awareness raising experts, and political, educational and social leaders from Europe and beyond. As the main multi-stakeholder event of the Better Internet for Kids programme, it provides a key platform to highlight issues and awareness priorities concerning the impact of the digital transformation on youth. In line with the BIK+ strategy's participation pillar, the Safer Internet Forum seeks to amplify the voices of children and young people and through its consultation work, actively involve young in dialogue with policymakers and in digital policymaking.

4.1.3. Safer Internet Day

The annual Safer Internet Day campaign[101] which is coordinated by EUN and Insafe is a key focus for awareness centres and provides the most prominent example of awareness raising. Safer Internet Day began as an initiative of the EU SafeBorders project in 2004 and was taken up by the Insafe network as one of its earliest actions in 2005[102]. Safer Internet Day has evolved beyond its original European base and is now celebrated in approximately 180 countries and territories worldwide. From 2009 onwards, local organisation came under the auspices of Safer Internet Day Committees which further liaise with the Safer Internet Day Coordination Team in Brussels to strengthen linkages with countries outside the Insafe network and to ensure a harmonised promotion of the campaign across the world. Currently, more than 150 global SID Committees (and those working towards SID Committee status) now work

[98] https://www.betterinternetforkids.eu/en/policy/youth-pledge-for-a-better-internet

[99] https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online

[100] https://www.betterinternetforkids.eu/documents/167024/200055/Best-practice+guideline+-+Age-appropriate+design+with+youth+-+March+2021+-+FINAL.pdf/449ee94e-ce0d-c4be-d9cf-d768381d997c?t=1617107095397

[101] https://www.saferinternetday.org/

[102] https://www.saferinternetday.org/about

closely with the Safer Internet Day Coordination Team led by EUN on behalf of the European Commission.

Recent editions of Safer Internet Day, which takes place on the second day of the second week each February, have operated under the global campaign slogan of "Together for a better internet" to call attention to the importance of both a safer and a better internet, where everyone is empowered to use technology responsibly, respectfully, critically and creatively. The SID campaign targets a range of stakeholders – children and young people, parents and carers, teachers, educators and social workers, as well as industry, decision-makers and politicians – to encourage everyone to play their part in creating a better internet. National SID Committees implement awareness campaigns more locally, often with target themes tailored to relevant issues in the region.

Selected examples from the 2021 SID campaign (which took place within the constraints of the COVID-19 pandemic) include the following:

- In Bulgaria, in an event proposed by its Youth Panel, the topic of false information online was chosen and included demonstrations and short role-play debates on the most prevalent instances of false information, especially during the COVID-19 pandemic. Young people were engaged to join in debates about the dangers of fake news, how fake news can be circulated virally, and how it may be challenged, minimised or stopped.
- The German SID campaign similarly addressed disinformation through the theme of "What do I believe? Opinion making between fact and fake". This included learning resources and lesson plans to support classroom discussions.
- In Croatia, the main event was a webinar in which children had the opportunity to address a panel of well-known YouTube influencers about their approaches to online safety.
- Ireland's Safer Internet Centre hosted the #BeKindOnline webinar series, providing free webinars for parents and teachers to empower healthier online behaviour in children and young people. Additional activities for students encouraged them to reflect on issues around well-being online, particularly in the context of adolescent mental health in a time of crisis. Youth participants in an online peer-led training programme also shared their experiences.
- In the Netherlands, the Dutch Safer Internet Centre released a survey on online well-being during the COVID-19 period, with a special focus on online love and sexuality. The Dutch Helpline had witnessed an increase in calls for online help requests during COVID-19 lockdowns. However, as found by its survey, young people did not experience an increase in negative experiences (such as experiencing online sexual harassment, cyberbullying, and similar) than before COVID-19 with some respondents reporting that the atmosphere on social media was now more positive than before.

Safer Internet Day 2022 reached over 19,000 schools involving over 5,800 organisations across Europe. Worldwide, approximately 200 countries and territories participated in Safer Internet Day in some way.

4.2. Risk mitigation measures

Alongside awareness raising as one cornerstone of European policy to keep children safe are actions involving risk mitigation, i.e., initiatives to minimise risks to children when they use digital services so that they do not become a victim in the first place. Supporting safe digital experiences – protecting children from harmful and illegal online content, conduct, and risks and improving their well-being through a safe, age-appropriate digital environment – is indeed the first pillar of the BIK+ strategy, the main themes of which were addressed in section 3 on the EU Policy Framework. Complementing this analysis are a number of wider initiatives to support a safe environment for children such as industry self-regulation and the use of safety technologies.

4.2.1. The ICT Coalition for Children Online

The ICT Coalition for Children Online[103] is a self-regulatory initiative established in 2010 in which companies hold each other to account and sign up to a set of guiding principles to ensure that the safety of younger internet users is integral to the products and services. In 2012, the alliance developed the Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU[104] (the "ICT Principles") to encourage best practice in the areas of content, parental controls, dealing with abuse/misuse, child sexual abuse content or illegal content, privacy and control, and education and awareness. Members of the alliance pledge to encourage the safe and responsible use of online services and internet devices among children and young people, while supporting parents and carers in their supervisory role. At its inception, this was the first industry-led Europe-wide code of practice in the online safety arena and has served as a roadmap for the member companies, complementary to other national, European, and international policy initiatives. The membership comprises online service providers and telecommunications companies. Among the social media platforms which are members are Facebook, Google (YouTube), TikTok, Twitter and Yubo.

To support the transparency of its processes and to promote it as a robust self-regulatory process, companies publish self-assessment reports of individual company contributions to implementing the ICT Principles. This has been followed by periodic, independent reviews of the overall implementation. The first assessment of the ICT Principles took place in 2014 with a second full assessment currently underway[105].

4.2.2. Alliance to better protect children online

The Alliance to better protect minors online[106] is a self-regulatory initiative, overseen by the European Commission, which is designed to bring industry members together to improve the online environment for children and young people. The Alliance followed its predecessor initiative, the CEO Coalition, in 2017 as the primary self-regulatory initiative in Europe aiming to work together on online safety, particularly in those areas which can benefit from a coordinated approach and to achieve a model of innovation which places the safety of minors at the heart of its interests. The framework of the Alliance was set out in a Statement of Purpose, announced during Safer Internet Day 2017, in which

[103] https://www.ictcoalition.eu/

[104] https://www.ictcoalition.eu/medias/uploads/source/ICT%20Principles.pdf

[105] First Report on the Implementation of the ICT Principles. (2014). Available at: https://www.ictcoalition.eu/medias/uploads/source/First%20Report%20on%20the%20Implementation%20of%20the%20ICT%20Principles.pdf

[106] https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online

companies agreed to curb harmful content, harmful conduct and harmful contact (cyberbullying, sexual extortion and exposure to violent content), through three strands of action:

- User empowerment to promote enhanced use of parental tools, content classification and other tools for online safety. Reporting tools will be provided in a more accessible and user-friendly way. Companies will also focus on improving follow-up measures such as feedback and notifications.
- Companies commit to intensify cooperation and sharing of best practices, also by considering relevant input from NGOs, civil society, European, national and local authorities, and international organisations.
- Members of the Alliance intend to scale up awareness raising and also to promote and increase access to positive, educational and diversified content online.

The Alliance includes within its membership large social media platforms such as Facebook, TikTok and Twitter[107]. An independent evaluation in 2019[108] found that the Alliance is an original, relevant means to protect minors online. The evaluation also found that it had unrealised potential to foresee, discuss and forge common solutions across different stakeholder types, including existing and emerging threats to the safety of minors online. In 2020, several members of the Alliance signed up for the BIK Youth Pledge initiative, exploring ways to actively involve children and young people in the co-design of online platforms, and make privacy information on apps and services more age appropriate[109].

4.2.3. Online safety codes

Codes of practice based on self-regulation have a long history within European policies for online safety going back to the European Framework for Safe Mobile Use by Teenagers and Young Children – a self-regulatory initiative of the European mobile industry[110] and the EU Safer Social Networking Principles launched in 2009. A noteworthy trend has been a turn towards codes of practice deployed on a co-regulatory basis, and which have recently featured as key instruments to address particular types of harmful or illegal online content, such as hate speech and online disinformation.

