European Institute for Gender Equality

FROM LIVED REALITY TO POLICY ACTION:

Combating cyber violence against girls in the EU

An EU Agency

European Institute for Gender Equality

European Institute for Gender Equality

The European Institute for Gender Equality (EIGE) produces independent research and shares best practice to promote gender equality and eliminate discrimination based on gender. As the EU agency for gender equality, we help people achieve equal opportunities so everyone can thrive, independent of their gender and background.

We combine research, data and tools to help policymakers design measures that are inclusive and transformative and promote gender equality in all areas of life. We communicate our expertise and research effectively. We work closely with partners to raise awareness. We do this at the EU and national levels and with EU candidate and potential candidate countries.

Cite this publication:

EIGE, *From Lived Reality to Policy Action: Combating cyber violence against girls in the EU*, Publications Office of the European Union, Luxembourg, 2026.

Luxembourg: Publications Office of the European Union, 2026

PDF ISBN 978-92-9486-350-8 doi:10.2839/5514733 MH-01-26-045-EN-N

European Institute for Gender Equality
Gedimino pr. 16
LT-01103 Vilnius
LITHUANIA

Tel. +370 52157400
Internet: https://eige.europa.eu
Email: eige.sec@eige.europa.eu

Follow us

Contents

List of figures

List of tables

List of boxes

Contributors

This report is based on a study on cyber violence affecting girls commissioned by the European Institute for Gender Equality that was carried out by the Istituto per la Ricerca Sociale (IRS) in partnership with the Mediterranean Institute of Gender Studies (MIGS). The contributors from IRS were Prof. Dr Flavia Pesce, Elena Ferrari, Nicola Orlando, Maria Juliana Charry Camargo and Francesco Sanguineti, and those from MIGS were Susana Pavlou, Christina Kaili, Stalo Lesta and Maria Angeli. The following national researchers oversaw focus group discussions: Prof. Dr. Glowacz Fabienne, Maria Angeli, Dr. Anu Laas, Bianca Grafe, Dr. Elaine Byrnes, Dr. Lucia Beltramini, Agata Teutsch, Camelia Florina Proca, Virginia Gil Portolés, and Dr. Runa Baianstovu.

Additional contributions were made by experts from the Gender Equality Unit at the Directorate-General for Justice and Consumers. Dr Leonie Tanczer, Associate Professor in International Security and Emerging Technologies, University College London, provided inputs to an early draft. Sincere thanks are given to the participants of EIGE's consultation meeting, held remotely on 12 November 2025, for their feedback on draft policy recommendations. The participants included Elizabeth Ávila González, Prof. Kim Barker, Stephanie Futter-Orel, Inès Girard, Prof. Olga Jurasz, Zuzanna Kowalska, Marlene Matos, Dr. Janine Mc Ginn, Eva O'Byrne, Adèle Philtjens, Lisa Robinson, Silvia Semenzin, Sara Sighinolfi, Sylwia Spurek and Dr. Leonie Tanczer. Feedback on the draft policy recommendations was also received from Thomas Yaqoubi and

Abbreviations

AI	artificial intelligence
DSA	Digital Services Act
EIGE	European Institute for Gender Equality
EU-GBV	EU Gender-based Violence (Survey)
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
HBSC	Health Behaviour in School-aged Children (Survey)
ICT	information and communication technology
LGBTIQ+	lesbian, gay, bisexual, transgender, intersex and queer
NGO	non-governmental organisation
WHO	World Health Organization

Executive summary

This report examines cyber violence affecting girls and adolescents ([1]) in the European Union, analysing its prevalence, underlying drivers and consequences and reviewing the effectiveness of existing policy and legal responses. It is based on a mixed-methods research design that combines legal and policy analysis, statistical evidence and participatory insights from adolescents across 10 EU Member States, providing a comprehensive understanding of both the structural and lived dimensions of cyber violence and supporting evidence-based policy action at the EU and national levels.

The study was conceived as a bridge between research and policy, ensuring that empirical findings directly inform EU and national measures to prevent and respond to gender-based cyber violence.

The study explores how girls aged 13–18 define, experience and respond to cyber violence, both as victims and as bystanders, and considers the wider social and institutional contexts in which these experiences take place. The analysis of boys' (15–18) experiences focuses on social norms, masculinity, bystander behaviour and empathy. Particular attention is given to the ways in which gender norms, social expectations and patterns of digital interaction shape young people's perceptions and behaviours online.

The research is framed within the Beijing Platform for Action, with a focus on Area D on violence against women and Area L on the girl child, and supports EU efforts to prevent and address gender-based violence in all its forms.

([1]) The authors recognise that various terms are used to describe this phenomenon, including technology-facilitated abuse, technology-facilitated gender-based violence and technology-facilitated violence against women. For the purposes of this project, the term 'cyber violence' has been adopted, as it is the most commonly used within European context and aligns with Directive (EU) 2024/1385 on combating violence against women and domestic violence.

Key findings

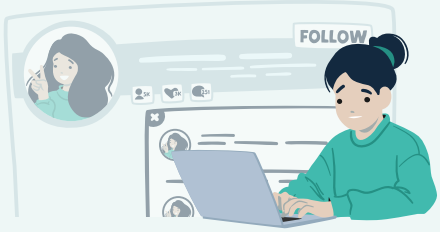
Cyber violence against women and girls is increasingly recognised as an integral part of girls' everyday lives

- For many girls, cyber violence is not an occasional threat but a persistent feature of their daily lives, shaping how they communicate and engage online. Girls describe constant exposure to harmful behaviours that make digital spaces feel unpredictable and unsafe.
- Cyber violence is part of everyday digital life, with harmful messages, insults, rumours and unwanted attention appearing daily or even hourly across platforms. Young people experience its overflow from online to offline settings, as harassment and exclusion often continue within schools or peer groups.

- Girls are targeted more frequently than boys, particularly in terms of sexual harassment, image-based abuse and attacks on reputation. Repeated exposure to these behaviours contributes to a sense that cyber violence is unavoidable and difficult to escape, as girls come to see it as part of the online environment they must navigate.
- Discussions in focus group settings highlighted that boys often engage in cyber violence to gain social approval from peers. Boys highlight how dominant norms of masculinity shape their online behaviour. Acts like non-consensual image sharing or group harassment are framed as performances to impress others or conform to peer expectations.

Girls are exposed to cyber violence from a young age

- Cyber violence begins when girls first start using digital technologies and social media, with many recalling early encounters with offensive or unwanted messages, sometimes before entering secondary school. Survey data confirms that unwanted messages and explicit content are among the most common forms of online abuse, with a significant share of girls reporting having had such experiences before the age of 15.
- Younger girls (13–15) report more relational and peer-based forms of aggression, including exclusion, gossip and body shaming, while older girls (16–18) more often face sexualised and coercive forms of abuse, such as online sexual coercion and extortion ([2]), deepfakes and non-consensual image sharing.
- Inappropriate or sexualised content appears even on platforms designed for children, showing that existing safeguards are insufficient. Girls called for earlier and age-appropriate prevention and digital literacy activities, noting that awareness sessions in schools often take place only after incidents have occurred.



2 Online sexual coercion and extortion of children is defined by the European Union Agency for Law Enforcement Cooperation (Europol) as a form of digital blackmail of children where sexual information or images are used to obtain sexual material, sexual favours or money from a victim (Europol, 2017). It is also a form of technology-facilitated gender-based violence, often referred to colloquially as 'sextortion' when affecting adult victims. Europol recommends that this colloquial term not be used in cases affecting children.

Sexual and image-based abuse, including AI-generated deepfakes, is a growing and particularly harmful form of cyber violence

- Sexual and image-based abuse is one of the most visible and damaging forms of cyber violence, with participants describing these experiences as deeply distressing and harmful to their privacy, reputation and sense of safety. Non-consensual photos are often taken or shared within school or peer environments, rapidly spreading beyond girls' control.
- The creation and distribution of manipulated or AI-generated images ('deepfakes' or 'deepnudes') is an alarming new form of abuse, used to humiliate or coerce girls and leaving them with little possibility of redress.
- The speed and reach of online sharing amplify the harm, as photos and videos can circulate widely in seconds. Even seemingly harmless images, shared voluntarily or with friends, can become a source of harassment or blackmail when used without consent or taken out of context.

Protections and institutional responses are not keeping pace with technological change

- Legal and policy analyses show that protections against cyber violence remain fragmented and uneven across the EU. Directive (EU) 2024/1385 on combating violence against women and domestic violence is a major step forward, and prioritising its full transposition into national law and implementation is key to significantly and positively impact women and girls' lives.
- Girls often perceive schools, police and other authorities to be ill-prepared or unresponsive, reporting that their complaints are sometimes dismissed or ignored. Fear of blame, shame and a lack of confidence in adults' ability to act effectively discourage many from reporting, leaving victims to handle harm on their own.
- Weak and inconsistent moderation practices allow harmful content to circulate widely, while online anonymity enables perpetrators to act with impunity. In line with Digital Services Act (DSA) provisions, stronger coordination between EU and national authorities, alongside binding accountability for digital platforms, is needed to ensure that technological progress is matched by adequate legal and institutional protection.

Peer culture and gender norms strongly influence the occurrence of cyber violence and the ways it is addressed

- Peer culture plays a crucial role in shaping how online violence unfolds and how young people respond to it. Harmful behaviours are often reinforced by social pressure to conform or maintain status, particularly among boys, and by gender norms that encourage victim blaming and double standards.
- Cyber violence reflects broader gender inequalities, with humiliation and control used to police girls' appearance, behaviour and online self-expression. Bystander inaction also perpetuates abuse: most adolescents have witnessed online violence without intervening, often out of fear or uncertainty.
- Intersectional factors such as age, race, disability, belonging to a religious minority, sexual orientation, gender identity and body size increase vulnerability, compounding the risks for some groups of girls. Participants called for inclusive and participatory prevention efforts that involve boys and promote empathy, respect and accountability.
- Good practices identified through national- and EU-level mapping show that gender-transformative education and dialogue-based approaches can challenge harmful norms, empower bystanders and reduce tolerance for online abuse.

Introduction

Across the European Union, cyber violence has emerged as a rapidly expanding form of gender-based violence that affects adolescents with particular intensity. As digital communication becomes deeply embedded in young people's social lives, online spaces increasingly shape how relationships are formed, negotiated and sometimes exploited. Recent EU-level analyses show that women and girls are disproportionately exposed to intrusive, sexualised or hostile behaviours online (EIGE, 2022), reflecting enduring gender norms and the shifting dynamics of peer interactions in digital environments.

With the rise of digital connectivity and the increased centrality of social media in adolescents' lives, the risk of technology-enabled harassment, non-consensual image sharing, cyberstalking and hostile online behaviours has intensified (Council of Europe, 2018). At the same time, European and international institutions have progressively come to recognise online gender-based violence as a pressing policy challenge (UN Special Rapporteur on VAWG, 2018; European Parliament, 2021a), highlighting its social and political relevance and its implications for children's rights, mental health and gender equality.

The existing datasets and institutional reports highlight the scale and diversity of online abuse. However, far less is known about how adolescent girls understand and interpret these behaviours in their everyday lives, how they respond when harm occurs and what support mechanisms they find meaningful, trustworthy or insufficient. By adopting a qualitative, participatory approach, this study explicitly positions adolescents as knowledge-holders rather than passive respondents – a methodological choice that enables their voices, perceptions and lived experiences to be meaningfully captured and foregrounded. They provide the most valuable evidence for EU- and national-level policy action.

The main objective of this study is to advance knowledge on how adolescent girls aged 13–18 experience cyber violence in the EU. This involves examining the ways in which they define and recognise cyber violence – both as victims and bystanders – while also analysing their perceptions of institutional and adult-led prevention efforts and their experiences of reporting incidents to parents, teachers or online platforms. In doing so, the research not only sheds light on girls' direct encounters with cyber violence, but also on their evaluations of the available support mechanisms and their reflections on their own behaviour online. Discussions with adolescent boys reflect their awareness of how cyber violence affects girls and touch upon how they behave when witnessing it.

The study adopted a multilayered methodological approach combining desk research and fieldwork in order to capture both the structural dimensions of the phenomenon under investigation and the lived experiences of those directly involved. Triangulation across data types – quantitative evidence, policy and legal frameworks, and participatory insights – ensured both breadth and depth ([3]).

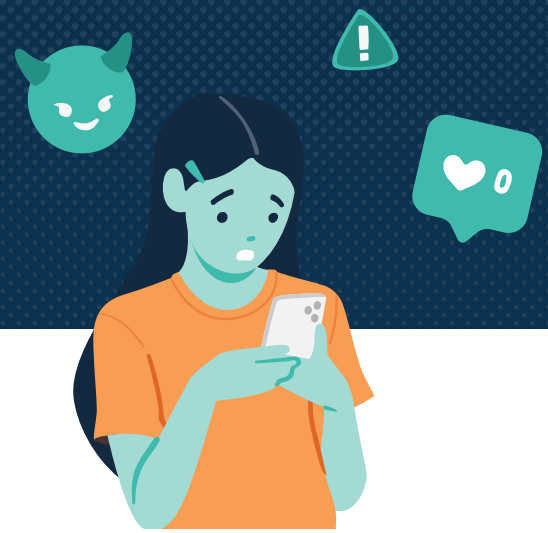
Desk research and a literature review provided the conceptual and empirical foundation for the qualitative research. The policy and legal mapping of international, EU and national frameworks helped to identify how cyber violence is regulated. Official sources were complemented by snowball techniques used to capture emerging national measures, providing a comparative overview of legal and policy responses across EU Member States. Statistical data analysis contextualised the phenomenon using EU-level and national surveys, comparative studies and EU-funded projects such as EU kids online. They helped quantify trends and connect structural data with qualitative findings.

The second pillar of the methodology was qualitative fieldwork carried out in focus groups, capturing adolescents' lived experiences. Across 10 Member States (Belgium, Germany, Estonia, Ireland, Spain, Italy, Cyprus, Poland, Romania and Sweden), 37 focus groups were run involving 133 girls (aged 13–18). Focus group discussions with 38 boys aged 15–18 also took place in three Member States (Ireland, Cyprus and Romania). Age-appropriate guides included interactive tools for younger groups and scenario-based discussions for older participants; boys' groups focused on social norms, masculinity, bystander behaviour and empathy.

Chapter 1 presents the conceptual and contextual foundations of cyber violence, including its definitions, main forms and the prevalence of data at the international, EU and national levels. Perceived causes and contributing factors are also analysed. Chapter 2 presents the findings from the qualitative fieldwork, highlighting the awareness and understanding of cyber violence that the girls and boys who took part in the focus groups across 10 Member States had. Chapter 3 explores in more detail girls' experiences of cyber violence, including the contexts, roles and dynamics involved. Chapter 4 examines the impacts of cyber violence on young people, highlighting their own perspectives on its social and psychological consequences. Chapter 5 addresses prevention and responses, reviewing some examples of international, EU and national frameworks and policy measures and young people's views on their effectiveness. Finally, the report concludes with key insights and policy implications, outlining recommendations for future EU and national action.

3 For a more detailed description of the methodology used, see Box 7 in the annex.

1 The phenomenon of cyber violence against girls and young women



1.1. Concepts and definitions of cyber violence

Cyber violence against women and girls is a multifaceted and intersectional form of gender-based violence, encompassing behaviours such as cyberstalking, online sexual harassment, non-consensual image sharing and gendered hate speech. These harms are shaped by societal norms that reinforce male dominance, relational dynamics like coercion and peer validation, and developmental factors that make adolescents especially vulnerable to online abuse (Cybersafe, 2020). Although academic discourse on cyber violence dates back to the mid 1990s ([4]) coinciding with the rise of internet usage and online platforms – wider recognition of cyber violence against women and girls has received sustained attention only in recent years. Earlier studies explored how technology reshaped dominant paradigms around gender, identity and sexuality (Gurumurthy et al., 2009), raising concerns about its role in enabling new forms of violence, particularly against women. As Judy Wajcman (2004, 2010, 2015) has argued, technology is deeply embedded in social power relations and far from neutral – it reproduces and reconfigures gendered hierarchies that can sustain symbolic and structural forms of violence.

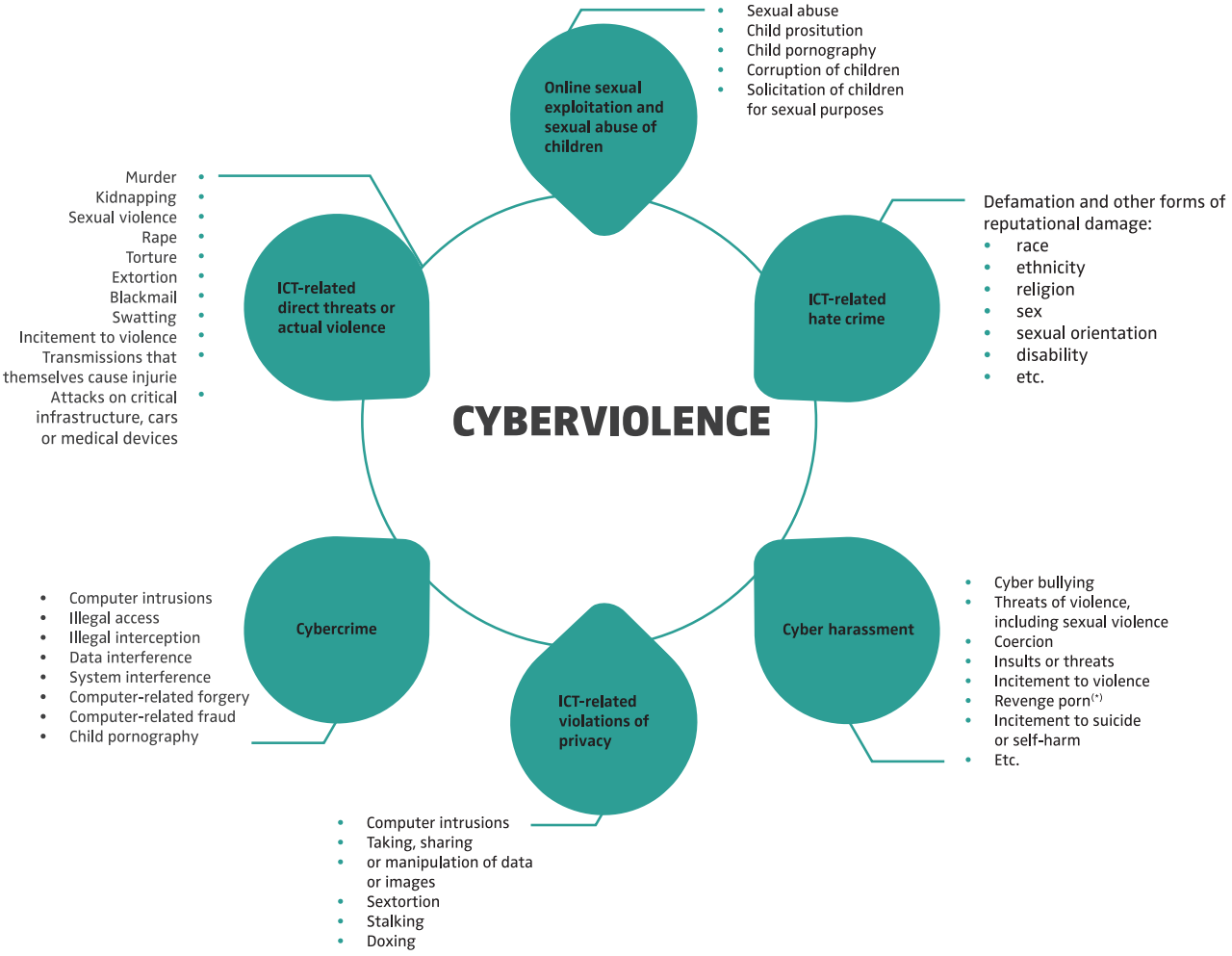
Given its rapidly evolving nature, cyber violence is classified in various ways, taking into account the type of behaviour, the characteristics of the victims and perpetrators, the technological tools used and the resulting impacts (Mukred et al., 2024). Other key elements in conceptualising cyber violence include the victim's perception of harm and the lack of consent (Koukopoulos et al., 2025).

4 For example, early studies on cyber violence – such as McGraw's 'Sexual harassment in cyberspace: The problem of unwelcome e-mail' ([1995]) and Adam's 'Cyberstalking and internet pornography: Gender and the gaze' (2002) – offer insights into the phenomenon and its consequences.

Cyber violence against women and girls covers a wide spectrum of online harms, including stalking, bullying, doxing, trolling, sexual harassment ([5]), defamation, hate speech and exploitation ([6]). Victims are often children, adolescents and women, with certain groups disproportionately affected and targeted. Perpetrators may act individually, collectively or through organisations, making use of social media, messaging applications (apps), email, phone communications and other digital channels.

The continuously evolving nature of cyber violence poses significant challenges for the development of conceptual and legal definitions. Its scale and speed make it one of the most pervasive and severe forms of violence in contemporary society (USAID, 2023). To enhance understanding and better reflect its complexity, the Council of Europe proposed a multi-dimensional framework for cyber violence (Council of Europe, 2018) that categorises various forms of online harm, such as privacy violations related to information and communication technology (ICT), cyber harassment, hate crimes and online child exploitation (Figure 1).

Figure 1 | Council of Europe's conceptual framework of cyber violence



Source: Council of Europe, 2018, p. 6.

(*) The term 'revenge porn' is commonly used in the legal and policy frameworks of Member States, whereas academic literature generally refers to 'non-consensual sharing of intimate images'. 'Revenge porn' can be misleading as it downplays the severity of the crime, the different range of gendered/sexualised forms of abuse and its profound impact on victims.

5 This term covers a wide range of actions such as image-based sexual harassment including creepshots, upskirting, non-consensual image or video sharing, cyberflashing, deepfakes and recorded sexual assault and rape.

6 This term covers a wide range of situations such as scamming for financial gain/extortion, grooming children or young people towards sexual activity or criminal activity.