The **EU Code of conduct on countering illegal hate speech online**[111] was launched in May 2016, to prevent and counter the spread of illegal hate speech online. The European Commission, together with Facebook, Twitter, YouTube and Microsoft, unveiled a Code of Conduct that included a series of commitments to combat the spread of illegal hate speech online in Europe. Instagram, Google+, Snapchat Dailymotion and TikTok subsequently announced their participation. Among other things, participating companies commit "*to educate and raise awareness with their users about the types of content not permitted under their rules and community guidelines*" but also to "*strengthen partnerships with civil society organisations by widening the geographical spread of such partnerships and, where appropriate, to provide support and training to enable CSO partners to fulfil the role of a "trusted reporter" or equivalent, with due respect to the need of maintaining their independence and credibility*" (p.3)[112].

[107] https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online

[108] https://digital-strategy.ec.europa.eu/en/library/report-independent-evaluation-alliance-better-protect-minors-online

[109] https://www.betterinternetforkids.eu/practice/articles/article?id=6189531

[110] https://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/ .

[111] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination-0/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[112] http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

The implementation of the Code of Conduct is evaluated through a regular monitoring exercise set up in collaboration with a network of organisations located in the different EU countries. Using a commonly agreed methodology, these organisations test how companies are implementing the commitments in the Code[113]. The most recent monitoring round published in November 2022 shows that the average removal rate (63.6 per cent) is similar to 2021 (62.5 per cent), but still lower than in 2020 (71 per cent). Evaluation has found that the quality of feedback to users' notifications has improved as compared to previous monitoring exercises[114]. In addition, the Commission also encourages participating companies to complement their focus on notice-and-action procedures with further support for more proactive awareness raising and education solutions, tackling the cause of online hate at its roots.

In September 2018, representatives of online platforms, leading social networks, advertisers and the advertising industry agreed on the self-regulatory **Code of Practice on Disinformation**[115]. Signatories committed to partnering with civil society, governments, educational institutions, and other stakeholders to support efforts aimed at improving critical thinking and digital media literacy. Online platforms and trade associations representing the advertising sector submitted a baseline report in January 2019 setting out the state of play of the measures taken to comply with their commitments under the Code of Practice on Disinformation. A self-assessment report of the signatories was published in October 2019 after one year of implementation of the Code[116]. The Commission published its assessment of the Code in September 2020[117] finding some important gaps and shortcomings despite the fact that the Code provided a valuable framework for a structured dialogue between online platforms and had brought about greater transparency of policies on disinformation. Following the issuance of Guidance by the Commission on strengthening the Code in May 2021[118], a Strengthened Code of Practice was delivered in June 2022.[119] In addition to the Code, the Commission also funds the European Digital Media Observatory (EDMO)[120] the aim of which is to create and establish a community of fact-checkers and researchers to help address and reduce the impact of disinformation at the EU, but also at the national level.

A key action outlined in the BIK+ strategy is facilitating the development of a **comprehensive EU code of conduct on age-appropriate design**. The Code aims to reinforce the involvement of industry in protecting children when using digital products, with the ultimate goal of ensuring their privacy, safety and security online. This process is explicitly aligned with the DSA Regulation where, under Article (52b), providers of online platforms are required to take appropriate and proportionate measures to protect minors, including "*adopting standards for protection of minors, or participating in codes of conduct for protecting minors"*. Online providers, according to the DSA, should consider best practice and available guidance such as that provided by the BIK+ strategy[121]. The development of the Code is also in line with obligations towards protection of minors under AVMSD and the special consideration

[113] https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/assessment_of_the_code_of_conduct_on_hate_speech_on_line_-_state_of_play__0.pdf

[114] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination-0/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[115] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[116] https://digital-strategy.ec.europa.eu/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

[117] https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

[118] https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation

[119] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

[120] https://edmo.eu/

[121] Article (52b) Protection of Minors https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

accorded to the processing of the personal data of minors under GDPR. The process of establishing a Special Group to assist the Commission in the development of the code was initiated in December 2022[122]. Its Terms of Reference include contributing to drafting of the Code and establishing a monitoring system including KPIs and a baseline.

4.2.4. Online safety technologies

Another key dimension of risk mitigation is the deployment by social media platforms of processes, strategies and technologies to prevent their misuse and to mitigate against violations of their terms of service or community guidelines. Moderating user-generated content on social media platforms involves a combination of user reporting (where users flag potential violations of the platform's community standards), human staff moderation and review of breaches of the rules and automated technologies to detect harmful content. The use of technology in content moderation systems offers benefits in part due to its ability to work efficiently at scale while reducing the burden on human moderators having to review continuous streams of harmful content. Although the effectiveness and accuracy of such solutions continue to improve, concerns remain about the reliability and accuracy of automated processes to detect diverse categories of harmful content reliably (Singh, 2019). Human moderation, therefore, remains an integral part of the content moderation process, particularly with regard to making decisions about removing content or accounts and reporting them to law enforcement.

An area where online safety technologies have proved effective to some extent is in the detection of child abuse material. Technologies based on digital fingerprinting or hash matching are the longest-established and most widely deployed. Hash matching technologies are used to tag, remove and prevent the re-upload of known images and videos of known child sexual abuse material. PhotoDNA, developed by Microsoft in 2009 is the most widely known and creates a unique digital signature (known as a "hash") of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. When matched with a database containing hashes of previously identified illegal images, PhotoDNA can help detect, disrupt and report the distribution of child sexual abuse material. PhotoDNA has been in use for over 10 years and is known to have a high degree of accuracy in the detection of child exploitation images[123].

Using technology to detect potentially harmful behaviour online is another area of online safety technology innovation. This poses greater challenges though the use of AI and machine learning continues to evolve in this area. Typically using algorithmic-based classifiers and forms of pattern recognition to identify potentially violative content, these technologies are not as accurate and need to be trained on large datasets to improve their effectiveness. Thorn's Safer tool[124], Google's Content Safety API[125], and Meta's AI technology[126] are examples of technologies that use or incorporate classifiers and AI technology to detect previously unknown child exploitation material. Combined with tools that detect known and previously "hashed" abuse material, their effectiveness in detecting new patterns of potential harm can be improved. Grooming or the solicitation of children for sexual purposes is an example of where such technology has been used. The most common approach is to

[122] https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design

[123] Impact Assessment Report accompanying the document "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0295.

124 https://safer.io/about/

[125] "Fighting child sexual abuse online". Available at: https://protectingchildren.google/#fighting-abuse-on-our-own-platform-and-services

[126] "New Technology to Fight Child Exploitation". Available at: https://about.fb.com/news/2018/10/fighting-child-exploitation/

apply tools to detect suspicious patterns in text-based communication and online conversations (Ali et al., 2023).

The use of technology to assist in the process of age verification is a topic that has received much attention. Age verification involves methods and techniques that are deployed in the digital environment to confirm the age of a user for a variety of purposes such as keeping children away from products, services and content that may be potentially harmful to their development such as gambling or adult sites. The BIK+ strategy states that, as a priority, the EC will work with Member States, relevant stakeholders and European standardisation organisations to strengthen age verification methods and will encourage market solutions through a robust framework of certification and interoperability. Despite existing requirements under AVMSD and GDPR, age verification mechanisms remain ineffective in many cases, with minimal requirements such as simply entering a birth date being the norm. The priority, as set out in the BIK+ strategy, is to support methods to prove age in a privacy-preserving and secure manner as referenced in the DSA Regulation and as illustrated by the work of the EU-funded euCONSENT pilot project[127].

4.3. Assistance to victims

Providing support to users when they encounter problems online as well as to those who may become victims of online harm is a further important aspect of online safety infrastructure. A range of services exists at the regional and national supported by state agencies and child welfare organisations targeted at local needs but many of which also benefit from coordination at the national and EU level.

4.3.1. Model National Response

The Model National Response (MNR) promoted by the WeProtect Global Alliance (2016) is a useful framework for considering what is required to support victims of online harm. The MNR focuses on specifically egregious types of harm, namely, child sexual exploitation and abuse. However, the framework is also applicable to other forms of online harm involving the child as a victim or where children are targets of abuse, for instance, in cases of cyberbullying, non-consensual sharing of intimate images, and extortion of where their personal data is misused.