At the policy level, EU policy documents have begun to refer to the United Nations' definition of cyber violence, as outlined in the 2018 report by the UN Special Rapporteur on Violence against Women and Girls (United Nations, 2018). The report defines cyber violence against women as 'gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately'.

This definition was reaffirmed in the 2021 European Parliament resolution on cyber violence (European Parliament, 2021a). A major legislative step followed with the adoption of the 2024 EU directive on combating violence against women and domestic violence (Violence against Women Directive). As the first comprehensive EU law addressing violence against women, the directive criminalises a wide range of cyber offences, including the non-consensual sharing of intimate or manipulated material, cyberstalking, cyber harassment, cyberflashing, cyber incitement to violence or hatred and online sexual harassment. It thus serves as a key legal foundation for defining and tackling cyber violence across the EU that recognises its complexity and evolving nature. Beyond providing a much-needed definition, the directive also includes several instrumental provisions on cyber violence, such as the obligation to take down content, the definition of appropriate reporting channels and the need for Member States to provide specialist support services for victims of cyber violence. Considering the above, Box 1 below outlines the most frequent forms of cyber violence.

Box 1 | The most frequent forms of cyber violence

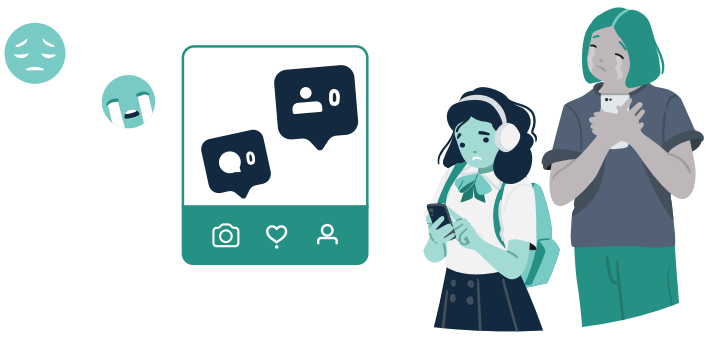
- Cyber harassment. This includes cyberbullying, online sexual harassment, the unsolicited receipt of sexually explicit material, mobbing and deadnaming. According to the 2024 EU directive, cyber harassment includes (i) repeatedly or continuously engaging in threatening conduct directed at a person at least where such conduct involves threats to commit criminal offences by means of ICT; (ii) engaging, together with other persons, by means of ICT, in publicly accessible threatening or insulting conduct directed at a person; (iii) the unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person; and (iv) making accessible to the public, by means of ICT, material containing the personal data of a person, without that person's consent.
- Cyberstalking. Repeatedly or continuously placing a person under surveillance, without that person's consent or a legal authorisation to do so, by means of ICT, to track or monitor that person's movements and activities.
- ICT-related violations of privacy. This includes the accessing, recording, sharing, creation and manipulation of private data or images, especially image-based sexual abuse, the non-consensual creation or distribution of private sexual images, doxing and identity theft.
- Recording and sharing images of rape or other forms of sexual assault.
- Remote control or surveillance. This includes by means of spy applications on mobile devices.
- Threats. This includes direct threats and threats of and calls to violence, such as rape threats, extortion, online sexual coercion and extortion (sextortion) and blackmail directed towards the victim, their children, their relatives or other persons who support the victim and who are indirectly affected.

- Sexist hate speech. Posting and sharing content that incites violence or hatred against women or LGBTIQ+ (lesbian, gay, bisexual, transgender, intersex and queer) people on the grounds of their gender identity, gender expression or sex characteristics.
- Inducements to inflict violence on oneself. This includes violence such as suicide, anorexia or psychological injury.
- Computer damage. This includes damaging files, programmes or devices and attacks on websites and other digital communication channels.
- Unlawful access. This includes unlawful access to mobile phones, email, instant messaging messages or social media accounts.
- Breach of the restrictions on communication imposed by means of judicial orders.
- The use of technological means for trafficking in human beings. This includes for the sexual exploitation of women and girls.

Source: European Parliament, 2021a.

In light of these definitions, inconsistencies in terminology across legal and academic contexts highlight the need for broad interpretations of cyber violence that can capture the diverse forms and expressions of violence it may refer to (EIGE, 2022).

While cyber violence can target any individual or group and encompass a variety of actions and behaviour, it disproportionately affects women and children (Council of Europe, 2018). Moreover, while men can also experience cyber violence, research (e.g. Backe et al., 2018; Hicks, 2021) shows that women and girls face greater risks due to entrenched gender norms and inequalities and often experience more severe and lasting consequences (EIGE, 2022). Given that younger individuals are the most active users of social media and ICT, international research ([7]) has highlighted that girls and young women face heightened vulnerability to specific forms of cyber violence, including but not limited to cyberbullying and the non-consensual sharing of intimate images. This underscores the need for a child-centred approach ([8]) that considers how psychological, developmental and societal factors influence young people's digital interactions (Cybersafe, 2020).



7 See, for instance, PLAN International, 2020; Vogels, 2022; Sciacca et al., 2023.

8 See Council of Europe, 2020. Additional literature on this topic is available in the Council of Europe's library, which features research on cyber violence categorised by target group, including studies focused specifically on children. See, for instance, WeProtect Global Alliance, 2016, 2021. For more information, please visit the Council of Europe's library on cyber violence: https://www.coe.int/en/web/cyber violence/library1.

Box 2 | Forms of cyber violence against women and girls considered for this research study

- Cyber harassment (including cyberbullying)
- Cyberstalking
- Non-consensual sharing of intimate or manipulated material
- Cyber incitement to violence or hatred directed at women and girls
- These forms of cyber violence are outlined in the 2024 EU Violence against Women Directive and are recognised as the most widespread forms of cyber violence (EIGE, 2022).

1.2. Prevalence and contexts of cyber violence

Cyber violence against women and girls is increasingly recognised as being part of a broader continuum of violence that includes both online and offline behaviours (Dunn, 2020; Lu et al., 2021; Machado et al., 2022). It is grounded in structural power imbalances and perpetuated by societal gender stereotypes (EIGE, 2024). Many forms of cyber violence, such as harassment, bullying and stalking, often originate in offline interactions, with the digital environment amplifying their scope and impact.

In a world where digital technologies are embedded in everyday life, the internet and related tools have become extensions of the environments in which women and girls experience violence. This digital dimension also has direct consequences for their safety, dignity and overall well-being (OAS, 2021). For instance, street harassment, bullying at school and intimate partner abuse may extend into digital spaces through cyber harassment, cyberbullying, and non-consensual image distribution and online stalking. Conversely, online interactions with strangers on social media can be exploited by the perpetrators and escalate into real-world threats, including of sexual violence. These patterns of abuse underscore the link between digital and physical violence against women and girls (OAS, 2021).

Studies reveal a significant overlap between cyber violence and offline abuse; for example, 70 % of victims of cyber harassment and stalking in the EU have also endured intimate partner violence, as shown by the EU Agency for Fundamental Rights (FRA) (2015). This overlap underscores the pervasive nature of cyber violence against women and girls and how it is embedded within broader patterns of systemic violence.

Moreover, ICT has played a significant role in enabling new strategies of abuse and control, particularly within intimate partner violence. Among young couples, such behaviours have become normalised within online–offline interactions and are often misinterpreted as signs of love (Lu et al., 2021). This sort of online abuse includes demanding access to a partner's passwords, monitoring their online activities and restricting their interactions on social platforms.

Research consistently shows that, among women, sexual harassment and stalking are the most commonly reported forms of cyber violence (UN Women et al., 2023). A particularly alarming aspect of online harassment is its potential for widespread distribution beyond the control of either the sender or recipient. In extreme cases, the creation and sharing of sexual images involving minors constitutes the creation and sharing of child sexual abuse material (Smahel et al., 2020).

Data from the EU Gender-based Violence (EU-GBV) Survey (2021 wave) ([9]) further indicates that receiving unwanted messages or emails is the most widespread form of (cyber)violence repeatedly performed by the same perpetrator (9 %), surpassing public offensive comments (4 %) or image-based abuse (1 %) (Figure A.7 in the annex). Notably, some victims reported having such experiences before the age of 15, further highlighting that exposure to violence begins in childhood (Figure A.8 in the annex).

Testimonies from young participants in this study's focus groups further confirm that even seemingly harmless images – such as a swimsuit photo – can trigger harassment, blackmail or long-term reputational harm, reflecting research that highlights how content can quickly become uncontrollable once shared.

Research also indicates that age, alongside gender, plays a crucial role in the occurrence of cyber violence (FEMM Committee et al., 2018; Pichel et al., 2021; López-Castro et al., 2023; Schittenhelm et al., 2024). Social media use is most prevalent among girls and young women and less common among older women. For younger women and girls these platforms serve multiple purposes, including maintaining friendships, communicating with family, exploring job opportunities and engaging with wider social networks. Yet, women do not need to be active internet users to experience cyber violence or abuse. They may still be targeted, for example through the online distribution of sexual content or sexual exploitation on trafficking websites (FEMM Committee et al., 2018).

A 2020 global survey conducted by the World Wide Web Foundation and the World Association of Girl Guides and Girl Scouts ([10]) found that 52 % of young women and girls reported experiencing some form of online abuse. Notably, respondents aged 15 to 19 expressed particular concern over the unauthorised sharing of private images and videos. Similarly, Plan International (Plan International, 2020) has estimated that 58 % of young women and girls worldwide have experienced online harassment on social media platforms, noting that most girls report their first experience of social media harassment happening between 14 and 16 years of age.

Teenage boys and young men have been found to be specifically targeted for online sexual coercion and extortion, often referred to as 'sextortion' (Thorn, 2024; WeProtect Global Alliance, 2024, Foster, 2023). In such cases, victims face blackmail or threats of intimate images being shared. Such pictures or videos may have been shared by the victims or AI-produced. Predators then demand sexual favours, sexual content and most often money from the victim in exchange for not disseminating the images. Evidence from various countries points to the perpetrators operating in organised criminal networks often based in less-developed countries, with financial gain being the main motivator (Europol, 2017, Foster, 2023). With free generative AI tools becoming widely available, predators can easily use the victims' photos or videos posted on social media to create deepfake images and videos (WeProtect Global Alliance, 20242024). Evidence from Australia, the United Kingdom and the United States shows increases over the past few years in the number of cases of teenage boys facing such violence (eSafety's Commissioner and Australian Communications and Media Authority (ACMA), 2022).

Evidence at the EU level supports these findings, showing how the risks of cyber violence vary by both age and gender. According to data from the World Health Organization (WHO), cyberbullying is most prevalent among both girls and boys at the age of 13 across most Member States and regions in the EU. As seen in Figures A.1 and A.2 in the annex, the WHO's Health Behaviour in School-aged Children (HBSC) Survey

9 The 2021 wave of the EU-GBV Survey includes results from the 27 Member States. In total, the estimated average results for the EU-27 are based on data collected from 114 023 women ($^{18–74 \text{ years of age}}$) across the EU. Data collection took place between September 2020 and March 2024. Eurostat coordinated the data collection in 18 Member States, and the national statistical authorities of these countries carried out the survey. Italy agreed to share the data from its national survey to provide comparable data for the main indicators. In the remaining eight Member States, FRA and EIGE took responsibility for the data collection following the Eurostat methodological manual. More details on the survey methodology are available from Eurostat: https://ec.europa.eu/eurostat/cache/metadata/en/gbv_sims.htm.

10 This global survey was conducted in 2020 by the World Wide Web Foundation and World Association of Girl Guides and Girls Scouts using UNICEF's report platform concerning young people's experience of online abuse and harassment. There were 8 109 respondents, of which 51 % were women and 49 % were men. Survey data is available at https://ureport.in/opinion/3983/.

(Cosma et al., 2024) indicates that, in 2022, a higher percentage of 13-year-old girls experienced cyberbullying than boys in nearly all Member States (22 Member States) and in both the Flemish and Walloon Regions of Belgium. This gender gap is also observed among 15-year-olds, with girls reporting higher rates of cyberbullying in 15 Member States and in both Belgian regions.

Among 13-year-old girls, the prevalence of cyberbullying ranges from 10 % in Portugal and the Netherlands to 29 % in Latvia. For boys of the same age, rates range from 7 % in the Walloon Region of Belgium to 32 % in Lithuania. Among 15-year-olds, the variation is similar: for girls, reported rates of cyberbullying range from 7 % in Portugal to 24 % in Spain, while for boys, they range from 3 % in Spain to 31 % in Lithuania.

While earlier research suggested that incidents of cyber harassment were more prevalent in Member States with higher internet access rates (FRA, 2015), this link has become less relevant over time. Since 2015, disparities in internet access across Member States have significantly diminished ([11]), suggesting that connectivity level is not a meaningful indicator of the prevalence of cyber violence.

Additionally, although social media enhances communication and fosters social connections, its excessive or compulsive use may negatively impact well-being, and the well-being of children and adolescents in particular. Social media use among adolescents displays gendered patterns, with more girls than boys actively engaging with these platforms between the ages of 11 and 19 (Leonhardt et al., 2021). In addition, evidence indicates that girls experience stronger negative psychological effects linked to social media engagement.

For example, girls aged 11–13 are more likely than boys to report poorer sleep, body image concerns and depressive symptoms (National Academies of Sciences, Engineering, and Medicine, 2024).

Excessive social media use among girls has been associated with vulnerability to depression and anxiety, largely due to societal pressures related to self-evaluation, body image and conforming to beauty standards. These pressures can contribute to dissatisfaction, emotional distress and low self-esteem (Sala et al., 2024). Research further shows that susceptibility to these negative effects varies by age and gender: girls aged 11–13 and boys aged 14–15 show greater risk of decreased life satisfaction as their social media engagement increases (National Academies of Sciences, Engineering, and Medicine, 2024).

Findings from the HBSC study provide additional evidence of this association, highlighting concerns related to 'problematic social media use', which is defined as use exhibiting addictive-like symptoms ([12]). As seen in Figures A.3 and A.4 in the annex, in nearly all Member States in 2022, girls were more prone than boys to report the problematic use of social media at both ages 13 and 15, with the exception of Finland ([13]). Among 15-year-olds, the lowest percentage of girls exhibiting symptoms of problematic social media use was observed in the Netherlands and Denmark (7 % in both), while Romania had the highest rate at 28 %. For boys, the lowest rates of reported 'problematic social media use' were found in the Netherlands, Hungary and Latvia (3 %), with Romania again showing the highest rate at 18 %.

As seen in Box 3, at the national level, several Member States have conducted specific surveys on cyber violence to better understand its prevalence, the groups affected and its consequences.

11 See Eurostat data on level of internet access across Europe: https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/table?lang=en.
12 The HBSC data on problematic social media use is available at https://data-browser.hbsc.org/measure/problematic-social-media-use/.
13 In Finland, boys aged 15 were more likely than girls of the same age to report problematic social media use ([12 % compared to 8 %]).

Box 3 | Examples of surveys on cyber violence carried out in Member States

- **France.** A 2022 survey by Feminists against Cyber Harassment ([14]) found that the majority of respondents who were victims of cyber violence were women (84 %) and individuals who experienced online discrimination based on their gender identity and sexual orientation (43 %). People with disabilities and from religious minorities also faced disproportionate risks and greater barriers to reporting.
- **Slovenia.** The ClickOFF! project (2024) (Šulc et al., 2024) found that over 50 % of girls aged 13+ had experienced cyber violence . Older students reported higher rates of both victimisation and perpetration. Among primary school students, 15–16-year-olds reported the highest rates of victimisation (57 %), while 15-year-olds were most likely to carry out cyber violence (10 %).
- **Netherlands.** Dutch Central Bureau of Statistics data (2022/2024) ([15]) shows that 1 in 5 young people (aged 15–24) experienced online threats, bullying, stalking or the non-consensual distribution of images. In 2024, 22 % of girls aged 16–18 reported online sexual harassment, compared with 7–8 % of boys ([16]). Regarding offline sexual harassment, the data further revealed that young women are disproportionally affected ([17]).
- **Portugal.** The Portuguese Association for Victim Support has reported data from the Safer Internet Helpline, which it has operated since 2019. In 2019, the helpline recorded 827 cases related to online sexual violence, of which 676 involved child sexual abuse material. Moreover, most of the cases reported to the helpline for support against cybercrime involved young people aged 11 to 17.
- **Belgium.** The 2022 #YouToo? Survey ([18]) found that 1 in 5 young people had experienced cyberbullying, often at an early age, indicating a need for early digital literacy and prevention. In 2026, a study on cyber violence in the context of dating found that 66 % of respondents reported being pressured to send nude photos on dating apps and that 60 % of respondents who did send a nude photo via an online dating site were then threatened with its distribution ([19]).
- **Italy.** A 2023 survey by the Osservatorio Indifesa ([20]) showed that nearly 80 % of adolescents viewed the internet as unsafe. Top concerns included cyberbullying (23 %), identity theft and social isolation (18 % both), while other issues included non-consensual intimate image abuse (14 %), harassment (10 %) and stalking (7 %).
- **Germany.** The 2024 Cyberlife study by Bündnis gegen Cybermobbing (Alliance against Cyberbullying) ([21]) found that 2 million students had experienced cyberbullying. Key issues included a low awareness among parents and schools and heightened vulnerability among socially isolated young people. Alarmingly, 1 in 4 affected students had suicidal thoughts, with suicide being a leading cause of death among 15–25-year-olds.

14 https://www.vscyberh.org/.
15 '2.2 million cybercrime victims in 2022' – Statistics Netherlands.
16 'Prevalence monitor on domestic violence and sexually transgressive behaviour 2024' – Statistics Netherlands.
17 'Prevalence monitor on domestic violence and sexually transgressive behaviour 2024' – Statistics Netherlands.
18 'Cyberbullying: One in five young people in Belgium have been victims' – The Brussels Times.
19 'Les violences numériques dans le contexte du dating et des relations entre (ex-)partenaires en Belgique' – Institut pour l'égalité des femmes et des hommes.
20 'Online violence: Protection and prevention of minor victims' – Terre des hommes.
21 Tension between Fascination and Danger: Cyberbullying among school students – Cyberlife.

1.3. Perceived causes and contributing factors

Cyber violence is deeply rooted in broader social structures, gender norms, peer dynamics and the rapidly evolving digital landscape. It is not only shaped by the behaviour of individuals but also by structural inequalities that make certain groups more vulnerable. **Key underlying causes include unequal power relations between women and men, gender stereotypes and the lack of effective safeguards in online platforms.** Age and other intersecting factors such as socioeconomic status, minority identity or disability can also significantly influence both exposure to and the impact of cyber violence. Adolescents, for example, are at greater risk as they navigate social development, increased online engagement and peer pressure, while girls and young women disproportionately face sexualised forms of online abuse. Persistent gender stereotypes and norms, including societal expectations about how women and men should look, behave or express their sexuality, normalise certain forms of online harassment and are often used to justify and downplay abuse.

Early instances of cyberbullying are frequently dismissed by children themselves as jokes or harmless fun. Younger children, in particular, may not recognise these behaviours as cyberbullying, perceiving them instead as tolerable – especially when the actions lack perceived malicious intent (Baas et al., 2013). **This minimisation normalises harmful behaviours and delays the recognition of abuse as a serious issue.** However, three key characteristics differentiate cyberbullying from innocent pranks or playful interactions: intention, repetition and a power imbalance (Baas et al., 2013).

Adolescents aged 15 to 16 report greater exposure to and receipt of online sexual content than their younger peers aged 12 to 14, with girls experiencing this more frequently than boys. As seen in Figure A.9 in the annex, at the EU level there is a significant correlation between age and the receipt of sexual messages. In the 14 Member State covered by the EU Kids Online study, a larger percentage of young people in the older age group (15–16 years old) reported receiving this type of message than in the younger age group (12–14). This highlights how greater online activity, coupled with gendered expectations about female sexuality, increases risks and exposure for older adolescent girls in particular. As illustrated in Figure A.10 in the annex, in most Member States represented, except for Croatia and Malta, girls are more affected by unwanted sexual requests than boys.

Age is therefore a significant contributing factor, as developmental transitions occurring during adolescence heighten both digital engagement and vulnerability to cyber violence. Older adolescents who are more active online and are more likely to engage in risk-taking behaviours face greater exposure to sexualised interactions. This increased risk is compounded by social expectations around sexuality, gendered double standards and peer validation practices. Indeed, while exposure to sexual content is increasingly seen as a normal part of adolescent sexual development, it also heightens the risk of cyber violence (Murphy, 2024).

Findings from the EU-GBV Survey confirm these age-related differences in exposure to cyber violence. Younger women report a higher prevalence of image-based abuse, such as the non-consensual publication of photos or videos. For instance, 37 % of women aged 25–34 and 23 % of those aged 18–24 report such experiences, compared to just 3 % of women aged 55–74. On the other hand, of the types of (cyber) violence experienced by older women (55 years old and above), the most common was offensive or embarrassing public comments (Figure A.6 in the annex). These patterns indicate that age, life stage and type of digital engagement are important drivers shaping the different risks seen across groups.

As with all forms of gender-based violence, cyber violence against women and girls is also shaped by a variety of other intersecting factors that exacerbate vulnerability and marginalisation in digital spaces. These include disability, sexual orientation, political beliefs, religion, social background, migration status and even celebrity status (GREVIO, 2021). Such intersecting identities can compound discrimination, making cyber violence both more frequent and more harmful.

Numerous studies emphasise the intersectional nature of cyber violence against women and girls, revealing that women and girls with diverse identities and backgrounds often face heightened risks of online abuse. For instance, FRA (2015) found that 34 % of women with disabilities reported experiencing physical, sexual or psychological violence, including online threats, compared with 19 % of women without disabilities. Disability-related stigma, barriers to reporting and isolation further intensify the harm.

Ethnicity and minority status also significantly influence the risk of online abuse. A 2017 FRA study (FRA, 2017) focusing on minorities indicated that younger migrants experience more in-person and online harassment than older migrants. Among migrants and minorities, these forms of harassment erode trust in institutions and hinder social integration (FRA, 2015). Young people's perspectives during focus groups add a lived dimension to these findings, as several described how their race and visible expressions of faith make them targets online. Thus, prejudice and systemic racism are powerful contributing factors to online harassment.