Victim support and empowerment is included as one of the essential pillars required at the national level for effective responses to preventing and tackling children sexual abuse and exploitation[128]. Victim support services in this context refer to five distinct capability areas which are central to building national level responses to support victims and include the following aspects:

- *End-to-end support*: providing planned, integrated and multi-stakeholder support for victims and survivors.
- *Child protection workforce*: ensuring that frontline professionals and those providing support to children are appropriately trained in providing support and in emerging and complex issues such as children's "self-generated" sexual material.
- *Compensation, remedies and complaints arrangements:* provision of measures to allow children and victims accessible support in compensation, legal remedies and complaints procedures.

[127] https://euconsent.eu/

[128] https://www.weprotect.org/model-national-response/

- *Child helpline*: accessible to all children 24/7 offering confidential support and referral mechanisms.
- *Appropriate support services for children and young people*: access to specialised medical and psychological services; and rehabilitation, repatriation and re-socialisation services.

A review of the implementation of the MNR in 2022 found that over two-thirds of surveyed countries (69%, or 29 of 42) have integrated support for victims/survivors. 95% of countries surveyed have a national child helpline in place. Most child helplines are run by NGOs with national governments operating some. Most countries have some of the required aspects of effective remedy or reparations in place. However, there are significant differences between countries, partly due to different legal definitions of the terms (WeProtect Global Alliance, 2022, p. 13).

4.3.2. Helplines

Child helplines are support services for children and young people, and occasionally to parents and professionals, that provide information, advice and assistance on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct such as (cyberbullying or sexting)[129]. Helplines form an integral part of the Safer Internet Centre (SIC) in each country within the Insafe network of 31 national awareness centres. Helplines provide a confidential counselling and support service and offer information, support, guidance and referral for young people as well as adults with responsibility for children. Helplines are designed to be accessible to young people and can increasingly be contacted via a variety of means - telephone, email, web forms, Skype, and online chat services.

Helplines are important in providing listening and emotional support as well as information to assist users with issues they may encounter in their lives. Among the features noted in the literature (Dinh et al., 2016, p. 9) that make child helplines an indispensable resource are the following:

- Anonymity reduces the psychological barrier that prevents many from seeking help;
- Callers have more control over the helping situation since they can terminate the interaction whenever they choose;
- Accepting calls from anyone on any topic may ease the decision to seek help;
- Helplines are staffed by volunteers or professionals, who have proven their effectiveness in helping people in crisis due to their spontaneity, warmth, and authenticity;
- Assistance, in many cases, is available at the callers' convenience, 24 hours a day; and
- Geographical barriers are easily bridged since callers may receive help or support wherever their location.

A review undertaken in 2016 of selected examples in the Insafe network found that helplines are ideally positioned to identify new and emerging risks in online safety (Dinh et al., 2016). Through their close interactions with young people, helplines hear first-hand problems that young people experience online. Collecting this information and using it to develop effective safety responses is now a central part of what helplines do.

Helpline data from the period from July to September 2022[130] reported that there were over 17,500 contacts made to the network reflecting an upward trend in the numbers of people contacting

[129] https://www.betterinternetforkids.eu/en/policy/insafe-inhope

[130] https://www.betterinternetforkids.eu/en/practice/helplines/article?id=6992077

helplines as has been the case for the last three years. Cyberbullying remains the most common reason for contacting a helpline accounting for 14 per cent of all contacts. 6% of contacts were related to sextortion which has been increasing in the volume of calls to Insafe helplines over successive quarters.

The main users of helplines were reported to be young people aged 12 to 18 with this age group representing almost 60 of all contacts made. Helplines also receive contacts from parents/carers and from teachers asking for advice and guidance in supporting the children and young people in their care or who they are working with. During the 2022 reporting period parents accounted for over 20 per cent of those who reach out to helplines.

4.3.3. Hotlines

The creation of hotlines, or cyber tip lines, as a mechanism for members of the general public to report issues they may come across in the course of their internet use was an early response to tackling harmful and illegal content online. In their original conception, hotlines were intended to strengthen policing of the Internet by fostering greater cooperation between law enforcement, industry, civil society and the public (Carr, 2021). The National Center for Missing & Exploited Children (NCMEC) in the United States was one of the first organisations to establish a CyberTipline in 1998 in response to the growing problem of child sexual exploitation online. In 1999, the non-governmental organisation, Childnet International, established the International Hotline Providers in Europe Forum, providing a space for hotlines to meet and exchange information. With support from the European Commission's Daphne programme, the initiative laid the foundation for the establishment of the INHOPE Association in 1999, now representing a network of 50 Hotlines around the world (INHOPE, 2021).

INHOPE is the global network of hotlines dedicated to combating online child sexual abuse material. The network consists of 50 hotlines in 46 countries (as of December 2021) that provide the public with a way to anonymously report illegal content online with a focus on CSAM. Reports are reviewed by trained content analysts who review and classify the reported material. If confirmed illegal, law enforcement agencies are advised, and a notice and takedown order is issued to the relevant hosting provider so that the content is removed from the digital world as rapidly as possible.

In addition to receiving and reviewing reports, hotlines in some jurisdictions also process other categories of illegal content in accordance with local and national laws. For instance, hotline.ie – the Irish national hotline – also receives reports in relation to intimate image abuse (intimate images and videos shared online without the person's consent) and assists victims in securing the takedown of abusive images.

Most hotlines are run by non-profit organizations and collaborate with other stakeholders in the digital ecosystem including law enforcement, the Internet industry and civil society organisations. According to an international review carried out by NCMEC, a large portion (67 per cent) of hotlines are limited to either one or two funding sources. Ninety-six per cent of organizations offer services in addition to the hotline, and 85 per cent accept hotline report types in addition to CSAM (Stroebel & Jeleniewski, 2015).

This section of the study has reviewed some of the main European responses and solutions that have evolved to support young people in their participation in the digital environment. However, as the report of the BIK Policy Map has argued[131], problems such as those linked to social media effects on children's development are complex and require a collective effort on the part of many stakeholders. Effective policy implementation needs a common agenda, shared measurement systems, mutually reinforcing activities, continuous communication, and backbone support to have real impact (Kania

[131] https://www.betterinternetforkids.eu/en/policy/bikmap

and Kramer, 2011). Drawing on the findings of the current study, conclusions and recommendations for policymakers are offered to advance this goal.

5. CONCLUSIONS AND RECOMMENDATIONS

KEY FINDINGS

The main findings of the impact of social media on children's development are summarised. The main concerns raised concern the suitability of social media content and functionality for the age and stage of development of the child.

Risks experienced by children are not always easily separated and frequently coincide, with some children more vulnerable to potential harms than others.

Significant policy, legal and regulatory initiatives have been developed which include provisions for children's protection and empowerment.

A series of recommendations are outlined which address the importance of key concepts including safety by design and age appropriate design; the role of age assurance and digital identity systems; continued policy development in the area of children's privacy; and the importance of sustained research in the form of longitudinal studies and a research observatory function at EU level.

5.1. Impact of social media on children's development

This study provides an overview of the main findings from the research field on the influence of social media on the development of children and young people.

As the study documents, social media are a prominent part of children's everyday lives and are used extensively by children across the EU. Many children start to use social media from an early age, raising concerns about the appropriateness of such platforms for their age and the consequences for their development at a particularly important time in their development.

Through their social media use, children may encounter a diverse range of risks which in this study are discussed under the headings of content, contact, conduct and contract risks, as documented by the CO:RE classification of online risks (Livingstone & Stoilova, 2021). In practice, such risks may not always be so easily separated, and research shows that risks frequently cluster together, intensifying with use and making some more vulnerable than others.

Research shows that children routinely encounter harmful content such as cyberhate, content on eating disorders, sexual content and disinformation which they have not sought and much of which is driven by the algorithmically-based recommendation systems which underpin how content is served to users on social media platforms.

Children are also subject to unwanted contact from adults who are not within their social network or friends list and may pose significant dangers through threats of exploitation and extortion. While children often report confidence in their own ability to manage such risks when making new contacts online, research shows that they are not always aware of the risks they may face or have the skills to detect the dangers posed by strangers contacting them.

Children face particular risks at a formative stage of their development through persistent experiences of bullying in social media environments. Experiences of cyberbullying are commonplace and remain among the most reported topics to European helplines. Online bullying is a complex phenomenon that brings together many of the risks considered in the study – including harassment, sharing images without consent, and increased vulnerability to harmful content. The combination of risks may also be especially impactful for certain children at key formative stages. Research shows that support needs to be targeted to the most vulnerable and that support from family and peers as well as school-based programmes that support social-emotional learning, mentoring, and education on online safety can play a positive role.