From the perspective of children and young people, factors such as race, religion, ethnicity (Ratajczak et al., 2019), social class, disability, sexual orientation and gender identity increase the risk of online harm (Project deSHAME, 2017). Studies confirm that adolescent girls from disadvantaged socioeconomic backgrounds or minority groups or with disabilities are disproportionately affected. For example, Wallace et al. (2023) found that about 40 % of the variance in cyber violence victimisation among girls aged 14–18 is attributable to intersectional factors. Similarly, data from the Pew Research Center (Vogels, 2022) shows that experiences of cyberbullying among US youth vary not only by age but also by physical appearance, ethnicity, sexual orientation and political beliefs. These findings highlight how personal identity markers interact with societal power dynamics to shape patterns of risk. Recent findings from Belgium show that young adults and LGBTIQI+ people are particularly vulnerable to online violence on dating apps due to their greater use of digital tools in relationships and dating, which foster certain forms of online violence. For LGBTIQ+ people, this violence can also be compounded by specific risks, such as outing or the exploitation of sensitive personal data, further increasing their vulnerability (Gilen, A., et al, 2025).

Vulnerabilities can also arise from personal circumstances, such as family challenges, previous abuse or gang involvement (Project deSHAME, 2017). The HBSC Survey (Cosma et al., 2024) indicates that peer cyber violence often reflects socioeconomic circumstances, with children from families of low affluence being more likely to be affected by cyber violence. This pattern is observed in several Member States in the EU with a few exceptions in which the prevalence of cyber violence is higher among children of families with high affluence ([22]). Moreover, problematic social media use and cyberbullying do not show significant variation across family affluence groups (Table A.7 in the annex).

Chapter 1 has mapped the conceptual landscape of cyber violence against girls and young women, highlighting its forms and prevalence. Yet, this only partially captures how such violence is experienced in daily life. To complement this body of evidence with lived experience, the study engaged directly with adolescents. As part of this research, focus groups were conducted with girls and boys in Belgium, Germany, Estonia, Ireland, Spain, Italy, Cyprus, Poland, Romania and Sweden to explore how young people – particularly girls – perceive, define and experience cyber violence. These discussions provided crucial first-hand insights, encompassing both personal experiences and the observations of peers. Focus group findings are integrated into the following chapters, as young people's voices are used to illustrate and expand on existing evidence. In doing so, the following chapters shift their focus from theoretical frameworks to lived realities, amplifying the perspectives of girls and boys and linking their experiences to the broader body of research.

22 As shown in Table A.6 in the annex. In these areas there is a significant difference in the prevalence of cyber violence based on family affluence ($^{at\ p < 0.05}$) for girls and/or for boys.

2 Perceptions of cyber violence among girls and boys

2.1. Experience and understanding of cyber violence

As discussed in Section 1, cyber violence is a pervasive and rapidly evolving threat that disproportionately affects children, teenagers and young adults – particularly girls – with their developmental stage and gaps in legal protection potentially heightening the harm they experience (EIGE, 2022). Cyber violence manifests in various forms, including verbal harassment, psychological manipulation, reputational attacks and technology-enabled sexual abuse. Understanding these diverse forms is essential for young people to recognise abusive behaviours and respond effectively.

Young people's experiences and understandings of cyber violence differ significantly by age and gender (Vogels, 2022). This variation is further explored through girls' own accounts of cyber violence in focus group discussions, as detailed in the sections below. Older girls, for instance, are more likely to encounter invasive and sexually explicit forms of abuse, such as unsolicited explicit images, the non-consensual sharing of explicit images and persistent inquiries about their whereabouts and activities from individuals other than their parents. In contrast, younger girls tend to face offensive name-calling and false rumours being spread about them (Table A.4 in the annex). This progression suggests that, as girls grow older, the cyber violence they experience becomes increasingly sexualised and controlling. Moreover, these patterns align with girls' own descriptions of public humiliation, social exclusion and appearance-based judgement, showing that cyber violence gains complexity as girls mature.

Technology-facilitated intimate partner violence as a growing concern

An emerging focus of research on cyber violence targeting girls and young women is technology-facilitated intimate partner violence. This form of abuse is characterised by actions such as the control, harassment, stalking and mistreatment of a partner through technology and social media (Zweig et al., 2014).

This form of intimate partner violence may occur both within current relationships and after relationships have ended, and it can manifest in emotional, physical or sexual forms. Perpetrators use a wide range of digital methods: unauthorised access to email or social media accounts, GPS tracking and the use of stalkerware, emotional manipulation and online threats are all common. The use of 'smart' home devices for surveillance and stalking, alongside AI tools, is also common. Notably, these behaviours often continue even after the relationship has ended.

Technology-facilitated intimate partner violence is often intertwined with offline forms of dating violence, with both forms often occurring simultaneously (Van Ouytsel et al., 2020). Young people – particularly young women – may struggle to recognise these behaviours as abusive, complicating efforts to identify and address them.

Findings from the EU-GBV Survey confirm these patterns: about 1 in 9 women reported being pressured by a partner to disclose their whereabouts or being digitally tracked (via GPS, phone or social networks). When distributed by age, the occurrence is particularly high among women aged 35–44, where nearly 1 in 4 (23 %) reported such experiences (Figure A.5 in the annex).

Coercion to share sexual images is widespread

European data from project deSHAME (Project deSHAME, 2017) in Denmark, Hungary and the United Kingdom shows that 1 in 10 respondents aged 13 to 17 (9 % in Denmark, 7 % in Hungary and 12 % in the United Kingdom) reported being pressured by a boyfriend or girlfriend to share nude images, with girls being disproportionately affected. Additionally, 1 in 6 respondents (16 %) reported having kept a screenshot of a nude or sexually explicit image or conversation for future use (13 % in Denmark, 19% in Hungary and 16 % in the United Kingdom). Furthermore, 44 % of respondents acknowledged that young people may engage in online sexual harassment as a form of revenge against an ex-partner (51 % in Denmark, 33 % in Hungary and 47 % in the United Kingdom). Similar findings are illustrated by the Cybersafe project, which, through focus groups with young people aged 13–17 in Estonia, Greece, Italy and Northern Ireland, found that online partner violence – especially men's abuse of women – is frequently discussed among teenagers (Cybersafe, 2020).

Anonymity online increases risks for vulnerable groups

The anonymity provided by digital platforms allows individuals to easily conceal their identity, putting young women, girls, and sexual, gender and ethnic minorities at greater risk (Smith, 2023). Focus group participants echoed these concerns, reporting stalking, fake profiles and the persistent monitoring of personal digital spaces as everyday threats. The ease with which people can create fake profiles or impersonate others in online spaces heightens the risks for those seeking connection, making these environments inherently unsafe and potentially violent, with emotional consequences (Smith, 2023). Moreover, the digital nature of online abuse can lead young people to underestimate its impact, believing that simply logging off or blocking the abuser offers sufficient protection (Afrouz et al., 2024). Thus, understanding how anonymity exacerbates risks can enhance girls' awareness of potentially harmful online interactions, encouraging them to recognise unsafe behaviours early.

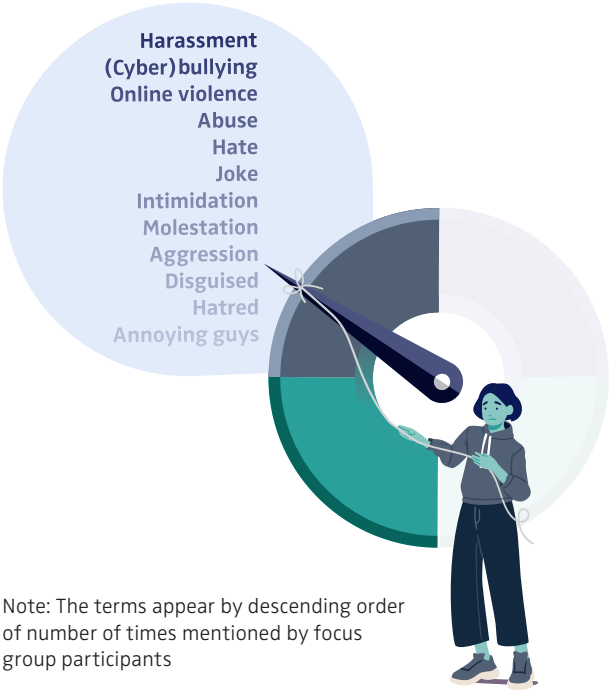
2.2. Understanding cyber violence through young people's voices

Insights from the focus groups with girls (aged 13–18) carried out within the framework of this study provide a deeper understanding of these patterns. Girls demonstrated a multifaceted understanding of cyber violence, shaped by their lived experiences and social environments. When asked about the term 'cyber violence' ([23]), girls described a broad spectrum of everyday behaviours, rather than isolated or extreme incidents. These included verbal and psychological abuse; sexualised forms of cyber violence; coercion, manipulation, and blackmail; and body shaming and appearance-related judgement.

Before analysing specific themes in detail, it is important to highlight the broader forms of online aggression highlighted earlier – verbal harassment, social exclusion and reputational harm – which were also prevalent in these discussions. Girls often linked cyber violence to wider patterns of bullying, intimidation and social exclusion. While these behaviours may not always be overtly sexual or gendered, they nonetheless contribute to digital environments in which girls frequently feel unsafe, scrutinised or unwelcome.

Though less frequent, other important themes that emerged and are highly relevant to how girls understand and perceive the cyber violence that affects them are linked to gossip groups among peers, the ridiculing of mistakes, the spreading of false rumours and group bullying, all of which reinforce a sense of vulnerability in online settings. Additionally, girls used terms such as 'patriarchy', 'sexism' and 'discrimination', indicating an awareness that cyber violence is not just interpersonal but rooted in broader societal norms, gender stereotypes and gender inequalities.

FIGURE 2 | Main terms used by girls to describe cyber violence in the form of general aggression and violence



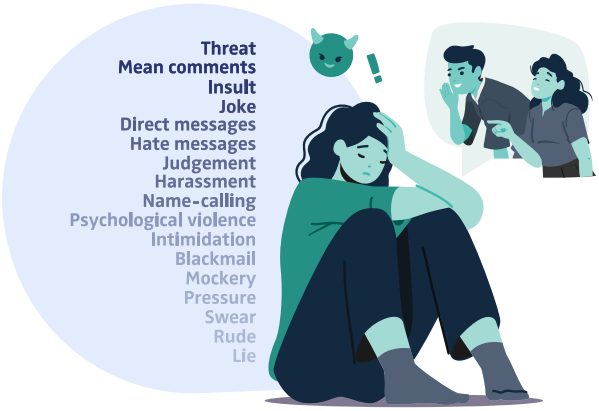
Note: The terms appear by descending order of number of times mentioned by focus group participants

Source: Authors, based on focus group discussions.

Girls also associated cyber violence with more generalised online aggression, including bullying and intimidation (Figure 2). Even when not explicitly sexual or gendered, such behaviours foster an environment of hostility in which girls feel unsafe, unwelcome or under constant scrutiny. Another recurring concern among girls is the misuse of technology to distort, manipulate or steal personal content. Girls expressed fear over practices like photo editing, doxing and the creation of fake content using private images – highlighting a growing awareness that cyber violence often entails the loss of control over one's personal information and digital identity. In addition, girls identified behaviours such as stalking, invasion of privacy, the use of fake accounts and anonymous calls as forms of cyber violence. This understanding, while not always linked to explicit threats, highlights a persistent sense of being monitored, watched or tracked online.

23 This section offers a snapshot of how girls spontaneously interpreted the term 'cyber violence' during the focus group discussions and what they associated it with, in response to the question 'What comes to mind when you hear the term cyber violence?' It reflects their initial, unfiltered perceptions and associations. The aim is not to redefine or develop a formal conceptual framework for cyber violence, nor to introduce new terminology. Instead, this section sheds light on the language, images and references that girls themselves use when thinking about the topic.

FIGURE 3 | Main terms used by girls to describe cyber violence in the form of verbal and psychological abuse



Source: Authors, based on focus group discussions.

Verbal aggression online was described as especially pervasive, frequently occurring in comment sections, private messages or group chats (Figure 3). Girls' testimonies reinforce research findings that online spaces are often defined by ambient hostility, where insults, threats and harassment are routine rather than exceptional.

Note: The terms appear by descending order of number of times mentioned by focus group participants

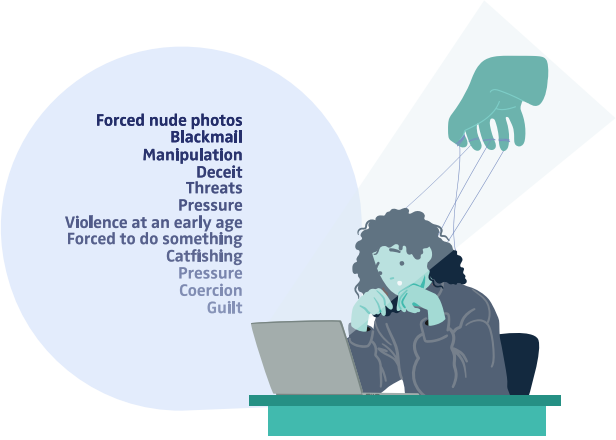
FIGURE 4 | Main terms used by girls to describe cyber violence in the form of sexual cyber violence

Source: Authors, based on focus group discussions.

Sexual cyber violence emerged as a central concern for girls (Figure 4). They associated cyber violence with unsolicited nudes, grooming, image-based abuse and revenge porn. Their language reflected a deep awareness of both the forms and emotional consequences of these behaviours.

Note: The terms appear by descending order of number of times mentioned by focus group participants

FIGURE 5 | Main terms used by girls to describe cyber violence in the form of coercion, manipulation and blackmail

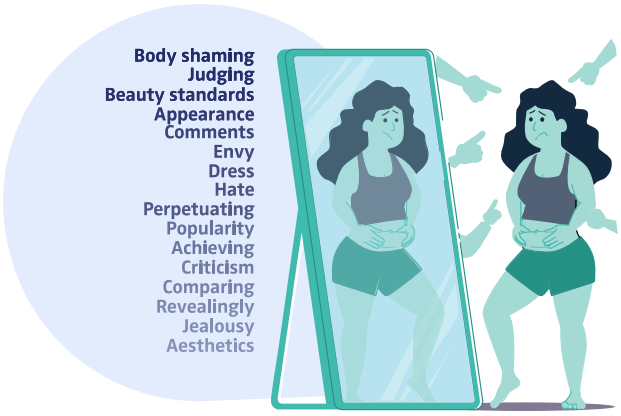


Source: Authors, based on focus group discussions.

Girls frequently pointed to manipulation as a significant aspect of cyber violence (Figure 5). Its methods – such as blackmail – were often framed as ongoing strategies of control that exploit trust and emotional vulnerability. One of the clearest manifestations of this dynamic is the pressure and coercion to share sexual content. Perpetrators exploit trust, manipulating victims into sending nude images or engaging in sexual interactions online. This pressure can escalate into blackmail, such as threats to leak private messages or images unless the victim complies (Salazar et al., 2023).

Note: The terms appear by descending order of number of times mentioned by focus group participants

FIGURE 6 | Main terms used by girls to describe cyber violence in the form of body shaming, judgement and beauty standards



Source: Authors, based on focus group discussions.

Appearance-based judgements, body shaming and social comparison were also cited as common and damaging forms of online harm (Figure 6), underscoring how gendered expectations and socially imposed beauty standards heighten girls' vulnerability to harm in digital environments.

Note: The terms appear by descending order of number of times mentioned by focus group participants

As evidenced by the literature in the field, girls' understanding of cyber violence also differed by age, reflecting their developmental stages, digital exposure and social environments. Younger girls, aged 13 to 15, were more likely to focus on more immediate, visible and relational forms of cyber violence. Their concerns were closely tied to familiar social settings such as school and peer groups. Many described experiences of bullying, exclusion from group chats, judgemental behaviour and body shaming as key forms of online harm. They also expressed anxiety around their appearance and social comparison, frequently referencing beauty standards and body evaluation. A strong theme among this age group was fear of visibility and reputational damage, with terms like 'public humiliation', 'sharing screenshots' and sexually derogatory labels reflecting concerns about being exposed, judged or ridiculed in online spaces.

Older girls aged 16 to 18 demonstrated a broader and more complex understanding of cyber violence, one that incorporated structural and psychological dimensions. They frequently referenced sexualised forms of harm, including online sexual coercion and extortion, sexual and image-based abuse and grooming. Mental health impacts were more commonly discussed in this group, with references to trauma, suicide and long-term emotional harm reflecting a keen awareness of the enduring psychological consequences of cyber violence.

> **"Beauty standards are making it difficult for girls to feel like themselves and feel good with themselves ... about how our body should look or our face or our hair. And I think that's why we see more bullying and violence towards the females."**
>
> **(GIRL 13–15, CYPRUS)**

Additionally, older girls appeared more familiar with the misuse of technology, describing incidents involving deepfakes and deepnudes, edited photos and doxing and expressing concern over the manipulation and theft of personal digital content. Their fears were heightened by the rapid advancement of AI, which they saw as enabling new and more harmful forms of cyber violence. One of the most alarming developments in this area is the proliferation of deepnudes or videos containing non-consensual synthetic intimate imagery (De Vido, 2024). The combination of readily available data, current technological capacity and the spread of deepfake applications allows explicit videos to be fabricated without consent

(EIGE, 2021). This technological ease dramatically expands the potential pool of perpetrators and intensifies the risk, as harmful content can be generated and disseminated faster, more widely and with greater anonymity than ever before.

Boys aged 15–18 years, on the other hand, demonstrated a multifaceted understanding of cyber violence as it affects girls, identifying behaviours that ranged from verbal harassment to more severe forms of sexual and psychological abuse. Bullying and verbal abuse – such as insults, threats and swearing – were the most frequently cited forms of cyber violence among boys in this age group. These behaviours were commonly described as occurring within peer settings and were sometimes normalised or downplayed as part of everyday online culture.

> **Now with AI I heard about a girl committing suicide because the boys from her class took pictures of her and thanks to AI, they made it look like she was naked and sent it to everyone.**
>
> **(GIRL 16–18, POLAND)**

Older boys more frequently identified sexual forms of cyber violence, including online sexual coercion and extortion, sexual and image-based abuse and grooming. This suggests that awareness of or exposure to such behaviours increases with age, though national and cultural contexts may also play a role. Indeed, in Ireland, Cyprus and Romania – the three countries where focus groups with boys were conducted – recent legislation has criminalised various forms of cyber violence. These legal changes seem to have reinforced boys' awareness, not only broadening their understanding of the issue but also strengthening their recognition of the serious emotional and reputational harm such actions can cause girls, particularly in cases involving the sharing of personal images or online blackmail.

Finally, boys also pointed to specific digital platforms where these behaviours occur, such as Fortnite and Snapchat. They described tactics like catfishing and the creation of fake accounts used to exploit, deceive or humiliate others online.

3 How girls experience cyber violence

Focus group discussions with girls from all participating Member States revealed a broad spectrum of experiences of cyber violence, both as victims and as witnesses. We then categorised these experiences into the forms of cyber violence listed in the 2024 directive to avoid introducing new terms and concepts and to align girls' experiences more closely with the terms provided therein. These accounts point to four distinct yet interconnected forms of abuse: (sexual) cyber harassment, cyberstalking, cyberbullying and image-based cyber violence ([24]). These forms correspond to the literature's descriptions of verbal, psychological and sexual abuse and the coercion and reputational attacks commonly encountered in girls' online lives. Participants consistently described digital spaces as hostile and unsafe. Many spoke openly about personal experiences of abuse, while others described incidents affecting their peers.

(Sexual) cyber harassment

Sexual violence and exploitation emerged as the most frequently cited forms of cyber violence across Member States and age groups. Participants reported receiving unsolicited sexual content and being confronted with predatory behaviour online. Examples included receiving explicit sexual images via Snapchat and encountering men on platforms such as Omegle ([25]) who would abruptly expose themselves during casual conversations. Participants also mentioned being added by accounts with sexually explicit usernames such as 'Horny in [city]' ([26]) or 'sending nudes', which they described as a normalised and routine part of their online interactions. Some participants recounted harassment by older men who would dismiss their age as irrelevant with 'it's okay, I don't mind' when the girl disclosed being underage. Others described persistent targeting despite repeated blocking, with perpetrators creating multiple fake accounts to continue contact.

24 See Table A.5 in the annex for specific examples of the types of cyber violence experienced by girls as victims and witnesses.
25 Omegle, a free online chat platform that connected users anonymously, shut down in November 2023. The platform faced increasing scrutiny over its role in facilitating harmful interactions, including sexual exploitation and abuse. For more information, see https://www.bbc.com/news/business-67364634.
26 The name of the city has been removed to protect the privacy and anonymity of the participants.

> **There was this person who, from his profile, seemed to be an older man who sent messages because this girl had an Instagram profile and he kept sending her various provocative messages, asking her to send him photos of herself in her underwear or even without [underwear], perhaps in certain positions, not the most appropriate. And every time she blocked him, he created other profiles and continued to write to her, so he didn't accept rejection.**
>
> **(GIRL 13–15, ITALY)**

Cyberstalking and coercion

Cyberstalking and coercion were also common themes, with girls describing unwanted and persistent online contact. In Sweden, participants reported that photo requests often appeared early in conversations and escalated to pressure to send photos. In Italy, girls described older men circumventing blocks with fake profiles and cases of emotional blackmail, such as ex-partners threatening suicide to manipulate girls into continued contact.

Some participants described coercion involving disturbing tactics, such as sending images of self-harm to compel compliance.

> **I think we've all noticed, either on TikTok or Instagram, a girl who posted photos and now there are messages you can write to someone when they post a story, which are anonymous, and the things people write to her in those messages are very nasty and have very disgusting content.**
>
> **(GIRL 16–18, CYPRUS)**

Cyber harassment (including cyberbullying)

Participants described cyberbullying and social exclusion as deliberate efforts to isolate, shame or humiliate victims, often in peer networks. This included exclusion from group chats, targeted gossip and the creation of online groups to ridicule specific individuals. Anonymous messaging on platforms like Instagram and TikTok was cited as a common vector for abuse.

> **I think we've all noticed, either on TikTok or Instagram, a girl who posted photos and now there are messages you can write to someone when they post a story, which are anonymous, and the things people write to her in those messages are very nasty and have very disgusting content.**
>
> **(GIRL 16–18, CYPRUS)**

Image-based cyber violence

The non-consensual creation, sharing or manipulation of intimate images was reported as a widespread and particularly damaging form of cyber violence. Participants described incidents involving deepnudes /

non-consensual synthetic intimate imagery, the secret recording of intimate moments and image-based blackmail – even participants from younger age groups.

> **She didn't want to date him, be in a relationship, and he literally made a deepfake of her, and he started just sending it around school.**
>
> **(GIRL 13–15, POLAND)**

One girl discovered her ex-partner had secretly photographed her during intimate moments, leaving her terrified by the knowledge that the images could resurface.

> **I was with a guy who I later found out had taken a picture of me when we had sex. It hasn't been shared but I'm still like this: 'he can keep it, he can keep it'. It's unsafe to know that it's there, because even if he deleted it, he could still have it on his phone.**
>
> **(GIRL 13–15, SWEDEN)**

Another recalled a case from primary school of image-based abuse and blackmail.

> **I had a classmate in primary school ... and someone took a picture of her, and it was really embarrassing, and he was threatening her that he would publish it if she didn't send him the homework or help him with the test and things like that, or money, even sometimes.**
>
> **(GIRL 13–15, CYPRUS)**

3.1. Where and how cyber violence happens: roles and interactions

Girls participating in the study described experiencing or witnessing cyber violence across a wide range of digital platforms (Table 1). They stressed that abuse was not isolated to a single site or app; instead, it adapted to the technical features, cultures and norms of each platform. In other words, the type of violence experienced was often shaped by what the platform enabled – whether anonymity, image-sharing, private messaging or real-time interactions.

Table 1 | Forms of cyber violence associated with different digital platforms according to focus group participants

Platform	Description of the platform	Forms of violence
Instagram	Social media platform focused on photo and video sharing, including stories and reels.	Harassment via DMs; exposure of private photos; hate pages.
Snaptchat	Multimedia messaging app known for disappearing messages, filters and short-form video content.	Unsolicited nudes; deepafakes; exposure account; suicide threats; offers of money for photos from unknown men.
TikTok	Social media platform centered on short-form video creation and sharing, popular for trends and music-based content.	Grooming; sexist memes/comments; pornographic content in comments; ' sugar baby ' solicitations(*).
Discord	Communication platform designed for voice, video and text chats, often used by gaming and interested-based communities.	Grooming by adult; emotional manipulation; requests for nudes.
Omegle	Online chat website that randomly pairs users for anonymous text or video conversations.	Repeated sexual flashing; coercive chat-based sexual interactions.
Gaming platforms (e.g. Valorant)	Interactive platforms where users play online multiplayer games, often with voice/text chat and competitive elements.	Sexist voice chat abuse; constant belittlement of girls.
Messenger /chats	Instant messaging apps used for realtime text, voice and video communication.	Harassment groups; AI-generated content for mocking.
Youtube Kids	Video streaming app offering curated, age-appropriate content for children, with parental controls and educational content.	Inappropriate content disguised as child-friendly videos.

(*) Sugar baby solicitations refer to situations where individuals – often adult men – approach younger girls or women with offers of financial and material support in exchange for attention or sexual favours. DMs; direct messages.

Source: Authors, based on focus group discussions.

Platforms such as Instagram, TikTok, Snapchat and WhatsApp were highlighted as the primary spaces where cyber violence occurs, from harassment and bullying to verbal abuse and the non-consensual sharing of intimate images. Participants also noted that each platform's design shapes the risks they faced, such as TikTok's public comment sections, Snapchat's disappearing messages and WhatsApp's group chats, which are used for gossip or exclusion.

Even platform features such as emojis, fake accounts and comment functions were understood as tools that could be used for bullying and harassment. Girls also expressed concern over algorithm-driven risks, particularly the rise of AI-generated deepfakes and manipulated content that reinforced sexist and violent norms.

On Instagram, girls reported receiving harassing messages through direct messaging, being targeted on hate pages and having private photos shared without their consent. Snapchat was described as a space where unsolicited nudes and deepfake images circulated widely, sometimes through exposure accounts ([27]). Some participants also recounted being pressured with threats of self-harm from perpetrators – such as threats of committing suicide – as a form of pressure or manipulation linked to image-based abuse.

TikTok was associated with a culture of normalised sexism. Grooming behaviours, body-shaming memes and sexualised trends were cited as common, alongside comments that objectified or humiliated girls. Some girls described encountering solicitations for 'sugar baby–sugar daddy' arrangements, suggesting that commercial forms of sexual exploitation were reaching younger audiences through the platform. Concerns were also raised about the lack of strict regulations on some social media platforms.

On other platforms, such as Discord, girls described being emotionally manipulated by older users through grooming and persistent pressure to send nudes. The platform's private and group chat features were seen as enabling prolonged, coercive interactions, often under the guise of shared gaming interests or community membership. Moreover, Omegle was described as a space of constant sexual exposure. Girls recounted being flashed or coerced into inappropriate chat exchanges by strangers, who were often adults.

> **"I was on this Omegle already with my friends on a sleepover … I connected with a guy like that. I'm like 'hey', 'where are you from', a conversation, and suddenly I'm 'wait, what are you doing?' … he put out his [genitals]. It's all the time!"**
>
> **(GIRL 13–15, POLAND)**

Other private messaging apps such as Messenger were also found to host harassment, with participants describing group chats that exist solely to target girls and the circulation of AI-generated content designed to mock or intimidate. Even platforms designed specifically for children were not exempt. On YouTube Kids, girls described encountering inappropriate or sexualised videos disguised as child-friendly, exposing them to harmful content at a very young age.

Online gaming environments, meanwhile, exposed girls to explicit sexism in their voice chats. Girls described being told to 'go back to the kitchen' or being belittled regardless of their gaming performance. Such experiences illustrate how gendered hostility remains deeply embedded in gaming culture.

27 Exposure accounts are social media profiles – often anonymous or unofficial – that are created and used specifically to publicly share personal, private or sensitive content about individuals, typically without their consent.

Profiles of and relationship to perpetrators

Unlike offline forms of gender-based violence, cyber violence against women and girls has the potential to involve a wider and more diverse array of perpetrators (Figure 8). This is largely due to the ease with which individuals can participate in online abuse and amplify its harmful effects (UN Women, 2024b). In this context, there are two main types of perpetrators: primary perpetrators and secondary perpetrators (UN Women, 2024b). Primary perpetrators are those who initiate and incite incidents of online gender-based violence. They are responsible for starting the harmful actions or content, whether through harassment, threats or explicit violence. Secondary perpetrators, on the other hand, are individuals who contribute to the spread of cyber violence against women and girls by downloading, forwarding or sharing abusive content, thereby amplifying its reach and impact.

The European Women's Lobby proposes a list of different types of online abusers ([28]). Perpetrators can be strangers to the victim, or they can be individuals from the victim's personal or professional circles, such as family members, friends or colleagues. A global meta-analysis of the offenders of online crimes against children provides estimations that, overall, 68 % of all perpetrators were family members or acquaintances of the victim. Furthermore, 44 % of perpetrators were under 18, suggesting a large proportion of peer-to-peer violence (Sutton et al., 2023). More dangerous and organised groups, such as sexual predators, traffickers, paedophilic networks and transnational criminal organisations, are also among the most significant categories of perpetrators in cases of cyber violence against women and girls (EWL, 2017).

While acts of cyber violence occur online, the underlying motivations for these actions stem from the offline world, influenced by emotional, psychological, ideological and cultural factors that shape the perpetrator's profile and behaviour (Cybersafe, 2020). Many young people (aged 12–18) often perceive perpetrators as victims themselves, describing them as lonely, weak or also experiencing violence. Family and relational dynamics – including parental monitoring, supervision and family conflict and support – also play a significant role in shaping the perpetration of cyber violence among young people (López-Castro et al., 2019).

Focus group discussions across participating Member States illustrate how these dynamics are experienced in practice.

FIGURE 7 | Perpetrators and associated forms of cyber violence, according to focus group participants

Strangers → Most sexual harassment on platforms like *Omegde, TikTok, Discord, Snaptchat*

Peers/classmates → Cyberbullying, revenge porn, stalking, exclusion, gaming abuse

28 See Table A.8 in the annex.

Current/former intimate partners → Grooming, coercive control, sharing private material after breakups, threats

Friends/ former friends → Betrayal, spreading rumours, participation in mocking chats

Older men (often unknown) → Grooming, sexual coercion, deepfake distribution, 'sugar daddy' offers

During the focus groups, girls consistently emphasised that cyber violence frequently originates within their social circles or intimate relationships. Cyberbullying and social exclusion typically involve classmates or peers, mirroring HBSC findings on peer perpetration. According to the HBSC Survey, the perpetration of cyberbullying peaks at age 13 for both boys and girls across most Member States and EU regions ([29]). Within the context of peer groups, peer norms and attitudes heavily influence actions. Power, popularity, status and perceived notions of masculinity emerge as possible motivations for participating in harmful behaviours online (Project deSHAME, 2017).

Intimate relationships also emerged as a central context in which cyber violence occurs: girls described experiences of image-based abuse, coercion and cyberstalking by romantic partners or former partners. Such cases illustrate how perpetrators exploit trust and intimacy to gain access to private material or to exert ongoing control.

> **"The person you are in a relationship with has a behaviour that you as a person do not like, you break up with that person, and they continue to write and to bombard you with messages. They do not accept this is over and continue to harass you. Or victimize [them]self and try to manipulate you to stay within the relationship."**
>
> **(GIRL 16–18, ROMANIA)**

3.2. The pervasive and normalised nature of cyber violence

Girls consistently described cyber violence as pervasive and inescapable, which is in line with research that demonstrates their disproportionate exposure to online abuse. Rather than viewing cyber violence as an isolated incident, girls described it as a pervasive and routine aspect of their digital lives. Many girls stated that almost every girl they knew had experienced some form of online abuse. Comment sections, group chats and direct messages were described as unsafe spaces where hate, mockery and judgement were commonplace. The anonymity of online spaces was frequently mentioned as a factor that emboldens perpetrators and allows harmful behaviour to occur without consequences.

29 See Figures A.13 and A.14 in the annex.

The focus group findings also revealed a shared understanding that girls are more frequently the target of cyber violence than boys. Girls described sexualised harassment, appearance-based insults, image-based abuse and social exclusion as particularly gendered forms of abuse. While girls acknowledged that other girls can also perpetrate harm – especially through exclusion, mockery or judgement – they were clear that boys were more often responsible for severe forms of abuse, such as coercion or sharing intimate images.

How peers respond to these incidents further compounds the harm. Victim blaming plays a key role in how young people respond to these forms of abuse. Girls fear being blamed for sending intimate images or videos, for example, which can prevent them from seeking help or reporting the abuse. This fear of judgement can be exacerbated by psychological factors such as self-blame, reputational concerns and shame (Mclocklin et al., 2024).

Online–offline intersections of cyber violence

Cyber violence rarely remains confined to digital spaces. Girls described a blurring of boundaries between the online and offline worlds, where harassment, threats and reputational damage originating on the internet frequently escalated into real-life situations or vice versa. In this regard, existing research suggests that, for children, experiences of cyber violence are often closely linked to offline bullying, especially within school settings (Chiang et al., 2021).

This overlap between digital and physical spaces was also evident in the girls' accounts, in which cyber violence was portrayed as a continuum that seamlessly shifts between platforms, relationships and environments. They shared many examples of online abuse leading directly to offline harm, such as digital monitoring escalating into physical stalking.

> **"I know someone who was going out in a group of friends and a friend of her boyfriend kept writing to her. And when she said, I'm not interested in being more than friends, he kept insisting. And she said I will block you and never speak to me again. And the guy actually came to throw stones in her window at night."**
>
> **(GIRL 16–18, ROMANIA)**

They also described how offline violence shifts into online spaces. Girls described situations where perpetrators, after engaging in face-to-face bullying or violence, continued their harassment through social media or messaging platforms.

> **"And then she decided to start posting videos on TikTok ... some people from her school found her and wrote negative comments all the time, and it went viral and everyone started making fun of her."**
>
> **(GIRL 13–15, CYPRUS)**

In other cases, initially online interactions laid the groundwork for offline harm, such as prolonged harassment and stalking.

> **Everything was fine for a few months, but then my friend had a lot of problems and had to go to counselling and see a psychiatrist because this guy would do anything to get her back, stalking her, sending her messages and trying to deprive her of everything.**
>
> **(GIRL 16–18, ITALY)**

The digital and offline overlap is also evident in cases of emotional manipulation, where online abuse extended into victims' daily lives and disrupted their routines.

> **He used to say to me that 'well if you don't write back to me, am I going to kill myself' and it was like he was, he was in a different time zone, so it often happened that I would stay up all night to talk to him, because I didn't want him to kill himself.**
>
> **(GIRL 13–15, POLAND)**

These accounts illustrate that young people do not experience online and offline life as distinct spaces but as interconnected ones, where online and offline forms of violence are deeply intertwined.

3.3. Young people's perspectives on intersectional risks in cyber violence

Qualitative insights drawn from the focus groups reveal the everyday realities of cyber violence and the social contexts shaping these experiences. Conversations with both girls and boys highlighted how individual identity factors, together with broader social, structural and cultural dynamics, contribute significantly to their exposure to and experiences of online abuse. These lived experiences echo the findings of the existing literature, which show that age, gender and other intersecting social vulnerabilities play an important role in girls' experiences of cyber violence.

Individual/identity-based factors

Focus group participants demonstrated a strong and nuanced understanding of how personal characteristics – such as race, gender, disability, appearance, religion and age – interact with social expectations and norms to increase their risk of exposure to online abuse.

Many described how online spaces replicate offline sexism, reinforcing patriarchal systems that undervalue and objectify women and girls. Posting personal content, especially images showing the body or those that do not conform to conventional beauty standards, was frequently linked to a heightened risk of receiving negative or sexualised comments. However, according to the girls, simply being visible or active on social platforms often invites unwanted attention and criticism.

For example, girls who do not meet traditional standards of attractiveness or who physically stand out were perceived to be more likely targets of shaming and objectification online. Several girls noted that

those who 'stand out from the crowd are more likely to get hate'. In this context, the beauty standards perpetuated online – often privileging thinness and white skin – lead to stigmatisation and the bullying of those who do not conform (Azzarito et al., 2017).

> **Women are not a minority, but they are still discriminated against for various reasons, and this is reflected online.**
>
> **(GIRL 16–18, ITALY)**

> **I have friends ... who have, for example, pictures in swimsuits. And all it takes is one such photo, and I have the impression that men feel that they are allowed to write.**
>
> **(GIRL 16–18, POLAND)**

Younger girls, especially those in early adolescence, were seen as particularly at risk due to their limited experience, lower digital literacy and greater susceptibility to peer influence or grooming.

Girls also highlighted how discrimination based on identity – such as LGBTIQ+ status – exacerbates risk. For example, one participant highlighted that transgender individuals, particularly trans women, often face delegitimisation and exclusion.

> **Transgender people are often treated differently ... told 'you're not a real woman'.**
>
> **(GIRL 16–18, GERMANY)**

This observation is supported by research showing that gender minorities within LGBTIQ+ communities often face stigmatisation and harassment, with cyber violence intersecting with racist, anti-LGBTIQ+ and transphobic abuse (Gius, 2023). Gender minorities report higher rates of online harassment, threats and sexual harassment (Gámez-Guadix et al., 2022; Vogler et al., 2023). More specifically, non-binary, genderqueer and transgender individuals encounter distinct risks and challenges compared to other minorities, underscoring the importance of more focused investigation in this area (Ray et al., 2024).

Disability was also noted as a significant factor increasing vulnerability. Girls shared that disabilities are often mocked through memes ([30]) or dehumanising humour and that people with disabilities are frequently pitied or devalued online. This echoes the FRA (2015) finding that women with disabilities experience higher rates of online threats and abuse.

30 A meme is an image, video, piece of text, or other type of content – typically humorous – that is copied and shared rapidly online, often with slight variations. In this context, focus group participants referred to memes created from images of individuals (often taken without their consent or from private content), which are edited, captioned or altered to mock, ridicule or harass the person and then circulated widely on the internet.

Racism was another prominent issue raised by focus group participants, particularly against those that may belong to a racial or ethnic minority in their community or country. Religion was also referenced as a basis for online hate directed at girls, particularly those who visibly express their faith.

> **I'm thinking specifically about people wearing the veil. They get a lot of hate online; it's very common.**
>
> **(GIRL 13–15, SWEDEN)**

These insights underscore that exposure to cyber violence is determined not only by individual behaviour, but also by the intersection of identity, visibility and entrenched social hierarchies.

Boys, on the other hand, pointed to individual traits and social positioning as factors that increase girls' exposure to cyber violence, suggesting that differences in appearance, personality, beliefs or social status made them more likely targets. They interpreted girls' online behaviours – particularly sharing content perceived as provocative – as attention-seeking or driven by a psychological need for validation. Meanwhile, perpetrators were commonly viewed as socially marginalised 'losers', acting out of boredom, for revenge or with a desire to assert dominance. This complements research showing that peer dynamics, social marginalisation and power imbalances are key drivers of cyberbullying and harassment (Baas et al., 2013; Project deSHAME, 2017).

Boys' explanations of the cyber violence affecting girls reflected an awareness of cultural norms, patriarchal attitudes and gender stereotypes. Many acknowledged that societal figures and public discourse promote misogyny, creating a culture that normalises male dominance and shifts responsibility on girls, particularly in cases of image-based online abuse. However, many expressed victim-blaming attitudes, with some boys holding girls accountable for the abuse, especially when they posted 'provocative photos'. However, a minority rejected this victim-blaming attitude, recognising that perpetrators bear the responsibility. Boys' explanations and justifications reinforce the literature on normalisation and double standards, which is where male perpetrators are often excused while female victims are blamed, highlighting systemic gendered power imbalances (EIGE, 2025).

> **Some girls post provocative photos of themselves online, and someone might grab them and do whatever they want with them and then comes the blackmail and everything else we mentioned earlier.**
>
> **(BOY 15–18, CYPRUS)**

Boys also perceived girls to be 'easier targets' due to assumptions about their emotional sensitivity or naivety, while less socially visible girls were seen as being less at risk, linking exposure to visibility and social participation.

Gender norms and stereotypes further shape how boys experience and respond to cyber violence. Fear of social exclusion discouraged boys from speaking out, especially when they were being bullied by girls, and parental reactions often reinforced expectations of toughness.

> **They'll say, 'You're a man and you care what they say about you?' Like, if you tell your dad, 'He hit me', he'll just say, 'Hit him back'. That's how it is!**
>
> **(BOYS 15–18, CYPRUS)**

Social, structural and cultural factors

Beyond individual traits, many girls pointed to wider structural and cultural factors that foster a permissive environment for cyber violence. They stressed that this violence is not the result of isolated online actions but deeply rooted in social norms that blame girls for abuse while excusing or rewarding boys who perpetrate it.

Gender and cultural norms

Across all focus groups, boys highlighted how dominant norms of masculinity shape boys' online behaviour. A strong pattern emerged, showing that boys often engage in cyber violence to gain validation and social approval from peers. Acts like non-consensual image sharing or group harassment were framed as performances to impress others or conform to peer expectations. In this context, girls are treated as 'trophies to show off to your friends' and 'having had lots of girlfriends is seen as being an alpha male, a strong male'. These peer-driven dynamics reflect the literature on adolescent risk-taking, social hierarchies and exposure to sexualised interactions online (Project deSHAME, 2017).

Possessing or sharing intimate images is often treated by boys as a symbol of power and status, while the girls involved are shamed. The logic of 'sexual conquests' and objectification was identified as a central driver of online abuse.

Younger girls, especially in Sweden, showed considerable awareness of the role of men's demands in online sexual exploitation, challenging victim-blaming narratives. This perspective aligns closely with Sweden's legal approach to the issue, which criminalises the purchase of sexual services.

Sexualisation and exploitation

Girls across Member States linked cyber violence to wider systemic issues such as the pornography industry and the early sexualisation of girls. Early exposure to pornography, especially when occurring in the context of limited age-appropriate and comprehensive sexuality education, can shape boys' perceptions of women, and often negatively. This supports evidence on there being systemic drivers of sexualised online abuse and adolescents' exposure to sexual content (Smahel et al., 2020).

> **I think it's also very much down to the internet that women have become so easily accessible. The pornography alone ... the fact that boys look at it at such an early age, that's really scary. And the fact that their view of women changes completely.**
>
> **(GIRL 13–15, GERMANY)**

Normalisation and double standards

A recurring theme was the widespread minimisation or dismissal of boys' harmful online behaviours. Peers, adults and institutions often excuse these actions as immaturity or jokes, contributing to a culture where such violence is normalised when perpetrated by men but considered a serious issue when exercised by women. Both girls and boys consistently described how girls who experience cyber violence are often judged, ridiculed or held responsible for the abuse, while boys are excused – or in some cases even praised – for the behaviour.

> **When boys do it, it's like 'oh, they're just having a laugh'.**
>
> **(GIRL 13–15, IRELAND)**

> **If a boy shares a photo, he's considered cool. If a girl does it, she's done something wrong.**
>
> **(GIRL 16–18, ITALY)**

Several girls reflected on how some boys' aggression in online spaces may stem from insecurity, emotional immaturity or fear of rejection. In these cases, cyber violence was perceived to be not only a way to impress peers but also a means to assert control or mask personal vulnerability. Others, however, described such actions as deliberate and malicious, particularly in situations involving break-ups or perceived rejection.