Further aspects of risks considered in the study include the many wide-ranging challenges that children face as a result of the commercialised environment of social media. Children encounter issues such as unfair practices, clickbait strategies and hidden marketing practices that contravene their rights and which are not in their best interests. Research shows that children are often ill-prepared with low levels of awareness of commercial practices and lack the critical skills to disaggregate marketing content in the context of their experience of social media.

A cross-cutting theme across all aspects of children's social media use is the topic of mental health and well-being. Research reveals this to be a complex area with inconclusive evidence for either a positive or negative impact on children's health and well-being. For researchers, policymakers and practitioners, probing the outcomes of problematic social media use – even if this is reported by only a minority of children – is an important issue that can provide further insights into specific vulnerabilities and priorities for intervention.

5.2. Supporting children in the digital environment

Supporting children to be safe, protected and empowered when they go online is a cornerstone of EU digital policies. Policies to protect and empower children online take a variety of forms and have been articulated most recently in the Better Internet for Kids (BIK+) strategy adopted in May 2022 and endorsed at a high level in the European Declaration on Digital Rights and Principles for the Digital Decade.

Ensuring a high level of protection for children when they go online is central to the regulatory rules set by the DSA, the Audiovisual Media Services Directive and the GDPR while implementation of the Unfair Commercial Practices Directive also envisages enhanced protections for children as consumers.

The policy and regulatory framework for children's protection and empowerment online within the context of children's rights was also noted in the study. Children's rights underpin the three pillars of the BIK+ strategy and act as the digital arm of the EU Strategy on the Rights of the Child. This is further articulated in policies and programmes that support the acquisition of digital literacy skills and competences and children's active participation in the policymaking process.

Supporting children's online safety and well-being is a multistakeholder activity reflected in the many different programmes and initiatives carried out nationally and at the EU level to raise awareness, lessen the chance of children encountering risks and support children if they become victims of online harm. Research highlights the importance of awareness raising and digital literacy to empower children to have the necessary skills to manage their use of digital services safely and responsibly. In this context, Safer Internet Centres through their respective awareness nodes, helplines, hotlines and youth panels play a crucial role. The high profile of the annual Safer Internet Day campaign internationally is a noteworthy outcome which has resulted from the collective work of Insafe SICs.

Mitigating risks to children is another central part of the policy framework in supporting children's protection and empowerment. Self-regulatory initiatives have a long track record with some important achievements in the course of developing practices in online safety. Technology developments also play a key role in mitigating risks on online platforms and form part of the solutions developed at the industry level, including technologies to support robust age verification. However, a clear shift towards forms of co-regulation is much in evidence as illustrated by the EU Code of conduct on countering illegal hate speech online as well as the Strengthened Code of Practice on Disinformation. The action outlined in the BIK+ strategy to develop a comprehensive EU code of conduct on age-appropriate design operating within the framework of the DSA is a further example of this trend.

5.3. Recommendations

As outlined in the study, the effects of social media on children's development is a large and complex subject area for which there is no single response or solution. While research continues to provide more significant evidence for the impact of digital transformation on children and young people, it is always necessary to have tailored responses to specific issues. However, more research is always required to ensure effective targeting and practical evaluation.

At a more general level, the following recommendations for policy are offered in light of the research outlined in the study.

1. *Safety by design is an important concept that should be endorsed and promoted within regulatory discourse.*
   As the research illustrates, social media is pervasive in the lives of children and young people. In that context, social media environments should be designed to be safe from the outset. Appropriate standards for safety by design can ensure that safety is neither a retrofit nor an afterthought but instead is "baked-in" from the start.

2. *Age-appropriate design has the potential to mainstream the safe, empowered and rights-respecting participation of young people and should be similarly promoted within the policy sphere.*
   As set out in the study, the Commission's support for the development of an EU Code of conduct on age appropriate design is essential to develop this approach further. To ensure its widescale adoption, further work is needed to operationalise the relevant practical processes and monitoring mechanisms associated with such a code.

3. *Continued development of privacy protections for children's data in the social environment is essential.*
   One of the distinctive areas of risk that children encounter relates to the data given off in the course of their social media use. Research shows that children often lack awareness of and the skills to manage these highly complex data ecosystems. The GDPR advances the position that children merit a higher bar of protection due to their evolving capacities. Yet, further development of processes, guidance and standards are needed to ensure best practices in supporting children's privacy in social media environments.

4. *Age assurance and digital identity systems require multistakeholder support if barriers to their implementation are to be overcome and to be effective.*
   Many of the challenges children encounter in using social media arise when they are not appropriately identified as children, thereby meriting higher levels of protection. The lack of adequate and privacy-preserving age assurance mechanisms, as required under GDPR, contributes to this problem. Therefore, all relevant obstacles to developing and rolling out robust age assurance systems should be addressed.

5. *To future-proof policies and to ensure that existing policies and initiatives are appropriate and effective, there is a need for a strong research observatory function at the European level.*
   The study called attention in several critical areas to the lack of or uneven evidence in some key areas regarding children's digital activities. The lack of sufficient comparative research at the

EU level and longitudinal studies on children’s development against the background of digitalisation stand out. Technologies can also quickly outpace policy and regulatory approaches creating new vulnerabilities for children. A higher volume of research on this topic is essential to keep pace with a rapidly evolving digital sphere.

REFERENCES

Ali, S., Razi, A., Kim, S., Alsoubai, A., Ling, C., Choudhury, M. D., Wisniewski, P. J., & Stringhini, G. (2023). *Getting Meta: A Multimodal Approach for Detecting Unsafe Conversations within Instagram Direct Messages of Youth*. *7*. https://doi.org/10.1145/3579608

Andrie, E. K., Sakou, I. I., Tzavela, E. C., Richardson, C., & Tsitsika, A. K. (2021). Adolescents' Online Pornography Exposure and Its Relationship to Sociodemographic and Psychopathological Correlates: A Cross-Sectional Study in Six European Countries. *Children*, *8*(10), Article 10. https://doi.org/10.3390/children8100925

Bada, M., & Clayton, R. (2020). *Online Suicide Games: A Form of Digital Self-harm or A Myth?* arXiv. https://doi.org/10.48550/arXiv.2012.00530

Balaban, D. C., Mucundorfeanu, M., & Mureșan, L. I. (2022). Adolescents' Understanding of the Model of Sponsored Content of Social Media Influencer Instagram Stories. *Media and Communication*, *10*(1), Article 1. https://doi.org/10.17645/mac.v10i1.4652

Ballester-Arnal, R., Giménez-García, C., Gil-Llario, M. D., & Castro-Calvo, J. (2016). Cybersex in the "Net generation": Online sexual activities among Spanish adolescents. *Computers in Human Behavior*, *57*, 261–266. https://doi.org/10.1016/j.chb.2015.12.036

Blaya, C., Audrin, C., & Skrzypiec, G. (2022). School Bullying, Perpetration, and Cyberhate: Overlapping Issues. *Contemporary School Psychology*, *26*(3), 341–349. https://doi.org/10.1007/s40688-020-00318-5

Boer, M., Stevens, G. W. J. M., Finkenauer, C., de Looze, M. E., & van den Eijnden, R. J. J. M. (2021). Social media use intensity, social media use problems, and mental health among adolescents: Investigating directionality and mediating processes. *Computers in Human Behavior*, *116*, 106645. https://doi.org/10.1016/j.chb.2020.106645

Brennan, C., Saraiva, S., Mitchell, E., Melia, R., Campbell, L., King, N., & House, A. (2022). Self-harm and suicidal content online, harmful or helpful? A systematic review of the recent evidence. *Journal of Public Mental Health*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JPMH-09-2021-0118

Burnette, C. B., Kwitowski, M. A., & Mazzeo, S. E. (2017). "I don't need people to tell me I'm pretty on social media:" A qualitative study of social media and body image in early adolescent girls. *Body Image*, *23*, 114–125. https://doi.org/10.1016/j.bodyim.2017.09.001

C3P. (2022). *An Analysis Of Financial Sextortion Victim Posts Published On R/Sextortion*. Canadian Centre for Child Protection. https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

Carr, J. (2021). Online Child Safety. In P. Cornish (Ed.), *The Oxford Handbook of Cyber Security* (pp. 377–394). Oxford University Press.