Girls also highlighted the role of certain online subcultures and influencers in shaping misogynistic attitudes. Spaces such as incel forums ([31]) were described as echo chambers that channel men's frustration and sense of rejection into hostility towards women, reinforcing harmful stereotypes and legitimising abusive behaviour.

While many girls strongly rejected the notion that victims are responsible for their own abuse, a few expressed more ambivalent views. These participants stressed that although girls are not to blame, they should be aware of the potential risks. Such perspectives illustrate the tension between rejecting victim-blaming narratives and recognising how social norms shape perceptions of 'risk' and responsibility.

31 Incel forums are online communities where individuals who identify as 'involuntary celibates' (incels) share frustrations about their perceived inability to form romantic or sexual relationships. These spaces often include content expressing resentment and, in some cases, hostile or misogynistic views.

Relationships as high-risk contexts

Finally, romantic and intimate relationships were repeatedly identified as high-risk contexts for cyber violence. Girls described experiences involving emotional manipulation, coercion into sharing intimate images and a betrayal of trust when those images were later shared or used for blackmail. This dynamic is exacerbated by the tendency of some young people to interpret controlling or aggressive online behaviours as signs of affection or attention, inadvertently normalising abuse (Lu et al., 2021). Such misinterpretations can delay help-seeking and contribute to under-reporting.

> **A lot also has to do with manipulation. How much the boy really wants something from her and how much he manages to get her under his claws and then really just works towards that and then just drops her afterwards.**
>
> **I also think that in a relationship it gets worse or more difficult, because then you have these 'rose-coloured glasses' … and then this complete trust, which makes it more difficult to realise that it's not trust or that he doesn't deserve trust.**
>
> **(GIRLS 16–18, GERMANY)**

Girls explained that trust and emotional dependency within relationships can make it hard for girls to resist coercion or recognise harmful behaviours. Violence in relationships was often seen as 'normal', difficult to identify ('you're so blinded') or excusable. There is, indeed, a mixed understanding among young people about what constitutes acceptable behaviour during cyberdating; some consider technology-facilitated intimate partner violence to be a 'relationship issue' rather than a form of violence. This echoes the current debate on what is 'normal' and what is not ([32]).

Break-ups were frequently identified as a critical flashpoint, often triggering acts of revenge such as the non-consensual sharing of private and often intimate images, including AI-created imagery; ongoing harassment; or public shaming. These patterns underscore how online abuse is deeply tied to power, control and the enforcement of gendered norms – even, and especially, within intimate relationships.

Perspectives from boys

Peer group dynamics emerged as a central driver of cyber violence. Boys explained that engaging in harassment can elevate one's social standing, particularly when high-status boys set the tone for abusive behaviour. This can foster a 'mob mentality' in which loyalty to the group is valued above individual relationships.

Masculinity norms and peer pressure were cited as consistent drivers of abuse. Online harassment – particularly mocking girls or sharing intimate images – was often framed as a way for boys to demonstrate toughness, prove their masculinity or gain peer approval. Opting out of such behaviour could be seen as 'less masculine', making participation a means to 'prove they're more manly'.

32 For more information, please see https://vision.city.ac.uk/news/tech-facilitated-abuse-and-the-new-normal/.

These dynamics were further shaped by gendered double standards and underlying homophobia. Participants pointed out that identical behaviours – such as posting revealing photos – were judged differently depending on the person's gender. Girls were labelled provocative, whereas boys were mocked or ridiculed. Some male participants demonstrated an awareness of broader systemic inequalities, but this recognition often coexisted with persistent victim-blaming attitudes.

> **Well, you post a naked photo online and expect a different response from people?**
>
> **(BOY 15–18, CYPRUS)**

Overall, the discussions revealed how deeply entrenched gender norms, double standards and power imbalances sustain a culture where cyber violence is normalised, responsibility is frequently shifted onto girls and perpetrators face little accountability.

3.4. Role of bystanders and peer influence

Bystanders play a crucial role in reducing the impact of cyber violence on victims. Intervening is recognised as a key strategy to combat this type of violence and mitigate its harmful effects. Offering direct support, such as comforting victims, can help reduce the emotional harm they experience. Indirect support, like reporting incidents to the authorities, can reduce the prevalence of harmful content online and promote positive actions among internet users (Rudnicki et al., 2023).

Despite this potential, many bystanders remain passive when encountering online hate. Research on cyberbullying reveals that approximately 50–90 % of adolescents have, at some stage, been a passive bystander to cyberbullying, failing to intervene in response to this type of abuse (Allison et al., 2016). Moreover, bystanders are more likely to act if they feel a connection to the victim and perceive the situation to be safe, which ensures that they will not become targets themselves.

Without these conditions, bystanders are less likely to take action and may even contribute to the spread of cyber violence.

Domínguez-Hernández et al. (2018) identified a range of factors that influence whether young bystanders (under the age of 20) choose to intervene in cyberbullying situations ([33]). These include contextual factors (e.g. friendships, social norms, incident severity, fear of retaliation and bystander dynamics) and personal factors (e.g. empathy, moral disengagement, self-efficacy and past experience). Similar themes emerged in the focus groups conducted with boys, who expressed complex attitudes, discussed dilemmas they had faced and made justifications about their roles as bystanders to cyber violence against girls. Three recurring patterns emerged: passive bystanding and avoidance as a form of self-preservation, peer norms that discouraged intervention and limited confidence in the effectiveness of taking action.

Passive bystanding and avoidance

Many boys described themselves as passive observers, often choosing to 'just watch' or record incidents rather than intervene – especially when the victim was a stranger. Fear of retaliation or of escalating the situation also influenced avoidance.

33 The key findings from their study are summarised in Table A.9 in the annex.

Boys often expressed the belief that victims should resolve issues themselves, particularly if they were not close friends. Such responses suggest a tendency to frame cyber violence as a personal issue rather than a collective responsibility, reinforcing patterns of victim blaming. Peer pressure and group dynamics also strongly shaped bystander behaviour. Many participants feared social exclusion or ridicule if they acted against the group. Some boys reported offering discreet support – such as private messages – rather than public intervention.

> **If you saw all your classmates just, like, seeing this and not doing anything, you wouldn't want to be the odd one out.**
>
> **(BOY 15–18, IRELAND)**

Low faith in bystander intervention

Overall, boys expressed scepticism about the effectiveness of intervening to stop cyber violence against girls. Many felt that taking a stand would expose them to criticism. Others emphasised a lack of motivation when they did not personally know the victim. These findings find echo the existing literature on bystander behaviour and masculinities in online settings. Research shows that male peer groups often discourage intervention when witnessing online abuse because taking a stand can threaten one's social status or masculine identity (Connell, 2005; DeKeseredy et al., 2013). Studies on cyber violence further suggest that digital environments amplify these social risks: intervening against sexist or aggressive content can expose boys to ridicule or retaliation from their peers (Powell et al., 2017). Moreover, empirical evidence indicates that empathy and personal connection to the victim are crucial motivators behind bystander action – when these are absent, the likelihood of an intervention taking place in cyberbullying or online harassment decreases significantly (Barlińska et al., 2013). Together, these studies highlight how peer norms, the fear of social repercussions and emotional distance shape boys' reluctance to intervene in instances of cyber violence against girls.

> **Miss, I've got my own problems, I'm not going to sit and deal with other people's issues.**
>
> **(BOY 15–18, CYPRUS)**

Several boys also believed that simple appeals to peers to stop their behaviour are ineffective, as 'People aren't going to listen if you just say, oh, stop or whatever. Words aren't going to do much'. However, some participants recognised that peer influence – especially from a male friend or older brother – could be effective in discouraging harmful behaviour, particularly at an early stage.

Some boys also acknowledged the potential value of reaching out to victims privately. While such actions show empathy, they also reflect a reluctance to challenge harmful behaviours publicly.

4 Effects of cyber violence

4.1. Impacts of cyber violence and social dynamics

While cyber violence can impact anyone, women and girls are disproportionately affected, often enduring more severe and traumatic forms of violence that result in long-lasting effects on their behaviour, emotions, mental health, physical well-being and social interactions. The consequences are no different from those of offline harassment, bullying and stalking, but have stronger negative impacts (EWL, 2017).

For girls and young women, the psychological impacts of cyber violence against women and girls are particularly severe. Adolescents targeted by cyberbullying frequently report depression, anxiety and tendencies towards self-harm (Nixon, 2014). Younger victims often report feelings of sadness, hopelessness, anger and fear, with some studies suggesting that cyberbullying may be even more stressful than traditional bullying due to the anonymity of the perpetrators and the pervasive reach of online platforms (Sourander et al., 2010).

Different forms of cyber violence result in varying levels of harm, with visual content like pictures and videos causing the most severe psychological effects (Nixon, 2014). Cyberbullying also disrupts social relationships, contributing to isolation, diminished trust, loneliness and reduced self-esteem (Sciacca et al., 2023). These challenges are exacerbated by victims' reluctance to report or seek help, which is driven by fear of judgement, uncertainty about outcomes and doubts about how adults might respond (Project deSHAME, 2017). Indeed, whether young people seek help or try to handle things on their own depends on several factors: whether they recognise the behaviour as abusive, whether they know about the support available and whether they believe that family, schools or digital platforms can actually help. In practice, many young people only reach out after the abuse has caused significant harm – emotional, reputational, physical or financial (Freed et al., 2025). Other studies have also underlined the need for tools and policies to mitigate the harm of cyber violence and improve help-seeking (Janickyj et al., 2025).

European data confirms the effect on well-being of the heightened exposure of girls and young women to online harm compared to boys and young men. As shown in Figure A.11 in the annex, in all studied Member States except Lithuania, a significantly higher proportion of girls report harm ([34]) – with an average gender difference of 19 percentage points.

34 In the context of this project, 'harm' refers to the level of distress or upset experienced by the surveyed child or teen.

Age patterns show less consistency (see Figure A.12 in the annex). In countries such as Lithuania, Malta and Poland, older children report higher levels of harm, while in others, like Czechia, Estonia, Portugal, Romania and Slovakia, younger children are more affected.

4.2. Young people's voices on the consequences of cyber violence

Focus group discussions with girls confirmed these trends. Girls described the impact of cyber violence using emotionally charged terms such as 'depression', 'suicide' and 'trauma', reflecting their awareness not only of immediate harms but also of long-term emotional consequences. Boys echoed these terms, recognising the sadness, insecurity and desperation victims often feel. The fear of reputational damage emerged as particularly acute for girls and young women, who are frequently judged more harshly than boys in similar situations (Project deSHAME, 2017).

Emotional and psychological distress

The most pervasive theme emerging from the focus groups was the emotional and psychological impact of cyber violence. Participants described cyber violence as not only harmful in the moment but also having lasting effects on mental health and social interactions.

Girls frequently expressed feelings of sadness, fear, anxiety, insecurity and worthlessness, especially when responding to harassment, bullying or image-based abuse. Emotional distress was often compounded by self-blame and shame, which made seeking support or speaking out even more difficult.

> **"I know a girl that some people, mostly boys, were sending weird messages to ... saying that they wanted to see her face and she actually sent people her face and everything and she was feeling really bad and started covering her face everywhere. This created a huge impact on her life and eventually led to her being depressed and she couldn't go to school."**
>
> **(GIRL 16–18, CYPRUS)**

Some girls shared stories of peers experiencing severe distress, including suicidal thoughts, self-harm and depression, often following public exposure or online shaming. Appearance-based bullying, particularly regarding body weight or shape, was cited as especially harmful in fostering relentless scrutiny, often from anonymous perpetrators.

Loss of trust and social isolation

Another key consequence of cyber violence identified by the participants was a loss of trust, particularly towards peers, intimate partners and online communities. Victims often described emotional withdrawal and wariness towards future interactions.

Cyber violence can also lead to social isolation and peer rejection. One participant suggested that when private images are shared without consent, the victim is no longer seen as a full person but is instead reduced to the content of those images. As a result, peers may actively withdraw, reinforcing exclusion.

> **I think she'll probably be reduced to just that ... and people will actually forget who she really is. But then it will really just be, these are the photos, that it's her body, not her anymore.**
>
> **(GIRL 16–18, GERMANY)**

Digital exclusion

Cyber violence can restrict girls' participation in social and civic digital spaces. Harassment and sexist backlash often lead to them withdrawing from online gaming, political debates, content creation and other interactive spaces. In many cases, the threat of abuse is enough to silence their voices or deter them from engaging in online spaces. In some cases, victims resorted to uninstalling apps or even changing schools to escape harassment.

> **You want to start playing games, but you can't play games because you're met with sexist comments. You just want to act in politics, but you are met with ... threats sent simply on your social media. You want to act, but you are met with heckling. You want to run for campaign, but someone creates a trolling account for you ... The question is whether it's worth it. So, for me it just boils down to such an attempt to exclude.**
>
> **(GIRL 16–18, POLAND)**

Normalisation of violence

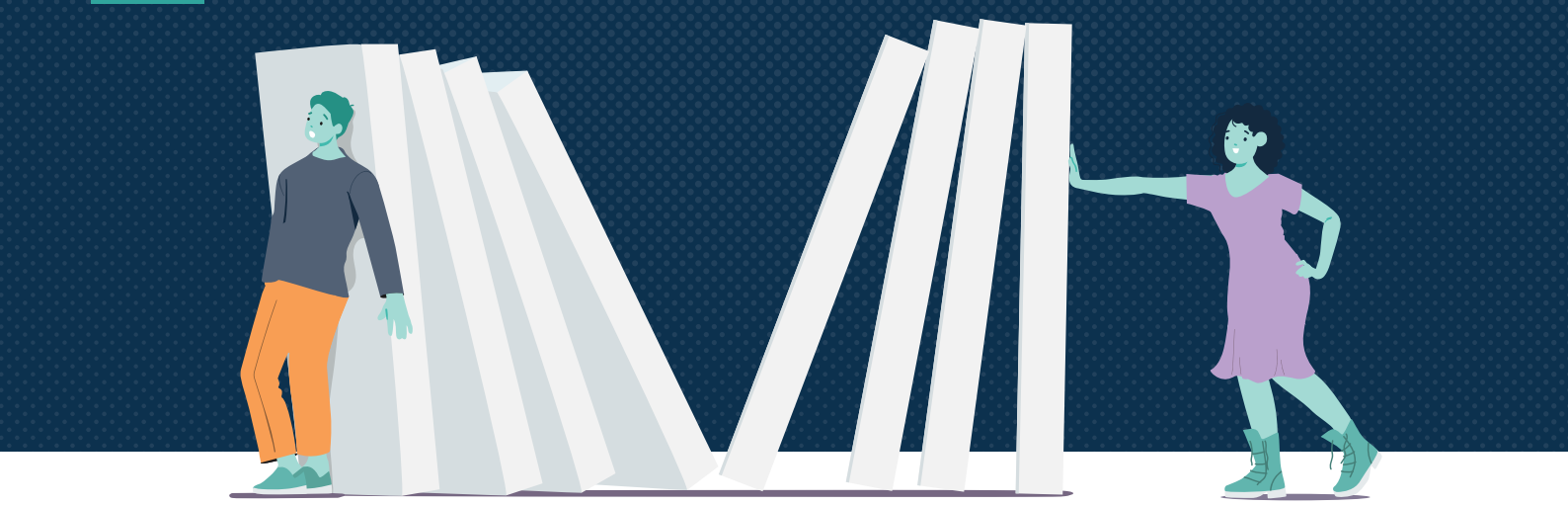
A subtle yet significant impact identified by focus group participants was the normalisation of harmful behaviours. Many girls observed that frequent exposure to cyber violence can lead to desensitisation, reducing the perceived seriousness of certain forms of abuse as younger generations learn to not 'take [it] that seriously'.

Several participants said they had grown up aware of both online and offline risks. They recalled being taught from an early age to be cautious. Despite this awareness, some girls expressed a sense of resignation, viewing cyber violence as inevitable and, therefore, seeing a need to adapt to this reality. This sentiment was voiced strongly in Belgium, where participants described cyberbullying as a 'part of life' and nearly impossible to escape.

> **Honestly, I don't think we can do much. The system is like that. To avoid it, you just have to blend in and disappear. Once it's over, it's over. It's a phase of life – you go through it and move on.**
>
> **(GIRL 13–15, BELGIUM)**

The enduring nature of online abuse was another major source of fear and anxiety. Participants described how harmful content – such as private photos – can resurface at any time, creating a persistent sense of vulnerability and threat. They noted that the same image or message might reappear in a different group chat or context, leaving them feeling powerless to prevent re-exposure.

5 Preventing and addressing cyber violence



5.1. International and EU frameworks addressing cyber violence against women and girls

While the EU does not have a standalone legal framework dedicated exclusively to gender-based cyber violence, recent progress includes the adoption of the aforementioned Directive (EU) 2024/1385 (Violence against Women Directive), which criminalises four main forms of cyber violence: the non-consensual sharing of intimate or manipulated materials, cyberstalking, cyber harassment (including cyberflashing ([35])) and cyber incitement to violence or hatred.

Set to be transposed by June 2027, this directive marks a significant milestone in addressing cyber violence: it explicitly recognises cyber violence as a form of gender-based violence and requires Member States to adopt preventive measures, to develop accessible and secure ICT reporting channels, to take suitable measures to ensure the takedown of content related to the offence, to provide specialist victim support services, to facilitate access to justice and to ensure coordination and cooperation between authorities. It also encourages Member States to ensure that their national procedures stay up to date with technological developments. This directive is a historic step as it requires all Member States to criminalise various forms of cyber violence.

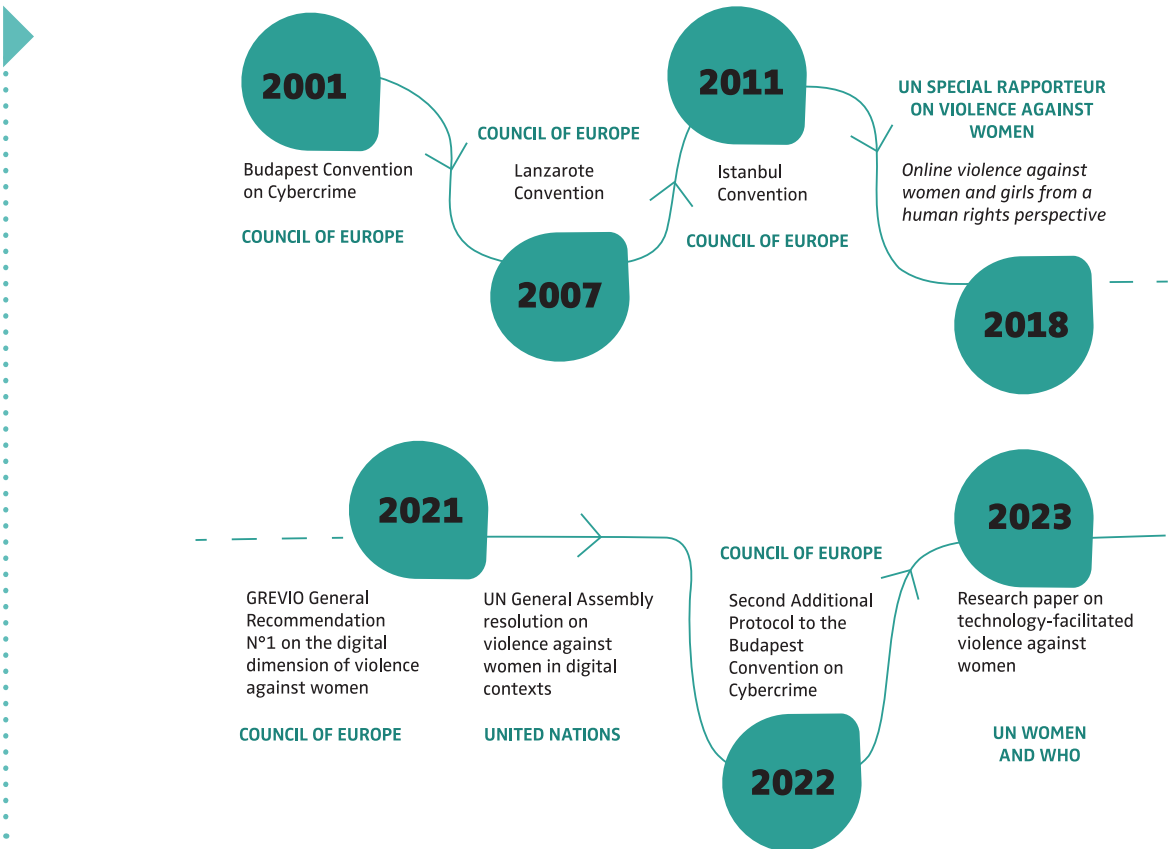
The evolution of EU policy reflects a growing awareness of the intersecting vulnerabilities of women and girls, which are shaped by factors such as age, ethnicity and socioeconomic status. Throughout the EU's broader regulatory landscape – which covers data protection, online content moderation, victim support mechanisms and child protection strategies – Directive (EU) 2024/1385 serves as the central framework that connects these initiatives, harmonising measures across Member States to criminalise and prevent cyber violence, protect victims and promote accountability online. Thus, while EU legislation does not take the form of a single, unified framework on cyber violence, a combination of binding and non-binding mechanisms has been used to address the issue comprehensively.

35 Cyberflashing is defined in the directive as 'the unsolicited sending of an image, video or other similar material depicting genitals to a person' ([recital 24]).

5.1.1. International frameworks addressing cyber violence

At the international level, several key instruments ([36]) provide standards and guidance that have shaped EU actions. UN documents, including the 2018 Report of the Special Rapporteur on Violence against Women Its Causes and Consequences on online violence against women and girls from a human rights perspective and UN Women and the WHO's 2023 research paper on technology-facilitated violence against women, emphasise international cooperation, platform accountability, victim-centred remedies and the inclusion of diverse perspectives during evidence collection and policymaking. The Council of Europe has advanced relevant frameworks such as the Istanbul Convention (2011), which explicitly addresses online abuse; the Budapest Convention on Cybercrime (2001) and its 2022 Second Additional Protocol, which enable cross-border cooperation in prosecuting cyber offences; and the Lanzarote Convention (2007), which protects children from sexual exploitation, including in digital spaces. In addition, Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) General Recommendation No 1 on the digital dimension of violence against women (2021) highlights the importance of national action plans, digital literacy and specialised training for law enforcement and judicial personnel on cyber violence. Together, these instruments provide guidance for prevention, policy development and the provision of support services.

FIGURE 8 | Timeline of examples of leading international legal and policy instruments addressing cyber violence



Source: Authors.

In November 2025, the Council of Europe approved a recommendation on accountability for technology-facilitated violence against women and girls ([37]).

36 Please see Figure 9 below. Detailed descriptions of examples of international instruments are provided in Table A.1 in the annex.
37 'Approval of key instrument on accountability for technology-facilitated violence against women and girls' – Gender Equality Commission.

5.1.2. EU regulatory developments on gender-based cyber violence

The EU has progressively strengthened its regulatory framework to address gender-based cyber violence, drawing on a wide range of legal and policy instruments .

Adopted in 2018, the General Data Protection Regulation (GDPR) has strengthened individuals' rights over their personal data and has established safeguards against its misuse. It has also provided for the personal right to request the removal of harmful or non-consensual personal content that has appeared online. While its privacy-based protection has been frequently used by victims of cyber violence, the effects of its provisions in successfully addressing gender-based forms of online abuse have been found to be limited (European Parliament Directorate-General for Parliamentary Research Services, 2024). More recently, the Digital Services Act (DSA) and the Artificial Intelligence Act (2024/1689)) have strengthened online safety by introducing stricter content moderation rules, enhanced victim protections and transparency requirements regarding the use of AI, including deepfake technologies. These advances demonstrate a growing recognition of the issue of cyber violence and the need for coordinated action across Member States.

Victim protection measures are equally important. The Victims' Rights Directive (2012/29/EU), currently under revision, sets minimum standards for support services, while the EU strategy on victims' rights (2020–2025) highlights the need for stronger protections in cases of cyber violence. Complementing this, the gender equality strategy (2020–2025) explicitly calls for tackling online gender-based violence.

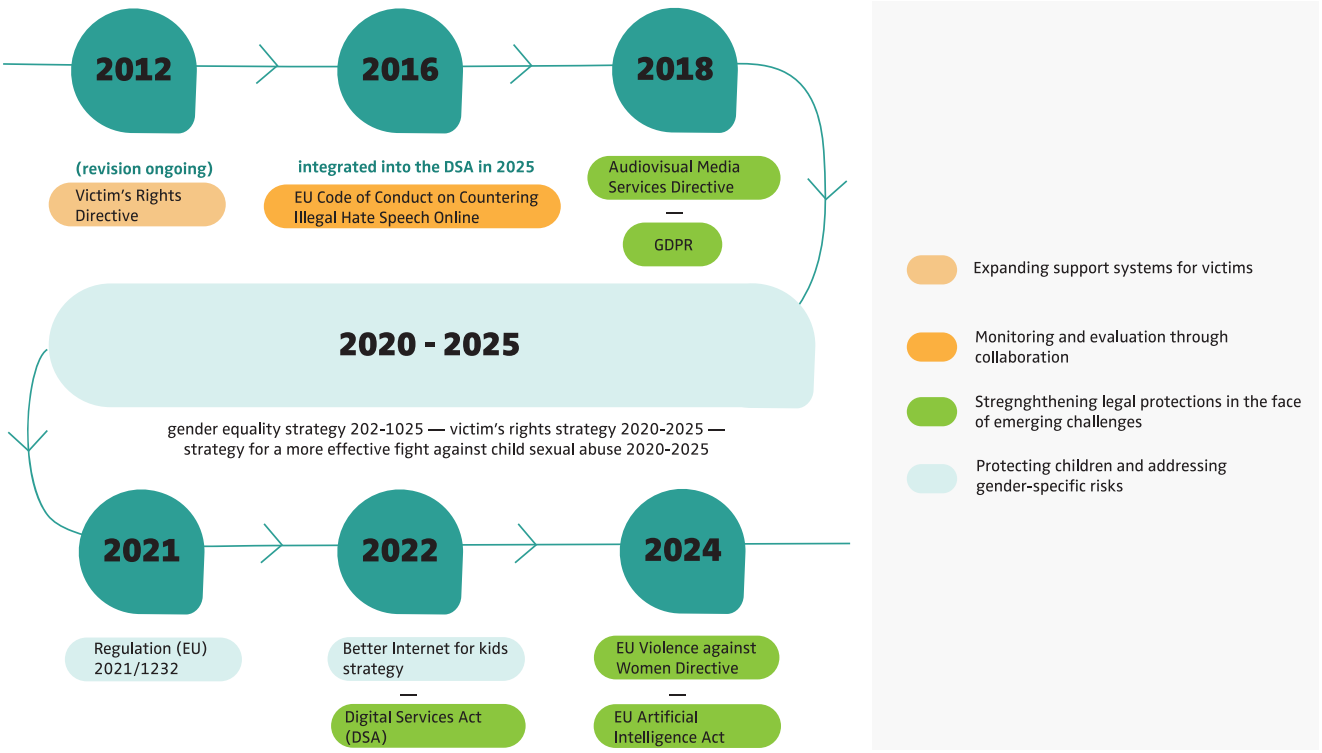
Child protection instruments also play an important role. Directive (EU) 2011/93 on combating the sexual abuse and sexual exploitation of children and child sexual abuse material, the primary legal instrument in this area, is under revision to reflect technological advances since its adoption in 2011 (European Parliament Directorate-General for Parliamentary Research Services, 2024). Regulation (EU) 2021/1232 enables providers to detect and block child sexual abuse material, while the EU strategy for a more effective fight against child sexual abuse (2020–2025) and the better internet for kids strategy strengthen online safety for children. The proposed EU Centre on Child Sexual Abuse further aims to centralise resources and improve victim assistance.

Alongside these frameworks, initiatives addressing hate speech play an important role. The 2016 EU Code of Conduct on Countering Illegal Hate Speech Online – recently integrated into the DSA (in 2025) – reinforces commitments made by major platforms to address hate speech and adopt best practices. Similarly, the Audiovisual Media Services Directive (2018/1808) includes provisions against hate speech and enhances protections in online media environments.

The adoption of Directive (EU) 2024/1385 (Violence against Women Directive) in 2024 constitutes the most recent and significant legislative commitment to combating cyber violence against women and girls. It requests that Member States criminalise cyber violence by setting minimum standards for the criminalisation of the four main forms of cyber violence, which are the non-consensual sharing of intimate or manipulated material, cyberstalking, cyber harassment and cyber incitement to hatred or violence.

This leaves open the possibility of Member States developing stricter national rules and penalties. The transposition of the directive is likely to address one of the most persistent challenges in developing an EU-wide approach to tackling cyber violence, namely the lack of harmonised definitions across Member States and jurisdictions (EIGE, 2025 p. 66). This is because it also requires Member States to collect data on these four forms of cyber violence, thus paving the way towards comparable data across Member States. To facilitate this process, EIGE was specifically tasked with establishing common standards and supporting Member States with the collection of comparable and standardised administrative data (EIGE, 2025).

FIGURE 9 | Timeline of examples of main EU regulatory developments on gender-based (cyber)violence as of December 2025



Source: Authors.

5.2. National approaches in Member States

Across the EU, national responses to gender-based violence and cyber violence vary considerably, reflecting the different legal frameworks, cultural contexts and technological capacities of its Member States. In most Member States, general criminal offences – such as harassment and stalking – cover both physical and digital forms of violence, including cyber harassment and cyberstalking. Legal precedents have extended these traditional definitions to online contexts. However, when cyber violence is addressed in terms of these general offences, cyber violence often lacks gender-specific language and rarely makes explicit reference to women.

While few Member States have laws specifically targeting cyber violence against women and girls, legislative efforts are under way in many Member States to introduce such tailored provisions. In most cases, national laws currently rely on general criminal offences like harassment and bullying, which are supplemented by broader definitions and civil protections.

5.2.1. Legal approaches across the EU

Member States have adopted different legislative approaches to address cyber violence. These include creating dedicated cyber violence laws, integrating cyber-specific offences into existing legislation or

embedding protection within broader frameworks on privacy or violence against women. Many Member States combine these approaches, resulting in mixed legal systems.

The 2022 EIGE study on combating cyber violence against women and girls (EIGE, 2022) classifies national legal approaches into three categories: those treating cyber violence as a distinct offence, as an aggravating factor or as a part of general offences. It also identifies national laws that explicitly mention women, girls or children and reviews national policies on cyber violence that include targeted protections for these groups.

Building on that study's findings, three main types of approaches have been identified, as discussed in the subsections below. The analysis reveals a proactive shift among Member States towards victim-centred approaches, cross-border cooperation and the inclusion of digital safety in broader strategies against violence and cybercrime. In addition, Table A.3 in the annex provides detailed examples of national case law related to cyber violence.

CREATING SPECIFIC CYBER VIOLENCE LAWS

Some Member States such as Belgium, Denmark, France and Portugal have adopted standalone laws or provisions that directly criminalise different forms of cyber violence. These include measures against cyberbullying, school and university harassment, image-based sexual abuse and the non-consensual sharing of intimate content. They have also introduced obligations for online platforms to remove harmful content, facilitate user reporting and preserve digital evidence. Table 1 contains examples of these sorts of measures.

Table 2 | Examples of cyber violence-specific legislation at the national level

Member State	Name of the measure and year	Description
Belgium	Law aimed at combating the non-consensual distribution of sexually explicit images and recordings (4 May 2020)	The law extends the competency of the Institute for the Equality of Women and Men to take legal action and assist adult victims of digital sexual violence, including victims of non-consensual image distribution, sextortion and deepnudes. The institute provides advice and support in removing non-consensual images. To this end, it works together with internet platforms such as Meta, Google and Pornhub, the platform stopncii.org and the federal police. Another institution, Child Focus, is responsible for underage victims.

Member State	Name of the measure and year	Description
Denmark	Danish Penal Code, Article 264d	Article 264d criminalises the non-consensual sharing of intimate images or videos, which is punishable by up to three years' imprisonment, with harsher penalties for cases involving minors or mass distribution. Although gender-neutral, it targets abuse that disproportionately impacts women and girls.
	Danish Penal Code, Articles 225, 231 and 242	Article 225 criminalises sextortion, Article 231 criminalises grooming and Article 242 criminalises stalking.
France	Law No 2020-766 aimed at combating hateful content online (Avia Law)	The law required platforms to remove explicit illegal content (e.g. hate speech, child pornography) within 24 hours, with penalties for non-compliance. The Constitutional Council later declared key provisions of the law unconstitutional, citing concerns related to freedom of expression. Its remaining provisions led to the creation of a public prosecutor's office for online hate and an Online Hate Observatory within the Autorité de regulation de la communication audiovisuelle et numérique (Arcom).
	Law No 2022-299 aimed at combating school bullying	The law criminalises school/university bullying (including cyberbullying), with the punishment being a fine of up to EUR 150 000 and 10 years in prison. It provides for the collection and preservation of digital evidence in relation to cyber offences.
	Law No 2023-566 aimed at establishing a digital majority and combating online hate speech	The law creates obligations for platforms to facilitate the reporting of content that infringes upon personal rights and to provide preventive information to users.
	Law No 2024-449 on securing and regulating the digital space (SREN Act)	The law regulates digital spaces, focusing on protecting citizens, particularly minors, from harmful content and combating cyber harassment, sextortion, online scams, hate and disinformation. The law introduces a new offence relating to sexual deepfakes. The punishment is two years' imprisonment and a fine of EUR 60 000 for disseminating a sexual deepfake publicly or to a third party without the person's consent. Sanctions increase this to three years' imprisonment and a EUR 75 000 fine if it was published using an online public communication service. The law also mandates the use of age verification systems on pornographic websites, with a penalty of heavy fines and site blocking if this is not implemented. This law entered into force in June 2025 and applies to all major pornographic websites.

Member State	Name of the measure and year	Description
Portugal	Article 193 of the Penal Code of Portugal, 2023	Law No 26/2023 of 30 May amended the Penal Code of Portugal by altering Article 193 to criminalise the non-consensual sharing of personal images through media, the internet or other means of widespread public dissemination. It provides that anyone who, without consent, disseminates or contributes to the dissemination of images, photographs or recordings that invade a person's private life, including the privacy of their family or sexual life, may be punished with imprisonment for up to five years, thereby strengthening legal protection against the non-consensual sharing of intimate content online. The same law also amended Article 197 to provide for aggravating circumstances; penalties for certain crimes are increased by one third if the offence is committed through social media, the internet or other widespread digital dissemination.

EXPANDING EXISTING CRIMINAL CODES TO ADDRESS CYBER VIOLENCE

Other Member States have adapted pre-existing criminal provisions to cover online contexts (see Table 2). This is the case in Member States such as Germany, Ireland, Italy, Austria, Poland, Romania and Finland ([38]). Offences such as stalking, harassment, grooming, defamation and hate speech have been extended to include digital environments. Amendments in this area often recognise cyber violence as a part of gender-based violence or domestic violence, enabling courts to impose greater penalties and protective measures when cases involve intimate partners or minors. This approach provides legal continuity and consistency but can lead to ambiguities, as offences are not always explicitly defined as being cyber-related, resulting in variable enforcement and limited gender sensitivity.

Table 3 | Examples of national legislation extended to cover cyber violence

Member State	Name of the measure and year	Description
Belgium	Article 417/8 and Article 417/9 of the Belgian Penal Code	The Belgian Penal Code criminalises the creation and distribution of deepnudes without consent. Creating a deepnude without the person's consent is considered a form of voyeurism (Article 417/8), while distributing a deepnude constitutes the non-consensual distribution of content of a sexual nature (Article 417/9 of the Belgian Penal Code).

38 In Finland, criminal provisions are neutral from a technological perspective; that is, their implementation does not depend on the means used.

Member State	Name of the measure and year	Description
Germany	Network Enforcement Act (NetzDG), 2017	This act mandates the rapid removal of illegal content from social media platforms ([39]), including hate speech, and requires these platforms to publish compliance reports. It also includes child protection measures and provisions against disinformation.
	Section 176 of the German Criminal Code (Strafgesetzbuch)	Expanded in 2020, Section 176 criminalises cybergrooming, including attempted cybergrooming.
	Reform of the Youth Protection Act (Jugendschutzgesetz), 2021	The act was reformed to enhance digital child protections ([40]).
Ireland	Harassment, Harmful Communications and Related Offences Act, 2020	Also known as 'Coco's Law', the act criminalises online abuse such as the non-consensual sharing of intimate images and cyber harassment. Intimate partner relationships constitute an aggravating factor during sentencing.
Italy	Law Decree No 11/2009	This decree introduced Article 612-bis on stalking into the Italian Code of Criminal Procedure.
	Cyberbullying Law (Law No 71/2017)	The law targets cyberbullying among young people, mandating the existence of school prevention programmes, content removal and support and rehabilitation services for both victims and perpetrators.
	'Red Code' Law ([41]), 2019	This law prioritises cases involving gender-based violence, recognising the growing role of ICT in harassment cases by emphasising protections for victims in the digital sphere.
	Revenge Porn Law, 2019	Part of the 'Red Code' legislation, this law criminalises the non-consensual sharing of intimate images or videos, with penalties of up to six years imprisonment and increased sanctions for cases involving minors or intimate partners. It prioritises such cases, as well as other forms of gender-based violence, to speed up the proceedings and reduce victim trauma, while offering protections such as anonymous reporting, psychological support and safeguards against retaliation.

39 The law requires social media platforms with over 2 million users to remove 'clearly illegal' content within 24 hours and all illegal content within 7 days of its posting, with a maximum fine of EUR 50 million for non-compliance.

40 'Germany: Media literacy and safe use of new media' – European Commission Youth Wiki.

41 Law No 69/2019 aims to speed up the judicial proceedings for specific types of crime that are forms of domestic and gender-based violence.

Member State	Name of the measure and year	Description
Austria	Section 107a of the Austrian Criminal Code	This section criminalises cyberstalking.
	Section 107c of the Austrian Criminal Code	This section targets persistent online harassment.
	Hate on the Internet Act, 2021	This legislative package introduced measures to improve the legal situation of those affected by cyber violence. For example, it facilitates civil claims against online hate. Victims of cyber violence are granted injunctive relief for hate postings that violate their human dignity. Such postings must be removed immediately. Victims of online hate are also entitled to free psychosocial assistance and legal assistance in court proceedings. It strengthened the criminal offence of incitement to hatred / hate speech and extended the scope of the offence of cyberbullying. The offence of 'upskirting' has also been added to the Austrian Criminal Code.
Poland	Article 190a of the Polish Penal Code, 2011	This article criminalises stalking and harassment, including such acts conducted via electronic means. Legal interpretations confirm that cyberstalking and cyberbullying are covered, even though the article does not explicitly use the term 'cyber'.
Portugal	Article 152 of the Portuguese Penal Code, 2018	Law No 44/2018 amended the Portuguese Penal Code to strengthen the criminal protection of private life on the internet. It introduced into paragraph 2(b) of Article 152 (on domestic violence) the non-consensual dissemination, via the internet or other widely accessible public media, of personal data, including images or sound relating to private life, as an aggravating form of domestic violence.
	Article 240 of the Portuguese Penal Code, 2024	Law No 4/2024 amended the Portuguese Penal Code by adding a paragraph to Article 240 on discrimination and incitement to hatred. It specifies that if the offences are committed through a computer system, the court may order the deletion of the relevant data or content, extending legal protections against online or digital forms of hate speech and discrimination, including gender-based harassment.
	Portuguese Penal Code	Through various general criminal provisions, Portuguese law has criminalised the invasion of privacy, crimes against the right to one's image, threats, stalking, incitement to hatred and hate speech, and these provisions also apply when the offences occur online or through electronic means.

Member State	Name of the measure and year	Description
Romania	Romanian Criminal Code	Romania amended its criminal code to explicitly criminalise cyber harassment and cyberstalking, enhancing penalties in cases involving intimate partner violence. It also covers the non-consensual distribution of intimate content, imposing severe sanctions, particularly when the victim is a minor or the perpetrator is a close relation. Online hate speech is similarly penalised.
	Amendments to Law 217/2003 on preventing and fighting against domestic violence, 2020	Through the amendments, the law recognises cyber violence as a means of coercion and control, allowing for protective measures such as prohibiting digital contact.
Finland	Finnish Criminal Code	While Finland relies on general criminal provisions, a recent amendment to the Finnish Criminal Code has expanded the application of sexual harassment law to include online contexts, providing better protection for victims of cyber violence. In particular, the law criminalises defamation, sexual harassment, illegal threats, stalking, violations of privacy and hate speech. These offences are punishable regardless of whether they occur online or offline.

EMBEDDING CYBER VIOLENCE PROTECTION IN BROADER LEGAL FRAMEWORKS

The third approach is integrating cyber violence into broader legislation on gender-based violence, sexual offences or child protection. In these cases, digital abuse is explicitly recognised as a form of coercion, discrimination or violence, ensuring that online behaviours are treated the same as offline ones. These frameworks often include preventive and educational measures – particularly targeting schools and young people – alongside victim support services (see Table 3).

Table 4 | Examples of provisions related to cyber violence that have been added to existing national legal frameworks

Member State	Name of the measure and year	Description
Belgium	Article 6 of the law of 31 July 2023 ([42])	The law amends Article 584 ([43]) of the Belgian Judicial Code to streamline summary proceedings in cases of the non-consensual distribution of sexually explicit content. Through an expedited procedure, victims can request a court order that requires the perpetrator(s) or the service provider to remove or render the images inaccessible. The law mandates that the president of the court of first instance ensures that the order contains all data necessary to identify the images or recording, facilitating their removal by service providers.
Cyprus	Law on the prevention and combating of violence against women and domestic violence, 2021	This law criminalises the non-consensual publication or threat of publication of sexual or pornographic material through digital or other means.
	Protection from harassment and stalking law (L.114(I)/2021)	The law extends the safeguards against harassment and stalking to online contexts.
Sweden	Swedish Penal Code	Under the Swedish Penal Code and related legislation, behaviours such as repeated online harassment, cyberstalking and the non-consensual sharing of private or intimate content are criminalised. The principle that conduct deemed illegal offline is equally illegal online helps ensure consistency between Swedish digital and physical legal frameworks. For example, criminal liability for rape and sexual violence includes acts committed remotely, for example online.
	Reform of the Sexual Crimes Act, 2018	In 2018 the Swedish sexual offences legislation was reformed. It is now an offence to perform a sexual act with someone who is not participating voluntarily. Thus, to convict a perpetrator of rape it is no longer a requirement to establish that violence or threats were used or that the victim's particularly vulnerable situation was exploited.

42 Loi du 31/07/2023 visant a rendre la justice plus humaine, plus rapide et plus ferme IV.
43 Article 584 of the Belgian Judicial Code.

5.2.2. Beyond legislative approaches at the national level

While many Member States have developed legislation targeting the perpetrators of cyber violence, some have also taken steps to aid victims by implementing policies and initiatives that offer victim support services and preventive measures. However, many of these approaches still lack a gender perspective that specifically considers the experiences of women and girls. As a result, these policies frequently fall short of offering a comprehensive response to gendered cyber violence against women and girls, who are disproportionately affected by cyber violence.

In some Member States, policies to address cyber violence primarily focus on educational and awareness-raising measures and campaigns, which are often directed at the general public or at particularly affected groups such as women and young people. Some examples of these initiatives are described in Table 4.