CC-Driver. (2022). *2022 Research Report*. https://www.ccdriver-h2020.com/_files/ugd/0ef83d_622d9f44dd7345cd80314333a92d74f1.pdf

Cernikova, M., Dedkova, L., & Smahel, D. (2018). Youth interaction with online strangers: Experiences and reactions to unknown people on the Internet. *Information, Communication & Society*, *21*(1), 94–110. https://doi.org/10.1080/1369118X.2016.1261169

Chiu, J., & Quayle, E. (2022). Understanding online grooming: An interpretative phenomenological analysis of adolescents' offline meetings with adult perpetrators. *Child Abuse & Neglect*, *128*, 105600. https://doi.org/10.1016/j.chiabu.2022.105600

Cioban, S., Lazăr, A. R., Bacter, C., & Hatos, A. (2021). Adolescent Deviance and Cyber-Deviance. A Systematic Literature Review. *Frontiers in Psychology*, *12*, 748006. https://doi.org/10.3389/fpsyg.2021.748006

Corbu, N., Oprea, D.-A., & Frunzaru, V. (2022). Romanian adolescents, fake news, and the third-person effect: A cross-sectional study. *Journal of Children and Media*, *16*(3), 387–405. https://doi.org/10.1080/17482798.2021.1992460

Coulter, N. (2021). Child Studies Meets Digital Media: Rethinking the Paradigms. In L. Green, D. Hoilloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.), *The Routledge Companion to Digital Media and Children* (pp. 19–27). Routledge.

Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., Harel-Fisch, Y., Malinowska-Cieślik, M., Gaspar de Matos, M., Cosma, A., Van den Eijnden, R., Vieno, A., Elgar, F. J., Molcho, M., Bjereld, Y., & Pickett, W. (2020). Social Media Use and Cyber-Bullying: A Cross-National Analysis of Young People in 42 Countries. *Journal of Adolescent Health*, *66*(6), S100–S108. https://doi.org/10.1016/j.jadohealth.2020.03.006

Daems, K., De Pelsmacker, P., & Moons, I. (2019). The effect of ad integration and interactivity on young teenagers' memory, brand attitude and personal data sharing. *Computers in Human Behavior*, *99*, 245–259. https://doi.org/10.1016/j.chb.2019.05.031

Dawson, K., Nic Gabhainn, S., Willis, M., & MacNeela, P. (2022). Development of a Measure to Assess What Young Heterosexual Adults Say They Learn About Sex from Pornography. *Archives of Sexual Behavior*, *51*(2), 1257–1269. https://doi.org/10.1007/s10508-021-02059-9

De Pauw, P., De Wolf, R., Hudders, L., & Cauberghe, V. (2018). From persuasive messages to tactics: Exploring children's knowledge and judgement of new advertising formats. *New Media & Society*, *20*(7), 2604–2628. https://doi.org/10.1177/1461444817728425

De Pauw, P., Hudders, L., & Cauberghe, V. (2018). Disclosing brand placement to young children. *International Journal of Advertising*, *37*(4), 508–525. https://doi.org/10.1080/02650487.2017.1335040

Deslandes, S. F., & Coutinho, T. (2020). The intensive use of the internet by children and adolescents in the context of COVID-19 and the risks for self-inflicted violence. *Ciência & Saúde Coletiva*, *25*, 2479–2486. https://doi.org/10.1590/1413-81232020256.1.11472020

Dias, P., Marôpo, L., Delgado, C., Rodrigues, M. D. R., Torres, J., & Ferreira, E. (2022). *'I'm not sure how they make money': How tweens and teenagers perceive the business of social media, influencers and brands*. https://doi.org/10.5281/ZENODO.6702887

Dinh, T., Farrugia, L., O'Neill, B., Vandoninck, S., & Velicu, A. (2016). *Insafe Helplines: Operations, effectiveness and emerging issues for internet safety helplines*. https://www.betterinternetforkids.eu/documents/167024/507884/Helpline+Fund+Report+-+Final/4cf8f03a-3a48-4365-af76-f03e01cb505d

Doyle, C., Douglas, E., & O'Reilly, G. (2021). The outcomes of sexting for children and adolescents: A systematic review of the literature. *Journal of Adolescence*, *92*, 86–113. https://doi.org/10.1016/j.adolescence.2021.08.009

ECPAT International. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. ECPAT International. http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf

ENABLE. (2015). *Bullying in Schools A summary of research and anti-bullying initiatives*. http://enable.eun.org/c/document_library/get_file?uuid=1b5a1cee-4e04-4cc6-8faa-f473bf348595&groupId=4467490

European Commission. (2018). *Fake news and disinformation online*. Publications Office. https://data.europa.eu/doi/10.2759/559993

European Commission. Directorate General for Health and Food Safety., ECORYS., University of Helsinki., & Kantar Public. (2021). *Study on the exposure of children to linear, non-linear and online marketing of foods high in fat, salt or sugar: Final report*. Publications Office. https://data.europa.eu/doi/10.2875/928620

European Union Agency for Law Enforcement Cooperation. (2021). *IOCTA 2021: Internet organised crime threat assessment 2021*. Publications Office. https://data.europa.eu/doi/10.2813/113799

Europol & EC3. (2017). *Online sexual coercion and extortion as a form of crime affecting chidren*. https://www.europol.europa.eu/cms/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Feijoo, B., & Sádaba, C. (2022). When Ads Become Invisible: Minors' Advertising Literacy While Using Mobile Phones. *Media and Communication*, *10*(1), Article 1. https://doi.org/10.17645/mac.v10i1.4720

Fındık, O., & Çeri, V. (2019). Online challenge related self harm in children and adolescents; Two case reports. *Anatolian Journal of Psychiatry*, *20*(0), 1. https://doi.org/10.5455/apd.39071

Folkvord, F., Bevelander, K. E., Rozendaal, E., & Hermans, R. (2019). Children's bonding with popular YouTube vloggers and their attitudes toward brand and product endorsements in vlogs: An explorative study. *Young Consumers*, *20*(2). https://doi.org/10.1108/YC-12-2018-0896

Frissen, T. (2021). Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults. *Computers in Human Behavior*, *114*, 106549. https://doi.org/10.1016/j.chb.2020.106549

Gámez-Guadix, M., Almendros, C., Calvete, E., & De Santisteban, P. (2018). Persuasion strategies and sexual solicitations and interactions in online sexual grooming of adolescents: Modeling direct and indirect pathways. *Journal of Adolescence*, *63*(1), 11–18. https://doi.org/10.1016/j.adolescence.2017.12.002

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. *Policy and Internet*, *12*(1), 6–19. https://doi.org/10.1002/poi3.236

Gold, M. (2021). Cybermobbing im Primarschulbereich. *Medienimpulse*, *Bd. 59 Nr. 1*, 51 Seiten Seiten. https://doi.org/10.21243/MI-01-21-07

Görzig, A., Blaya, C., Bedrosova, M., Audrin, C., & Machackova, H. (2023). The Amplification of Cyberhate Victimisation by Discrimination and Low Life Satisfaction: Can Supportive Environments Mitigate the Risks? *The Journal of Early Adolescence*, *43*(1), 5–36. https://doi.org/10.1177/02724316221078826

Green, L., Lumby, C., McKee, A., & Ólafsson, K. (2020). National Contexts for the Risk of Harm Being Done to Children by Access to Online Sexual Content. In L. Tsaliki & D. Chronaki (Eds.), *Discourses of Anxiety over Childhood and Youth across Cultures* (pp. 261–278). Springer International Publishing. https://doi.org/10.1007/978-3-030-46436-3_11

Greene-Colozzi, E. A., Winters, G. M., Blasko, B., & Jeglic, E. L. (2020). Experiences and Perceptions of Online Sexual Solicitation and Grooming of Minors: A Retrospective Report. *Journal of Child Sexual Abuse*, *29*(7), 836–854. https://doi.org/10.1080/10538712.2020.1801938

Groenestein, E., Baas, N., van Deursen, A. J. A. M., & de Jong, M. D. T. (2018). Strategies and cues adolescents use to assess the age of an online stranger. *Information, Communication & Society*, *21*(8), 1168–1185. https://doi.org/10.1080/1369118X.2017.1309443

Hajnal, Á. (2021). Cyberbullying Prevention: Which Design Features Foster the Effectiveness of School-Based Programs? : A Meta-Analytic Approach. *Intersections*, *7*(1), 40–58. https://doi.org/10.17356/ieejsp.v7i1.648

Harvey, P. (2020). Let's Talk About Porn: The Perceived Effect of Online Mainstream Pornography on LGBTQ Youth. In D. N. Farris, D. R. Compton, & A. P. Herrera (Eds.), *Gender, Sexuality and Race in the Digital Age* (pp. 31–52). Springer International Publishing. https://doi.org/10.1007/978-3-030-29855-5_3

Havighurst, R. J. (1972). *Developmental Tasks and Education,* (3rd edition). Addison-Wesley Longman Ltd.