Table 5 | Examples of educational and awareness-raising measures related to cyber violence in different Member States

Member State	Name of the measure and year	Description
Bulgaria	Cyberscout programme ([44])	Established in 2015, this educational initiative aims to enhance online safety awareness among children aged 11–12. Developed by the Bulgarian Safer Internet Centre, the programme aims to equip young students with the knowledge and skills to navigate the digital world safely.
Czechia	'Regions for a Safe Internet' campaign	Launched to raise awareness about online risks and promote preventive measures, this campaign targets school children. Since 2019, Czech regions have collaborated on this initiative, which includes e-learning courses for children, students, teachers, parents, police officers and social workers, as well as interactive online quizzes for students to test their knowledge of internet safety. The project also organises educational seminars.
	Police officer training	Since 2023, over 400 police officers have attended educational seminars on domestic and gender-based violence and gender-based cyber violence that were designed for law enforcement.
Germania	Coordination Center for Digital Violence ([45])	This local initiative, launched by the organisation Frauen helfen Frauen, supports professionals who accompany victims of cyber violence – counsellors, women's shelter staff and experts in the field of gender-based violence. The centre offers workshops that teach how digital abuse works and how it can be identified and stopped. Some seminars focus on practical issues like spyware and account security, while others deal with legal options and the challenges of privacy violations.
Spain	'PantallasAmigas' initiative ([46])	Established in 2004, the initiative promotes the safe use of digital technologies among children and adolescents. It offers educational content on cyberbullying, grooming, sexting and gender-based violence online. Its cyber managers programme uses peer-led approaches to foster digital responsibility.
	'#RedesSinMachismo' campaign ([47])	This is a media campaign launched in 2024 by the regional government of Andalusia to address the rise in digital gender violence.

44 https://eucpn.org/document/cyberscout-program.
45 https://www.fhf-heidelberg.de/de/digitale-gewalt/koordinierungsstelle-digitale-gewalt/.
46 https://www.pantallasamigas.net/.
47 https://www.produccionesvinyl.com/proyecto/redessinmachismo/.

Member State	Name of the measure and year	Description
France	'StopCybersexisme' campaign	Launched in 2017, this campaign aimed to raise awareness about digital sexual harassment and equip victims and witnesses with practical tools. It offers prevention toolkits comprising a poster, informational flyer, awareness video and a dedicated website ([48]). This platform defines cybersexism, offers guidance for victims, promotes self-protection and includes testimonials.
	French Laboratory for Women's Rights Online	Established in 2024 as a platform for dialogue and innovation to tackle online violence against women, this laboratory also serves as an incubator for concrete projects aimed at identifying, preventing and curbing online and technology-facilitated gender-based violence.
	pHARe anti-harassment programme	Fully implemented in all French schools since 2023, the programme tackles bullying through prevention, response mechanisms and awareness. It includes the 3018 hotline against online harassment, which is in all student materials, and trains staff to recognise and act on harassment. The central element of the programme is the 'Non au harcèlement' school competition. This annual contest invites students to co-create anti-bullying campaigns, encouraging peer-to-peer involvement in promoting empathy, respect and gender equality. The winner's campaign is promoted at the national level in schools.
	'Parents, parlons numérique' awareness campaign	Launched by the Ministry for Solidarity, Autonomy and Equality between Women and Men, this campaign equips parents with the tools and advice to help children develop healthy, respectful digital habits, especially in relation to online risks such as pornography and peer violence.
	Guide on intimate partner cyber violence	The French government published a guide in 2025 for professionals in contact with women victims of gender-based violence in partnership with the Centre Hubertine Auclert, a women's rights non-governmental organisation (NGO) that has expertise in cyber violence.
	Association for the fight against sexist cyber violence (Echap)	Founded in 2020, Echap is a feminist association that addresses the rise of digital violence against women and marginalised groups. They work closely with domestic and sexual violence support organisations, providing technical assistance in cases involving spyware, online harassment and privacy breaches. Echap also develops accessible guides on digital threats and offers workshops.

48 https://www.stop-cybersexisme.com/.

Member State	Name of the measure and year	Description
Italy	'Stop Sexting and Revenge Porn' campaign	The campaign was launched in 2021 by Mete Onlus to combat the non-consensual distribution of intimate images. It combined educational programmes, public awareness campaigns and online resources to empower young people.
Cyprus	Safer Internet Center – CYberSafety ([49])	Developed by the Cyprus Pedagogical Institute, the centre offers lectures and experiential workshops for students, teachers and parents to share information on the safe and responsible use of the internet and digital technologies. Since 2017, the institute has also organised summer camps focusing on internet safety alongside events around 'Safer Internet Day' every year in February.
Latvia	Safety messengers programme	Launched by the state police in 2022, the programme is a prevention initiative that aids educators and schools in teaching minors about safety risks and self-protection. Online violence and digital risks are specifically addressed through interactive role playing scenarios designed for two age groups (8–10- and 11–14-year-olds). These activities focus on different dangers in the online environment, including the risks of sexual abuse, how to recognise them and recommendations for prevention.
	'Dangerous online friendship' tool	Developed in 2022 by the Safer Internet Center in cooperation with the state police and the Children Protection Center helpline, this online tool helps children, adolescents and educators recognise grooming and receive advice and help ([50]).
Hungary	Netmentor peer mentoring programme ([51])	This programme is focused on promoting responsible internet use among young people through peer-to-peer mentoring, so that they understand its risks and possibilities. Among other activities, the Netmentor programme trains older students to become 'Netmentors' who lead workshops for younger peers on topics like online privacy, digital footprints and safe internet use. Educators are also trained to support and guide the mentors. The programme's workshops are designed to be engaging and interactive, encouraging active participation and reflection on online behaviour.

49 'Training in schools' – Safer Internet Center.
50 Dangerous online friendship website.
51 https://digitalisgyermekvedelem.hu/en/netmentor-peer-mentoring-program/.

Member State	Name of the measure and year	Description
Austria	#GemeinsamGegenCybergewalt (together against cyber violence)	Launched in 2023–2024, the project focused on identifying victims' counselling needs and tailoring support services accordingly. The project produced counselling materials and informational resources for both victims and the public. Even after its official end, the network behind the initiative continues to share content on platforms like Facebook and Instagram and provide updated guidance to counselling centres.
	#netzamazonen ([52])	Led by the counselling service Women advising Women (Frauen beraten Frauen), this project targets online dating safety, privacy and smartphone security. In 2024 the project published a handbook titled Is This Already Digital Violence? that offers a detailed analysis of the phenomenon.
Slovenia	Odklikni project: ClickOFF! Stop cyber violence against women and girls	Implemented from 2017 to 2019, the project aimed to raise awareness among young people about digital gender-based violence. The project included TV advertisements, posters, a mobile app, a dedicated website ([53]) and a manual for professionals working with young people. It also organised extensive training for educators, social workers, judges and police officers, highlighting the need to avoid gender bias and stereotypes when addressing online violence. Simultaneously, other Slovenian projects focused on preventing dating violence among young people from a gendered perspective.
Finland	'For you in social media' service ([54])	This service aims to combat cyberbullying and online sexual abuse among young people aged 8 to 21. Operated by non-profit organisations, this service directly engages with young people on platforms where they often encounter cyber violence. Beyond individual support, the service produces educational content to raise awareness about online safety and healthy digital relationships. Their videos cover topics such as recognising and responding to cyberbullying, understanding consent and navigating online interactions safely.

Source: Authors.

In addition to awareness-raising initiatives, some Member States have embedded actions targeting cyber violence into their national action plans. Some examples of this can be seen in Table 5.

52 https://frauenberatenfrauen.at/projekt/netzamazonen/.
53 http://odklikni.enakostspolov.si/.
54 https://suavartensomessa.fi/in-english/.

Table 6 | Examples of Member State national action plans containing actions targeting cyber violence

Member State	Name of the measure and year	Description
Belgium	National action plan to combat gender-based violence (2æ021–2025)	The action plan recognises the gendered nature of cyber violence and includes objectives to combat it. These are achieved through different measures such as an informational platform on cybersexism, improving police and judicial actions, and collaboration. The plan also supports law enforcement's capacity-building and awareness campaigns targeting adult social media users.
Czechia	Gender equality strategy (2021–2030)	The strategy addresses cyber violence within partner violence. It highlights forms of violence such as revenge porn and harassment via messages, which especially affect young people.
	Action plan for prevention of domestic and gender-based violence (2023–2026) and strategy for criminality prevention (2022–2027)	The action plan includes measures such as training police on domestic and gender-based violence, including cyber violence, and raising awareness on safe internet practises in schools.
France	Fifth plan to mobilise and combat violence against women (2017–2019)	Under the Swedish Penal Code and related legislation, behaviours such as repeated online harassment, cyberstalking and the non-consensual sharing of private or intimate content are criminalised. The principle that conduct deemed illegal offline is equally illegal online helps ensure consistency between Swedish digital and physical legal frameworks. For example, criminal liability for rape and sexual violence includes acts committed remotely, for example online.
	Interministerial plan for gender equality (2023–2027)	This plan's measures include improving the accessibility of complaint mechanisms and assistance for victims of cyber violence and strengthening training tools.
Croatia	Action plan for violence prevention in schools (2020–2024)	The plan includes measures targeting cyber sexual violence among children and young people. It supports school-based prevention programmes and defines specific forms of cyber violence, such as online hate speech, cyberstalking, cyber harassment, sexual harassment and sexting.

Member State	Name of the measure and year	Description
Italy	National plan to prevent bullying and cyberbullying at school (2016–2017)	The plan established training programmes and awareness campaigns for students and teachers and introduced helplines for affected students and families. This has evolved over time, with updated provisions and the 'ELISA' (E-Learning degli Insegnanti sulle Strategie Antibullismo) platform offering e-learning for teachers handling cyberbullying cases.
Cyprus	National strategy for the prevention and combating of violence against women (2023–2028)	The national strategy calls for stricter media regulation and improved data collection, integrating GREVIO recommendations on online violence.
	Cybersecurity strategy of the Republic of Cyprus 2020	The cybersecurity strategy includes measures to ensure the protection of critical information infrastructure, combat cyber threats and enhance resilience.
	National strategy for a better internet for children in Cyprus (2018–2023)	The national strategy for a better internet for children in Cyprus includes actions concerning children, but also teachers, parents and the wider public.
Malta	Children's policy framework 2024–2030	The framework includes targeted measures to address the heightened risks of cyber violence, while also recognising that girls are disproportionately affected. It tackles issues such as cyberbullying and online harassment.
Austria	National action plan to combat violence against women and girls (2025–2029)	The plan includes measures against digital violence, including violence using AI. It contains a dedicated chapter on digital violence and addresses the implementation of the EU Violence against Women Directive, including criminal offences relating to cyber violence.
Portugal	National strategy for equality and non-discrimination – Portugal + Equal	The national strategic plan to promote equality and combat discrimination has led to three action plans. The 2023–2026 action plan for the prevention and combating of violence against women and domestic violence includes measures such as strengthening legal protections against forms of online violence, particularly image-based sexual violence targeting women and girls and online hate speech (Measure 242), and training and upskilling professionals to address these forms of online violence (Measure 418).

Source: Authors.

Other Member States have recognised the importance of cross-sector collaboration in addressing cyber violence. Some examples of this can be seen in Table 6 below.

Table 7 | Examples of Member States collaborating across sectors to address cyber violence

Member State	Name of the measure and year	Description
Czechia	Be safe project	The project addresses cyberbullying, while also establishing a connection between schools, educational institutions and the police. Educators have access to up-to-date news and information on the latest trends in cyberbullying and cybercrime, which they can incorporate into their teaching.
Denmark	2017 interministerial programme	The programme brought together the Ministries of Education, Justice and Gender Equality to address digital sexual abuse. This initiative involved the creation of educational resources, public awareness campaigns and partnerships with civil-society organisations.
Germany	InterAktion project ([55])	Led by the Federal Association of Women's Shelters and Counselling Centres, the project, launched in 2023, connects women's counselling centres and helplines with local information technology professionals. By creating these partnerships, these stakeholders can address complex cases involving cyber violence.
Estonia	Targalt Internetis smartly on the web programme ([56])	The programme integrates cybersecurity experts into educational efforts, providing young people with the tools and training needed to identify and respond to online threats, including gender-based violence.
Lithuania	Safer Internet Consortium	The consortium is a collaborative model involving the Information Technology Centre that is part of the Ministry of Education and Science, the Communications Regulatory Authority, the NGO Child Line and the digital literacy organisation Langas į ateitį. These partners work in different sectors – including the government, technology, media and civil society – to create a safer digital environment for children and reduce their exposure to online risks.

Source: Authors.

EU-LEVEL COORDINATION AND MULTISTAKEHOLDER INITIATIVES

At the EU level, collaborative efforts continue to drive progress. A key player in these efforts is the International Association of Internet Hotlines (INHOPE), which began in 1999 with eight European hotlines and has since grown into a global network. It enables victims to report illegal online content, particularly child sexual abuse material, online grooming and hate speech, including xenophobia. All Member States are part of this network.

55 https://www.frauen-gegen-gewalt.de/de/aktionen-themen/bff-aktiv-gegen-digitale-gewalt.html.
56 https://www.targaltinternetis.ee/en/.

Another major initiative is Insafe, which operates under the European Commission's better internet for kids strategy. It runs Safer Internet Centres in 30 European countries, which offer education and support through helplines and hotlines for children, parents and teachers. These centres also forward reports of illegal or harmful online content to the appropriate authorities, such as internet service providers, law enforcement or INHOPE hotlines. Importantly, 'the centres include youth panels to ensure young people have a voice in shaping online safety policies and resources.

The EU also organises the annual Safer Internet Forum, bringing together policymakers, researchers, industry representatives, law enforcement and young people to address online safety challenges. The 2024 forum focused specifically on cyber violence and protecting young people from harmful content and bullying. Similarly, Safer Internet Day, celebrated each year in over 100 countries, raises global awareness of issues like cyberbullying and online sexual harassment. The #SaferInternet4EU campaign, launched in 2018, furthers this mission by supporting EU-wide initiatives to address emerging digital risks. Other examples of EU-funded projects are presented in Box 4.

Box 4 | Examples of EU-funded projects that promote a collaborative approach

CyberEqual project (2024)

This project is an Erasmus+ initiative involving Cyprus, Greece, Lithuania, Slovakia and Ukraine. It aims at educating and raising awareness among young people about cyber violence against women and girls. Its primary objectives include increasing knowledge on the prevalence of and legislation against cyber violence against women and girls, raising awareness and educating young people and professionals, motivating young people to protect themselves and equipping youth workers with tools to combat cyber violence against women and girls.

DeStalk (2021)

DeStalk is a European initiative run in Spain and Italy that is coordinated by Blanquerna-URL with support from the EU's rights, equality and citizenship programme. Its objective is to combat cyber violence and gendered cyberstalking. By 2022, the project had trained more than 350 professionals – primarily in Spain and Italy – who work in the field of gender-based violence. DeStalk has an online learning platform, creates practical tools and guidelines and supports regional campaigns to raise awareness about cyber violence and digital safety.

Cybersafe: Changing attitudes among teenagers on cyber violence against women and girls (2019–2021)

The Cybersafe project was a 30-month EU-funded initiative that brought together nine partners from various European countries – Austria, Denmark, Estonia, Greece, Italy, the Netherlands, Slovenia and the United Kingdom. Its primary goal was to develop, promote and disseminate innovative educational tools to address cyber violence against women and girls among teenagers aged 13 to 16. Through the project a Cybersafe toolkit was developed for teachers and other professionals working with young people who want to address cyber violence against women and girls in the classroom or in other settings. The Cybersafe toolkit offers resources and tools to organise and conduct four workshops addressing gender-based online violence. Its aim is to raise awareness and promote safe and responsible online behaviour among young people.

Targalt Internetis project (2019)

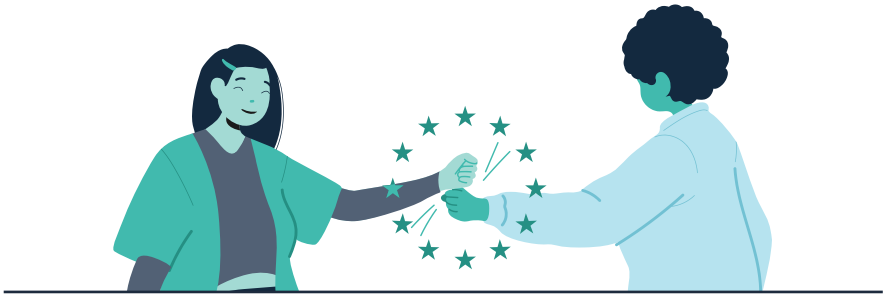
This project aims to promote smarter internet usage among children and their parents while actively working to prevent the online distribution of child sexual abuse material. Co-financed by the European Commission, the initiative encompasses a variety of activities designed to enhance awareness and education. These include training sessions and seminars tailored to children, parents, teachers and social workers, along with public awareness events aimed at the general population. Additionally, the project involves the creation of training materials that serve to inform children, teachers and parents about safe internet practices. To engage children and students with the subject creatively, the project hosts competitions that encourage participation and awareness. Furthermore, it provides assistance and counselling through the child helplines available at 116111, which are accessible via telephone, SMS, Messenger and other instant messaging services, offering guidance to children and parents on the safe use of the internet and digital mobile devices. The initiative also has a web-based hotline which enables internet users to report environments containing materials that violate children's rights to sexual self-determination and other inappropriate content. Since its inception in January 2019, the project has prioritised cooperation among various stakeholders in Estonia and across Europe, actively participating in the INHOPE and Insafe networks to strengthen its impact.

Project deSHAME (2017)

Project deSHAME is an EU-funded project aiming to prevent and respond to online sexual harassment. The project involved Denmark, Hungary and the United Kingdom and aimed at addressing and reducing peer-based online sexual harassment among young people aged 13 to 17. The project sought to empower local communities to work together to increase reporting among young people. To deal with these issues, the deSHAME project developed resources tailored to educators, parents and young people. These materials aim to raise awareness, educate about the harms of online sexual harassment and promote safe online behaviour. The project also produced an international adaptation toolkit to assist other countries and organisations in implementing similar initiatives to tackle online sexual harassment.

Work with perpetrators (2015)

This project provides valuable guidelines for addressing cyber violence, with a perpetrator-focused approach. A key principle of these guidelines is that the burden of protection should not fall on the victim, as they have the fundamental right to safety in digital spaces. Instead of placing the responsibility on individuals to avoid or mitigate online abuse, the project underscores the need for systemic solutions, including stronger legal frameworks, proactive intervention strategies and accountability measures for perpetrators. It also highlights the crucial role of collaboration among digital platforms, policymakers and law enforcement in preventing and addressing cyber violence, ensuring that victims are not forced to endure harm in silence but are supported through comprehensive protections and effective enforcement mechanisms.



OTHER PREVENTIVE MEASURES IN FOCUS GROUP COUNTRIES

When analysing in depth the Member States where focus groups were conducted, it is clear that their authorities and organisations have also implemented prevention-oriented strategies that aim to tackle cyber violence through targeted forms of support directed at children and young people, parents and relevant institutions.

Parental guidance plays a crucial role in providing emotional support and practical advice to girls experiencing cyber violence. However, parents often face significant challenges in understanding how to best respond to such situations. In Germany and Italy (see Box 5), awareness-raising and prevention campaigns have been launched to promote safe internet use and to provide parents with guidance on how to support children and young people when dealing with issues related to cyber violence.

Box 5 | Examples of campaigns for safer online environments – Germany and Italy

Germany's 'klicksafe' campaign, co-funded by the EU, promotes responsible internet use among children, young people, parents and educators. It includes specific resources to help address digital sexual violence, such as the brochure 'The first smartphone – How can I protect my child from sexual violence on the internet?', produced in collaboration with the Federal Ministry for Education, Family Affairs, Senior Citizens, Women and Youth and the Independent Commissioner for Child Sexual Abuse Issues. Another major initiative is 'active against digital violence', which supports victims of gender-based digital abuse through awareness campaigns and practical tools as part of Germany's broader digitalisation strategy.

In **Italy**, the initiative Scelgo io! (I Choose), launched in 2018 by the organisation Cuore e Parole and under the project Generazioni Connesse, offers online training and conferences for parents about the dangers of sexting for their children and provides guidance on protecting them from image-based abuse and cyber violence.

Source: Authors, using the 'klicksafe' programme and 'Generazioni Connesse' websites.

Other Member States (see Box 6) have adopted interesting practices to tackle cyber violence against young women and girls by combining education, technology and legal frameworks to foster a safer digital environment and prevent future incidents of cyber violence.

Box 6 | Examples of different approaches to tackling cyber violence – Belgium, Estonia, Ireland and Spain

Belgium's international plan SafeHaven uses Roblox (a popular online game platform) to teach young people about inappropriate behaviour in virtual worlds. It uses interactive games set in an e-pavilion give young people the tools to break down stereotypes, set boundaries and seek help. They are also encouraged to act as active bystanders both online and offline.

Estonia's web constables represent another innovative strategy; these are police officers dedicated to monitoring and responding to online abuse, including hate speech and harassment.

Ireland has integrated cyber violence prevention into its school curriculum through a short course on social, personal and health education (SPHE). Updated in 2023, the programme includes modules on respectful online communication, digital consent and recognising harmful behaviours in online interactions. It equips young people with the practical knowledge and skills to prevent and respond to cyber harassment and image-based abuse.

Spain also took a creative approach with the video game Conectado, which immerses players in the experience of a victim of cyberbullying over five days to encourage empathy and dialogue in educational settings.

Source: Authors, drawing on the SafeHaven website, junior-cycle social, personal and health education curriculum, Conectado website, and web page on web constables.

Alongside parental guidance and the integration of youth-centred and law enforcement measures, some Member States have implemented training programmes aimed at equipping teachers and specialised professionals with the skills to prevent and respond to the online risks faced by children and young people (for examples, see Box 7). These initiatives recognise that schools and professional support services are often the first to detect signs of cyber violence.

Box 7 | Examples of training programmes for teachers and specialised professionals – Poland and Sweden

In **Poland**, the Awareness Centre conducts webinars, classes and workshops for teachers and other specialists focused on digital safety. In addition, the Empowering Children Foundation runs an online learning platform that provides open-access resources on internet safety for teachers.