Helsper, E. J., & Smahel, D. (2020). Excessive internet use by young Europeans: Psychological vulnerability and digital literacy? *Information, Communication & Society*, *23*(9), 1255–1273. https://doi.org/10.1080/1369118X.2018.1563203

Hinduja, S. (2022, May 11). The Metaverse: Opportunities, Risks, and Harms. *Cyberbullying Research Center*. https://cyberbullying.org/metaverse

Hinduja, S., & Patchin, J. W. (2021). *Cyberbullying: Identification, Prevention, and Response*.

Hof, S. van der, Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The Child's Right to Protection against Economic Exploitation in the Digital World. *The International Journal of Children's Rights*, *28*(4), 833–859. https://doi.org/10.1163/15718182-28040003

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Who was first on Facebook? Determinants of early adoption among adolescents. *New Media & Society*, *18*(10), 2340–2358. https://doi.org/10.1177/1461444815584592

Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *Body Image*, *17*, 100–110. https://doi.org/10.1016/j.bodyim.2016.02.008

Holvoet, S., Jans, S. D., Wolf, R. D., Hudders, L., & Herrewijn, L. (2022). Exploring Teenagers' Folk Theories and Coping Strategies Regarding Commercial Data Collection and Personalized Advertising. *Media and Communication*, *10*(1), Article 1. https://doi.org/10.17645/mac.v10i1.4704

Hornor, G. (2020). Child and Adolescent Pornography Exposure. *Journal of Pediatric Health Care*, *34*(2), 191–199. https://doi.org/10.1016/j.pedhc.2019.10.001

Howard, P. N., Neudert, L.-M., Prakash, N., & Vosloo, S. (2021). *Digital misinformation / disinformation and children*. UNICEF Office of Global Insight and Policy. https://www.ictworks.org/wp-content/uploads/2021/10/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf

ICMEC. (2022, March 24). The new "Stranger Danger": Tactics used in the online grooming of children. *Medium*. https://icmec.medium.com/the-new-stranger-danger-tactics-used-in-the-online-grooming-of-children-f2e42bd81734

INHOPE. (2021). *INHOPE Annual Report 2021*. INHOPE. https://www.inhope.org/EN/articles/annual-reports?locale=en

Internet Watch Foundation. (2021). *The Annual Report 2021*. Internet Watch Foundation. https://annualreport2021.iwf.org.uk/

James, A., & Prout, A. (1997). *Constructing and reconstructing childhood: Contemporary issues in the sociological study of childhood* (2nd ed., p. xvii,260p.). Falmer.

Joint Research Centre. (2021). *How children (10-18) experienced online risks during the Covid-19 lockdown: Spring 2020 : key findings from surveying families in 11 European countries.* Publications Office. https://data.europa.eu/doi/10.2760/562534

Kandola, A., Owen, N., Dunstan, D. W., & Hallgren, M. (2021). Prospective relationships of adolescents' screen-based sedentary behaviour with depressive symptoms: The Millennium Cohort Study. *Psychological Medicine*, 1–9. https://doi.org/10.1017/S0033291721000258

Kania, J., & Kramer, M. (2011). Collective Impact. *Stanford Social Innovation Review*, *Winter*, 36–41. https://ssir.org/articles/entry/collective_impact

Kapus, K., Nyulas, R., Nemeskeri, Z., Zadori, I., Muity, G., Kiss, J., Feher, A., Fejes, E., Tibold, A., & Feher, G. (2021). Prevalence and Risk Factors of Internet Addiction among Hungarian High School Students. *International Journal of Environmental Research and Public Health*, *18*(13), 6989. https://doi.org/10.3390/ijerph18136989

Kardefelt-Winther, D. (2017). *How does the time children spend using digital technology impact their mental well-being , social relationships and physical activity? An evidence-focused literature review* (Issue December). https://www.unicef-irc.org/publications/925/

Kashy-Rosenbaum, G., & Aizenkot, D. (2020). Exposure to cyberbullying in WhatsApp classmates' groups and classroom climate as predictors of students' sense of belonging: A multi-level analysis of elementary, middle and high schools. *Children and Youth Services Review*, *108*, 104614. https://doi.org/10.1016/j.childyouth.2019.104614

Keipi, T., Räsänen, P., Oksanen, A., Hawdon, J., & Näsi, M. (2018). Exposure to online hate material and subjective well-being: A comparative study of American and Finnish youth. *Online Information Review*, *42*(1), 2–15. https://doi.org/10.1108/OIR-05-2016-0133

Lebedíková, M., Mýlek, V., Subrahmanyam, K., & Šmahel, D. (2022). Exposure to Sexually Explicit Materials and Feelings after Exposure among Adolescents in Nine European Countries: The Role of Individual Factors and Social Characteristics. *Archives of Sexual Behavior*. https://doi.org/10.1007/s10508-022-02401-9

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report. EC Safer Internet Plus Programme Deliverable D6.5*. EU Kids Online.

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe* [Monograph]. EU Kids Online, The London School of Economics and Political Science. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. *CO:RE Short Report Series on Key Topics*. https://doi.org/10.21241/SSOAR.71817

Lombana-Bermudez, A., Cortesi, S., Fieseler, C., Gasser, U., Hasse, A., Newlands, G., & Wu, S. (2020). *Youth and the Digital Economy: Exploring Youth Practices, Motivations, Skills, Pathways, and Value Creation* (SSRN Scholarly Paper No. 3622572). https://doi.org/10.2139/ssrn.3622572

Lozano-Blasco, R., & Cortés-Pascual, A. (2020). Problematic Internet uses and depression in adolescents: A meta-analysis. *Comunicar*, *28*(63), 109–120. https://doi.org/10.3916/C63-2020-10

Lukács, A. (2021). Predictors of Severe Problematic Internet Use in Adolescent Students. *Contemporary Educational Technology*, *13*(4), ep315. https://doi.org/10.30935/cedtech/10989

Machackova, H., Blaya, C., Bedrosova, M., Smahel, D., & Staksrud, E. (2020). *Children's experiences with cyberhate*. *EU Kids Online*. https://doi.org/10.21953/lse.zenkg9xw6pua

Mancheva, R. (2020). The Cyberbullying Phenomenon – Contemporary Narrative Form of Aggression in the School. *Postmodernism Problems*, *10*(1), 41–61. https://doi.org/10.46324/PMP2001041

Manning, M. L. (2002). Havighurst's Developmental Tasks, Young Adolescents, and Diversity. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, *76*(2), 75–78. https://doi.org/10.1080/00098650209604953

Marwick, A., Clancy, B., & Furl, K. (2022). Far-Right Online Radicalization: A Review of the Literature. *The Bulletin of Technology & Public Life*. https://citap.pubpub.org/pub/jq7l6jny/release/1

Massey, K., Burns, J., & Franz, A. (2021). Young People, Sexuality and the Age of Pornography. *Sexuality & Culture*, *25*(1), 318–336. https://doi.org/10.1007/s12119-020-09771-z

Matamoros-Fernández, A., Rodriguez, A., & Wikström, P. (2022). Humor That Harms? Examining Racist Audio-Visual Memetic Media on TikTok During Covid-19. *Media and Communication*, *10*(2), 180–191. https://doi.org/10.17645/mac.v10i2.5154

McCay-Peet, L., & Quan-Haase, A. (2017). What is social media and what questions can social media research help us answer. In *The SAGE handbook of social media research methods* (pp. 13–26). SAGE Publications Ltd London.

Meléndez-Illanes, L., González-Díaz, C., & Álvarez-Dardet, C. (2022). Advertising of foods and beverages in social media aimed at children: High exposure and low control. *BMC Public Health*, *22*(1), 1795. https://doi.org/10.1186/s12889-022-14196-4

Memon, A. M., Sharma, S. G., Mohite, S. S., & Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian Journal of Psychiatry*, *60*(4), 384–392. https://doi.org/10.4103/psychiatry.IndianJPsychiatry_414_17

Mikuška, J., Smahel, D., Dedkova, L., Staksrud, E., Mascheroni, G., & Milosevic, T. (2020). Social relational factors of excessive internet use in four European countries. *International Journal of Public Health*, *65*(8), 1289–1297. https://doi.org/10.1007/s00038-020-01484-2

Mori, C., Park, J., Temple, J. R., & Madigan, S. (2022). Are Youth Sexting Rates Still on the Rise? A Meta-analytic Update. *Journal of Adolescent Health*, *70*(4), 531–539. https://doi.org/10.1016/j.jadohealth.2021.10.026

Nash, V., Adler, J. R., Horvath, M. A. H., Livingstone, S., Marston, C., Owen, G., & Wright, J. (2015). *Identifying the routes by which children view pornography online: Implications for future policy-makers seeking to limit viewing* [Monograph]. Department for Culture, Media and Sport. https://www.gov.uk/

National Literacy Trust. (2018). *Fake news and critical literacy. The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools*. https://cdn.literacytrust.org.uk/media/documents/Fake_news_and_critical_literacy_-_final_report.pdf

Nutley, S., & Thorell, L. (2022). *Digital media and mental health problems in children and adolescents: A research overview - English summary* [Text]. Swedish Media Council. https://www.statensmedierad.se/rapporter-och-analyser/material-rapporter-och-analyser/2022/digital-media-and-mental-health-problems-in-children-and-adolescents-a-research-overview---english-summary

Obar, J. A., & Wildman, S. S. (2015). *Social Media Definition and the Governance Challenge—An Introduction to the Special Issue* (SSRN Scholarly Paper No. 2663153). https://doi.org/10.2139/ssrn.2663153

O'Connor, C. (2021). *Hatescape: An In-Depth Analysis of Extremism and Hate Speech on TikTok*. Institute for Strategic Dialogue.

OECD. (2018). *Children & Young People's Mental Health in the Digital Age*. OECD.

OECD. (2021). *Children in the digital environment: Revised typology of risks* (OECD Digital Economy Papers No. 302; OECD Digital Economy Papers, Vol. 302). https://doi.org/10.1787/9b8f222e-en

Ofcom. (2022). *Children and parents: Media use and attitudes report 2022*. Ofcom. https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2022/interactive

Office of the SRSG on Violence against Children. (2016). *Ending the Torment: Tackling Bullying from the Schoolyard to Cyberspace*. United Nations. https://doi.org/10.18356/27a397d3-en

Odgers, C., Allen, N. B., Pfeifer, J. H., Dahl, R., Nesi, J., Schueller, S., Williams, J. L. (2022). *Engaging, safe, and evidence-based: What science tells us about how to promote positive development and decrease risk in online spaces*. https://doi.org/10.31234/osf.io/rvn8q

Ojeda, M., del-Rey, R., Walrave, M., & Vandebosch, H. (2020). Sexting in adolescents: Prevalence and behaviours. *Comunicar*, *28*(64), 9–19. https://doi.org/10.3916/C64-2020-01

O'Neill, B., Dinh, T., & Lalor, K. (2021). *Digital Voices: Progressing children's right to be heard through social and digital media* (p. 114). Ombudsman for Children's Office. https://www.oco.ie/app/uploads/2021/09/Digital-Voices-Progressing-Childrens-right-to-be-heard-through-social-and-digital-media.pdf

Österreichisches Institut für angewandte Telekommunikation. (2018). *Kinder im Visier von Influencer-Marketing: Auf YouTube, Instagram und Snapchat*. Kammer für Arbeiter und Angestellte für Wien.

Paat, Y.-F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18–40. https://doi.org/10.1080/15332985.2020.1845281

Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse*, *32*(1), 30–54. https://doi.org/10.1177/1079063218800469

Paxton, S. J., McLean, S. A., & Rodgers, R. F. (2022). "My critical filter buffers your app filter": Social media literacy as a protective factor for body image. *Body Image*, *40*, 158–164. https://doi.org/10.1016/j.bodyim.2021.12.009

Peter, J., & Valkenburg, P. M. (2016). Adolescents and Pornography: A Review of 20 Years of Research. *Journal of Sex Research*, *53*(4–5). https://doi.org/10.1080/00224499.2016.1143441

Pew Research Centre. (2018). *Many Turn to YouTube for Children's Content, News, How-To Lessons* (p. 28). Pew Research Centre. https://www.pewresearch.org/internet/2018/11/07/many-turn-to-youtube-for-childrens-content-news-how-to-lessons/

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Phippen, A., & Bond, E. (2020). Momo Week: A Perfect Social Media Storm and a Breakdown in Stakeholder Sanity? In A. Phippen & E. Bond (Eds.), *Organisational Responses to Social Media Storms: An Applied Analysis of Modern Challenges* (pp. 27–48). Springer International Publishing. https://doi.org/10.1007/978-3-030-49977-8_3

Pothong, K., & Livingstone, S. (2021, September 29). UK "Secure by Design" vs Australian "Safety by Design". *Parenting for a Digital Future*. https://blogs.lse.ac.uk/parenting4digitalfuture/2021/09/29/secure-by-design/

Quayle, E. (2022). Self-produced images, sexting, coercion and children's rights. *ERA Forum*. https://doi.org/10.1007/s12027-022-00714-9

Reichelmann, A., Hawdon, J., Costello, M., Ryan, J., Blaya, C., Llorent, V., Oksanen, A., Räsänen, P., & Zych, I. (2021). Hate Knows No Boundaries: Online Hate in Six Nations. *Deviant Behavior*, *42*(9), 1100–1111. https://doi.org/10.1080/01639625.2020.1722337

Reinemann, C., Nienierza, A., Fawzi, N., Riesmeyer, C., & Neumann, K. (2019). *Jugend - Medien - Extremismus: Wo Jugendliche mit Extremismus in Kontakt kommen und wie sie ihn erkennen*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-23729-5

Rounsefell, K., Gibson, S., McLean, S., Blair, M., Molenaar, A., Brennan, L., Truby, H., & McCaffrey, T. A. (2020). Social media, body image and food choices in healthy young adults: A mixed methods systematic review. *Nutrition & Dietetics*, *77*(1), 19–40. https://doi.org/10.1111/1747-0080.12581

Rozendaal, E., & Figner, B. (2020). Effectiveness of a School-Based Intervention to Empower Children to Cope With Advertising. *Journal of Media Psychology*, *32*(3), 107–118. https://doi.org/10.1027/1864-1105/a000262

Rummo, P. E., Cassidy, O., Wells, I., Coffino, J. A., & Bragg, M. A. (2020). Examining the Relationship between Youth-Targeted Food Marketing Expenditures and the Demographics of Social Media Followers. *International Journal of Environmental Research and Public Health*, *17*(5), 1631. https://doi.org/10.3390/ijerph17051631

SaferInternet.at. (2017). *Aktuelle Studie zum Thema „Gerüchte im Netz": Jugendliche verunsichert durch Fake News*. Saferinternet.At. https://www.saferinternet.at/news-detail/aktuelle-studie-zum-thema-geruechte-im-netz-jugendliche-verunsichert-durch-fake-news/

Savimäki, T., Kaakinen, M., Räsänen, P., & Oksanen, A. (2020). Disquieted by Online Hate: Negative Experiences of Finnish Adolescents and Young Adults. *European Journal on Criminal Policy and Research*, *26*(1), 23–37. https://doi.org/10.1007/s10610-018-9393-2

Scully, M., Swords, L., & Nixon, E. (2020). Social comparisons on social media: Online appearance-related activity and body dissatisfaction in adolescent girls. *Irish Journal of Psychological Medicine*, 1–12. https://doi.org/10.1017/ipm.2020.93

Sedgwick, R., Epstein, S., Dutta, R., & Ougrin, D. (2019). Social media, internet use and suicide attempts in adolescents. *Current Opinion in Psychiatry*, *32*(6), 534–541. https://doi.org/10.1097/YCO.0000000000000547

Setty, E. (2021). Sex and consent in contemporary youth sexual culture: The 'ideals' and the 'realities'. *Sex Education*, *21*(3), 331–346. https://doi.org/10.1080/14681811.2020.1802242

Singh, S. (2019). *An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User-Generated Content* (p. 42). New America. https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/

Sklenarova, H., Schulz, A., Schuhmann, P., Osterheider, M., & Neutze, J. (2018). Online sexual solicitation by adults and peers—Results from a population based German sample. *Child Abuse & Neglect*, *76*, 225–236. https://doi.org/10.1016/j.chiabu.2017.11.005

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

Smahel, D., & Wright, M. F. (2014). *The meaning of online problematic situations for children. Results of qualitative cross-cultural investigation in nine European countries*. EU Kids Online. http://eprints.lse.ac.uk/56972/1/EU_Kids_Online_Report_Online_Problematic_Situations_for_Children_June2014.pdf

Smith, P. K., & Steffgen, G. (2013). *Cyberbullying through the New Media: Findings from an international network* (p. 283). Psychology Press. https://play.google.com/books?id=FUtKAgAAQBAJ

Staksrud, E. (2020). Sexual Images, Risk, and Perception among Youth: A Nordic Example. In *The Routledge Companion to Digital Media and Children*. Routledge.

Steer, O. L., Betts, L. R., Baguley, T., & Binder, J. F. (2020). “I feel like everyone does it”- adolescents’ perceptions and awareness of the association between humour, banter, and cyberbullying. *Computers in Human Behavior*, *108*, 106297. https://doi.org/10.1016/j.chb.2020.106297

Stoilova, M., Edwards, C., Kostyrka-Allchorne, K., Livingstone, S., & Sonuga-Barke, E. (2021). *The impact of digital experiences on adolescents with mental health vulnerabilities* (p. 88). London School of Economics and Political Science and King’s College London. http://eprints.lse.ac.uk/112931/1/Stoilova_the_impact_of_digital_experiences_on_adolescents_published.pdf

Stoilova, M., Livingstone, S., & Khazbak, R. (2021). *Investigating Risks and Opportunities for Children in a Digital World: A Rapid Review of the Evidence on Children’s Internet Use and Outcomes* (Innocenti Discussion Papers) [Innocenti Discussion Papers]. https://doi.org/10.18356/25211110-2020-03

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children’s understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, *24*(4), 557–575. https://doi.org/10.1080/1369118X.2019.1657164

Stroebel, M., & Jeleniewski, S. (2015). *Global Research Project: A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges*.

Svedin, C. G., Donevan, M., Bladh, M., Priebe, G., Fredlund, C., & Jonsson, L. S. (2022). Associations between adolescents watching pornography and poor mental health in three Swedish surveys. *European Child & Adolescent Psychiatry*. https://doi.org/10.1007/s00787-022-01992-x

Symons, K., Vanwesenbeeck, I., Walrave, M., Van Ouytsel, J., & Ponnet, K. (2020). Parents’ Concerns Over Internet Use, Their Engagement in Interaction Restrictions, and Adolescents’ Behavior on Social Networking Sites. *Youth & Society*, *52*(8), 1569–1581. https://doi.org/10.1177/0044118X19834769

Thorhauge, A. M., & Bonitz, M. (2020). Friends, lovers, risk and intimacy: Risk-taking as a socially meaningful practice. *MedieKultur: Journal of Media and Communication Research*, *36*(67), 037–054. https://doi.org/10.7146/mediekultur.v36i67.116141

Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, *13*(3), 415–432. https://doi.org/10.1002/poi3.250

UK SIC. (2016, June 2). Creating a Better Internet for All. *UK Safer Internet Centre*. https://saferinternet.org.uk/blog/creating-a-better-internet-for-all-report-launched

van den Eijnden, R. J. J. M., Geurts, S. M., ter Bogt, T. F. M., van der Rijst, V. G., & Koning, I. M. (2021). Social Media Use and Adolescents’ Sleep: A Longitudinal Study on the Protective Role of Parental Rules Regarding Internet Use before Sleep. *International Journal of Environmental Research and Public Health*, *18*(3), 1346. https://doi.org/10.3390/ijerph18031346

Van Der Hof, S. (2021, November 17). Age assurance and age appropriate design: What is required? *Parenting for a Digital Future*. https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Van Ouytsel, J., Punyanunt-Carter, N. M., Walrave, M., & Ponnet, K. (2020). Sexting within young adults’ dating and romantic relationships. *Current Opinion in Psychology*, *36*, 55–59. https://doi.org/10.1016/j.copsyc.2020.04.007

Van Ouytsel, J., Walrave, M., De Marez, L., Vanhaelewyn, B., & Ponnet, K. (2020). A first investigation into gender minority adolescents’ sexting experiences. *Journal of Adolescence*, *84*(1), 213–218. https://doi.org/10.1016/j.adolescence.2020.09.007

Van Reijmersdal, E. A., Rozendaal, E., Hudders, L., Vanwesenbeeck, I., Cauberghe, V., & Van Berlo, Z. M. C. (2020). Effects of Disclosing Influencer Marketing in Videos: An Eye Tracking Study among Children in Early Adolescence. *Journal of Interactive Marketing*, *49*(1), 94–106. https://doi.org/10.1016/j.intmar.2019.09.001

Vanwesenbeeck, I., Hudders, L., & Ponnet, K. (2020). Understanding the YouTube Generation: How Preschoolers Process Television and YouTube Advertising. *Cyberpsychology, Behavior, and Social Networking*, *23*(6), 426–432. https://doi.org/10.1089/cyber.2019.0488

Varadan, S. (2019). The Principle of Evolving Capacities under the UN Convention on the Rights of the Child. *The International Journal of Children's Rights*, *27*(2), 306–338. https://doi.org/10.1163/15718182-02702006

Verdoodt, V. (2020). *Children's Rights and Commercial Communication in the Digital Era*. Intersentia. KU Leuven Centre for IT & IP Law Series. https://intersentia.com/en/children-s-rights-and-commercial-communication-in-the-digital-era.html

Vissenberg, J., & d'Haenens, L. (2020). 'I sometimes have doubts about the news on Facebook': Adolescents' encounters with fake news on the internet. *Jurnal Komunikasi Indonesia*, *9*(2). https://doi.org/10.7454/jki.v9i2.12764

Vogels, E. a, Gelles-Watnick, R., & Massarat, N. (2022). *Teens, Social Media and Technology 2022*. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

Wachs, S., Mazzone, A., Milosevic, T., Wright, M. F., Blaya, C., Gámez-Guadix, M., & O'Higgins Norman, J. (2021). Online correlates of cyberhate involvement among young people from ten European countries: An application of the Routine Activity and Problem Behaviour Theory. *Computers in Human Behavior*, *123*, 106872. https://doi.org/10.1016/j.chb.2021.106872

Weimann, G., & Masri, N. (2020). Research Note: Spreading Hate on TikTok. *Studies in Conflict & Terrorism*, *0*(0), 1–14. https://doi.org/10.1080/1057610X.2020.1780027

WeProtect Global Alliance. (2016). *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*. WeProtect Global Alliance. (2022). *Framing the Future: How the Model National Response framework is supporting national efforts to end child sexual exploitation and abuse online*. We Protect Global Alliance. https://www.weprotect.org/framing-the-future/#full-report

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, *62*(1), 72–79. https://doi.org/10.1016/j.jadohealth.2017.08.014

York, L., MacKenzie, A., & Purdy, N. (2021). Attitudes to sexting amongst post-primary pupils in Northern Ireland: A liberal feminist approach. *Gender and Education*, *33*(8), 999–1016. https://doi.org/10.1080/09540253.2021.1884196

Zarouali, B., Verdoodt, V., Walrave, M., Poels, K., Ponnet, K., & Lievens, E. (2020). Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: Implications for regulation. *Young Consumers*, *21*(3), 351–367. https://doi.org/10.1108/YC-04-2020-1122

This study examines research on the impact of pervasive social media use on children's and young people's development. Acknowledging the many benefits children gain from being connected through social media, this study focuses on problematic use and the potential harm that may arise from content, contact, conduct and contract risks. Solutions are considered in light of EU policy and regulatory developments with particular reference to ensuring that children are protected, safe and empowered when they go online.

PE 733.109
IP/B/CULT/IC/2022-102

Print ISBN 978-92-848-0179-4 | doi:10.2861/ 043634 | QA-04-23-103-EN-C
PDF ISBN 978-92-848-0178-7 | doi:10.2861/ 141134 | QA-04-23-103-EN-N