Sweden's national 'safe internet use' training module provides structured professional development for teachers, librarians and school health personnel. Covering online behaviour, cyberbullying, gaming and information security, it promotes collaborative learning and its practical application in the classroom.

Source: Authors, based on the Polish Safer Internet Centre website and 'Safe internet use' training module web page.

5.2.3. Young people's perceptions of responses to cyber violence

Although the insights presented here are based on focus group discussions – and are therefore not intended to be generalised – they constitute a crucial and innovative contribution to understanding how adolescents experience and respond to cyber violence. The discussion reveals a complex interplay between individual coping strategies, peer dynamics, institutional responses and wider structural barriers. Participants' narratives highlight that experiences of shame, fear and mistrust often prevent victims from reporting violence or seeking help. At the same time, schools, parents and institutional actors are perceived as inconsistent in their responses or unprepared.

INDIVIDUAL RESPONSES

Girls' immediate emotional responses to cyber violence were shaped by age, perceived severity and the availability of support.

They often reacted by withdrawing emotionally, remaining silent or blocking perpetrators, driven by fear, shame or a desire to avoid escalation. These reactions were most common among younger girls (aged 13–15). Others described defensive confrontations, stating that they directly challenged aggressors online. Yet, even these active responses were often framed as last-resort reactions that occurred in the absence of support structures. Likewise, boys noted that shame – particularly in cases of image-based abuse – was a major barrier for girls in reporting incidents. Fear of judgement from parents or authority figures also emerged as a common key concern among girls and boys.

Nevertheless, for some girls, parental guidance played a formative role in shaping how they approached online safety, especially during their early adolescence. Peers also frequently played an important role as the first point of disclosure, offering emotional support, advice and serving as a bridge to wider support networks.

Boys' accounts revealed a more mixed picture. Some described positive cooperation between parents and schools, while others feared blame and misunderstanding.

INSTITUTIONAL RESPONSES

Perceptions of institutional support – including schools and the police – varied widely. Parents were generally seen as more reliable and protective than other actors, though disclosure to them was often hindered by fear of disappointment or blame.

Older girls (aged 16–18) tended to express greater scepticism towards institutional responses. This scepticism often stemmed from personal negative experiences or heightened awareness of structural barriers, such as unhelpful counsellors. A widespread lack of awareness about existing support services for girls and boys also reinforced the belief that 'the solution lies within us, and not in seeking help'.

Teachers and counsellors were seen as both potential allies and sources of frustration. Some boys valued trusted teachers who provided a safe space for disclosure. Others, however, expressed that some teachers exacerbated issues. Girls confirmed these feelings. They stated that they frequently found schools to be ineffective or dismissive. In many cases, trust in teachers was low, with several girls reporting that school staff downplayed or dismissed their experiences.

Some girls described feeling betrayed when counsellors promised confidentiality but later disclosed information to their parents without their consent. Others recounted positive experiences where teachers or counsellors intervened decisively, even if they were not always well equipped or sufficiently trained to deal with cyber violence. This ambivalence underscores the variability in school responses, which are often dependent on individual staff rather than systemic approaches.

> **The school counsellor never did anything. They just took notes and stuff. Then they called my parents and told them everything. And then I had to face my parents and take full responsibility. It was even worse. And that didn't just happen once. It happened more than once.**
>
> **(GIRL 16–18, BELGIUM)**

Police were viewed by both girls and boys with greater scepticism and frustration, despite there being instances where authorities took action. Many participants doubted the seriousness with which authorities treated cyber violence, citing long delays, inaction or outright dismissal. Boys, in particular, ridiculed the idea of involving the police.

> **No one is going to call the police. Who's such a wimp that they'd call the police? Very few police officers would take this issue seriously.**
>
> **(BOY 15–18, CYPRUS)**

Girls also reported frustration with ineffective investigations and delays.

> **I was contacted two and a half years later ... The complaint didn't really work out.**
>
> **(GIRL 16–18, BELGIUM)**

YOUNG PEOPLE'S VIEWS ON ADULT SUPPORT

Girls across Member States and age groups generally viewed adults as disconnected from the realities of young people's digital lives. Many described adults – including parents and teachers – as lacking the awareness, sensitivity and training to respond effectively to cyber violence. Participants frequently reported that adults either downplayed their experiences or responded in ways that discouraged disclosure.

> **Parents sometimes don't believe or like ... generally older people don't believe us.**
>
> **(GIRL 13–15, ESTONIA)**

> **Many adults ... around you tend to solve things by saying that it's not that important, when you feel that it is important and then it really hurts you.**
>
> **(GIRL 13–15, ROMANIA)**

Some girls expressed reluctance to seek help from parents, fearing punishment or misunderstanding rather than support. While some felt close to their parents and believed they could provide help, others emphasised that their parents lack an understanding of the digital world. Other participants held adults accountable for their early and excessive exposure to technology.

> **I have acquaintances who received a phone with internet access at 3–4 years old … it seems to me that you got out of the womb and you were messed up by your parents; they just wanted you to shut up so they just gave you a tablet …. Now you don't know how to socialise, and you don't have communication skills and you're like, 'what am I doing here?'**
>
> **(GIRL 13–15, ROMANIA)**

The perceived role of teachers and school psychologists in prevention and intervention was mixed. Younger girls often trusted some teachers, particularly those who were kind or relatable. School psychologists were also mentioned as helpful. However, many participants felt that schools lack genuine support mechanisms, with teachers and institutions often appearing indifferent or failing to act and, therefore, leading girls to think that 'school is the last place to ask for help'.

The willingness of girls to seek adult support appears to be influenced by contextual factors. In some Member States – such as Italy, Cyprus and Sweden – they expressed greater disappointment in adult responses, whereas in others – such as Estonia and Ireland – girls were more inclined to trust adults, describing school and family as emotionally responsive or supportive.

Age also shapes perceptions of adult involvement. Younger girls (aged 13–15) were generally more open to confiding in trusted adults, particularly teachers and parents. Older participants (aged 16–18) were more sceptical, citing emotional distance, communication breakdowns and generational differences, particularly regarding digital culture, sex and relationships.

LIMITATIONS AND YOUNG PEOPLE'S RECOMMENDATIONS FOR EFFECTIVE PREVENTION

Across Member States, most girls agreed that prevention strategies are limited, outdated or poorly implemented. School-based initiatives were often described as superficial, repetitive and disconnected from young people's digital realities. Brief lectures, repeated campaigns and school assemblies delivered by the same individuals were seen as largely ineffective.

Likewise, boys identified a critical gap in early and meaningful education on cyber violence, noting that current school-based interventions are often delivered too late or lack relevance.

Girls also reported that the resources for preventing or responding to cyber violence are insufficient, particularly regarding support structures. Barriers to effective prevention included a lack of confidentiality in small communities, vague or ineffective reporting mechanisms, insufficient age-appropriate education and cultural taboos limiting open discussions. These challenges were especially pronounced among older girls (aged 16–18).

> **Even if schools raise awareness of cyber violence, that is not effective because adults don't know how to reach teenagers.**
>
> **(GIRL 16–18, ITALY)**

Boys further called for stronger accountability for perpetrators, especially in addressing legal gaps related to image-based abuse, including deepfakes ([57]). This concern reflects an emerging theme within cyber violence, as online abuse in virtual reality and metaverse environments presents unprecedented challenges due to weak regulations, insufficient moderation and societal attitudes that minimise or dismiss online abuse as not 'real' (Chawki et al., 2024).

Girls proposed practical recommendations for improving prevention and support mechanisms, including:

- improved access to mental health professionals;
- anonymous and confidential reporting options;
- peer-based online chat and support services;
- support services that are visible, trustworthy and emotionally accessible;
- more open and structured discussions in schools about cyber violence;
- interactive, participatory and experiential education using real-life examples;
- clear and easily accessible information on how and where to report abuse;
- prevention programmes that address both victims and perpetrators;
- comprehensive training for teachers on how to communicate effectively with young people about sensitive topics.

57 In Ireland, creating a deepfake is not currently illegal, but distributing/resharing deepfakes is illegal under the Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law), explored in Section 2.4.

6 Conclusions

Cyber violence against women and girls is a pervasive, deeply gendered continuum of violence – driven by unequal power relations and reinforced by social norms – that shapes and constrains the digital lives of girls and young women.

Cyber violence is a widespread, complex and deeply gendered phenomenon that affects both digital and physical environments, forming a continuum of abuse. It is rooted in societal norms, gender stereotypes and unequal power dynamics that reproduce offline hierarchies of gender and control within online spaces. These dynamics appear in behaviours that objectify, control or silence girls and young women. They reflect wider social norms that reward male dominance and shame female sexuality. Among boys, certain acts of cyber violence are often condoned and seen as a way to gain approval from peers or prove masculinity, while girls who experience abuse are blamed or mocked. This creates a digital culture where aggression is linked to power, and responsibility for harm is shifted onto victims.

Girls and young women experience cyber violence as a routine part of their digital and social lives, with distinct age-related patterns: younger girls (aged 13–15) are more likely to face exclusion, gossip and body shaming, while older girls (aged 16–18) are more frequently subjected to sexualised forms of violence such as online sexual coercion and extortion, grooming and non-consensual image sharing. Teenage boys are also found to be specifically targeted for online sexual coercion and extortion by perpetrators operating in organised criminal networks, with financial gain being the main motivator. Younger adolescents are also increasingly being exposed to sexualised and coercive forms of online abuse, underscoring the widening reach and normalisation of digital violence.

Evidence from the focus groups further highlights that incidents of cyber violence often originate in offline settings such as schools, communities or peer groups and escalate online, spreading rapidly across multiple platforms and social arenas. This escalation from physical to digital spaces amplifies harm, blurs boundaries and makes abuse harder to contain.

A diverse range of perpetrators, enablers and passive bystanders sustains and amplifies the cycle of cyber violence against women and girls.

Cyber violence is perpetrated by a wide range of people, including peers, intimate partners and organised groups. Digital anonymity enables and amplifies abuse, reducing accountability and enabling the spread of harmful behaviours. In addition to primary perpetrators, secondary actors who share and react to abusive content contribute significantly to its perpetuation. Bystanders also play a pivotal role: while some may intervene, many remain passive due to social pressure and fear of reprisal. The focus group findings show that boys, in particular, can act as both perpetrators and potential allies. Acts such as non-consensual image sharing or group harassment are often discussed as performances meant to impress others or conform to peer expectations. This ambivalence underscores the need for greater efforts to cultivate empathy and accountability among bystanders.

Intersectional inequalities heighten vulnerability and deepen the impact of cyber violence on marginalised groups.

The findings underscore that cyber violence is shaped by intersecting identities and structural inequalities. Factors such as disability, ethnicity, religion, gender identity and socioeconomic status compound risk, with marginalised girls and young women facing higher exposure to cyber violence and having fewer avenues for support. Focus group participants highlight how online spaces often reproduce offline systems of oppression – such as sexism, racism and transphobic abuse – making certain groups more visible, targeted and less protected. These inequalities not only increase the likelihood of experiencing cyber violence but also intensify its emotional and social consequences.

Systemic discrimination and unequal access to justice further exacerbate these vulnerabilities. Marginalised girls and young women often face significant barriers when seeking protection, including a mistrust of institutions, lack of awareness about their legal rights and limited access to affordable legal assistance. Addressing cyber violence against women and girls therefore requires an intersectional approach that recognises how overlapping forms of disadvantage amplify harm and perpetuate inequalities.

Cyber violence has enduring psychological, emotional and relational consequences that extend far beyond the digital realm, profoundly affecting victims' mental health, social trust and sense of identity.

The continuum of cyber violence extends beyond the digital realm, creating lasting psychological, emotional and relational harm. The psychological and social impacts of such violence are profound, with victims frequently reporting high levels of anxiety, depression, trauma and diminished self-esteem that have long-term consequences for their mental health and relationships. Many adolescents describe experiences of social isolation and distrust, sometimes using terms such as 'depression', 'suicide' and 'trauma' to convey their distress. Fear of stigma, victim blaming and reputational damage further discourage reporting, thereby perpetuating cycles of silence.

The enduring nature of online abuse – with harmful content capable of resurfacing long after the initial event – means that its emotional, psychological and relational effects remain deeply rooted and long-lasting. Moreover, beyond its impacts on the individual, repeated exposure to online abuse also contributes to the normalisation of violence. Young people have begun to view cyberbullying and harassment as inevitable aspects of digital life, something to be endured rather than challenged. This normalisation not only magnifies the emotional toll of cyber violence but also entrenches patterns of acceptance and disengagement, reinforcing its enduring impact across both digital and social spheres.

The EU Violence against Women Directive provides a much-needed common framework in terms of definitions and enforcement mechanisms. Its full transposition into national law and implementation should be prioritised to deliver results.

Efforts to address cyber violence against women and girls are currently hampered by the large number of definitions used across Member States and jurisdictions and by the rapid evolution of digital technologies, including AI. The diverse manifestations of cyber violence – which range from harassment to image-based abuse – and the wide spectrum of motivations and relational dynamics that it entails require nuanced understanding and context-sensitive interventions. These must also account for broader cultural, institutional and social factors, including entrenched gender norms that normalise male aggression and victim blaming, peer dynamics that reward abusive behaviour and reinforce double standards, the influence of online subcultures and pornography in shaping misogynistic attitudes, and institutional patterns that excuse boys' harmful conduct while failing to protect or believe girls.

The Violence against Women Directive provides clear definitions that can underpin the development of harmonised indicators, data collection processes and monitoring and policy evaluations. As such, it has the potential to promote greater consistency and coordination across Member States.

Current prevention, education and support systems do not reflect young people's digital realities, leading to isolation and a lack of trust and leaving many without effective protection.

Findings reveal a significant disconnect between existing prevention efforts and adolescents' lived experiences. During focus groups, girls expressed frustration with school-based campaigns, adult and parental responses and institutional mechanisms that they perceived as outdated, superficial or disconnected from their digital lives.

School campaigns about cyber safety are viewed as ineffective because they fail to engage with the actual platforms, practices and risks young people encounter daily.

Adolescents consistently expressed that adults underestimate the significance of online spaces and the severity of the harm experienced there. Instead of acknowledging and validating these experiences, adults are often seen as minimising them. This lack of understanding deepens feelings of isolation and invalidation, particularly when young people seek help from institutions such as schools or counselling services. Many described inconsistent or poorly coordinated institutional responses, including breaches of confidentiality and the downplaying of their experiences, which erode trust and deter further disclosure.

This mismatch undermines confidence in prevention and support mechanisms, discouraging reporting and leaving many adolescents without adequate protection. Structural barriers further compound the problem: young people often lack clear information about where to seek help, and in smaller communities fear of exposure or gossip acts as a powerful deterrent.

Altogether, the findings highlight both progress and persistent challenges. Cyber violence against women and girls is firmly embedded within the continuum of gender-based violence and cannot be addressed in isolation from broader social, cultural and institutional contexts. While EU policy has evolved to recognise the complexity and urgency of digital abuse, gaps in its implementation and different responses across Member States continue to limit its effectiveness. Moving forward, coordinated, intersectional and youth-centred approaches are essential to ensure meaningful prevention, protection and accountability across the EU.

7 Policy recommendations

Combating cyber violence against women and girls across the EU requires coordinated, multilevel strategies and actions involving both EU institutions and Member States. It also requires alignment between EU directives, national legislation and local implementation frameworks. The recommendations from this research can be grouped into four interrelated areas: prevention and education, legal and policy frameworks on cyber violence, victim support and protection, and monitoring and evaluation.

Prevention and education

Guarantee early, gender-sensitive prevention that reflects girls and boys' digital realities.

- Introduce mandatory, gender-responsive digital literacy curricula into primary and secondary schools, covering digital identity, digital footprints, online interactions and misinformation detection (including deepfakes and manipulated content). To achieve this, build on national examples whose positive impact has been demonstrated.
- Promote a culture of digital self-care in education institutions by raising students and educators' awareness of digital safety (e.g. privacy settings, safe documentation of evidence, reporting tools) through regular 'digital safety screenings' in schools, where students review their online presence and privacy settings with guided support.
- Include specific learning objectives for boys and young men on masculine gender norms, peer pressure, accountability and the role of complicity in cyber violence.
- Integrate evidence-based bystander intervention training into school curricula, youth work and digital literacy programmes to teach young people how to safely intervene, report, disrupt or support a peer being targeted online. To this end, build on successful bystander intervention programmes from specialised support services focusing on violence against women.

Ensure prevention efforts are co-created with and responsive to girls' experiences.

- Collaborate with youth-led and community-based civil-society organisations, especially those working with diverse groups of young people, using participatory pedagogy to build upon common intelligence, while recognising young people's expertise in digital practices.
- Co-design prevention programmes with adolescents, ensuring that their educational materials address cyber violence, including sexualised abuse, image-based violence and victim-blaming narratives.
- Promote peer-led support initiatives where trained girls and boys can discuss harassment, coercion and healthy digital relationships, thus creating safe spaces to share experiences.
- Ensure that girls and boys' participation in co-creation does not translate into responsibility shifting towards victims. To this end, strive to provide a safe space for their voices and expertise while ensuring that victims receive professional specialised support.
- Provide parents and caregivers with practical guidance on digital parenting, including tools and resources to help them detect and address online abuse early.

Challenge harmful gender norms and address intersecting risks.

- Develop targeted programmes for boys that challenge sexist social norms and offer positive alternatives through role models, mentorship and youth-led discussions on respect, consent and healthy relationships. Such programmes can build on and be integrated into comprehensive sexuality education curricula.
- Create targeted outreach for girls facing intersecting forms of discrimination (e.g. migrant girls, girls with disabilities, LGBTIQ+ young people) to address their specific online risks and barriers to support.

Integrate prevention into broader EU and national policy frameworks.

- Fund structured youth advisory panels to inform national- and EU-level prevention strategies.
- Fund EU-wide campaigns featuring girls' voices to destigmatise the reporting of intimate image abuse and highlight the harms of perpetrating and sharing such content.
- Ensure that the prevention of online gender-based violence is enforced through fully implementing existing EU legislation and policy frameworks, including the European Commission's action plan against cyberbullying ([58]), the DSA, the EU strategy on the rights of the child, the EU youth strategy, and the Violence against Women Directive.

Encourage and support technological innovations that improve the prevention of cyber violence.

- Promote building responsibility into platform and product design to anticipate ways platforms' technical features can be misused for abuse.
- Ensure that social media platforms invest in the development of innovative technological solutions to anticipate, detect and deter acts of cyber violence specifically targeting girls and young women.
- Ensure that platforms strengthen deterrence through both messaging tools (e.g. pop-up warnings before sharing non-consensual images) and technical tools (e.g. image-based detection systems that flag potential violations). Such measures can shape user behaviour proactively and have a strong preventive function.
- Mandate the proactive detection and moderation of harmful trends, especially those targeting girls and LGBTIQ+ young people.

Improve EU-wide cooperation on image hashing and non-consensual image databases.

- By building on existing platforms such as Stop Non-consensual Intimate Image Abuse, facilitate collaboration between the European Union Agency for Cybersecurity, national cybersecurity centres and trusted third-party organisations.
- Support the interoperability and standardisation of image hashing databases to enable the consistent detection and removal of harmful content across platforms.
- Ensure that victim reporting mechanisms at the national level are directly linked to these technical infrastructures so that, once an image is hashed and flagged, it is recognised and blocked across multiple services.

58 'Action plan against cyberbullying – protecting children online' – European Commission.

Legal and policy frameworks on cyber violence

Ensure robust, harmonised regulation and enforcement across the EU.

- Reaffirm the EU's political will and commitment to enforce and build on existing legal frameworks, especially the DSA, the AI Act and the GDPR. In the context of the ongoing discussions on the digital omnibus package, uphold core safeguards.
- Ensure full enforcement of the DSA and the full transposition and implementation of the AI Act and the Violence against Women Directive, including gender-specific obligations regarding prevention, reporting and victim support.
- Employ common, harmonised definitions of the different forms of cyber violence established by the EU Violence against Women Directive and the cyber violence against women and girls measurement framework developed by EIGE to facilitate the collection of comparable, sex-disaggregated EU-wide data on online gender-based violence.
- Commend and pursue full coordination between national institutions and the European Board for Digital Services to monitor and improve social media platforms' compliance with DSA requirements.
- Disseminate and encourage adherence to the European Commission's guidelines on protecting minors online, adopted in July 2025.

Strengthen Member States' cybersecurity awareness and protocols to better respond to cyber violence.

- Develop clear EU-wide referral routes for national support services to access technical expertise – whether through national cybersecurity centres, computer security incident response teams or law enforcement units. Such expertise would equip practitioners with the appropriate technical support to respond to tech-facilitated abuse cases.
- Build on expertise at the EU level, for example from the European Union Agency for Cybersecurity, to strengthen these links by promoting consistent technical guidance, training and cross-border information sharing.
- Develop pathways for mutual learning and information sharing at the EU level with the view to build on successful national initiatives.
- Develop an EU protocol for responding to cyber violence in schools, detailing the steps involved in documentation, reporting, evidence preservation and stakeholder collaboration.

Mandate strong platform accountability and the creation of victim-friendly reporting tools.

- Promote the creation of strong mechanisms that monitor social media platforms' compliance with the DSA and the EU Violence against Women Directive, especially in terms of their moderation practices, reporting and support to users. The establishment of an independent monitoring body could provide useful coordination and oversight.
- Increase the number and visibility of EU-approved trusted flaggers / third parties to facilitate the rapid reporting and escalation of cases involving illegal content.
- Involve specialised support services for violence against women in the development of user-centred, anonymous and accessible mechanisms for reporting incidents of cyber violence to digital platforms, including hotlines, mobile apps and online portals.
- Ensure that reporting mechanisms address the intersectional dimension of cyber violence. In particular, the needs and reporting behaviour of users of different age groups, especially younger ones, should be taken into account to maximise the accessibility of reporting.
- Ensure that DSA takedown obligations are implemented, with clear time frames and notifications sent to victims once the content is removed.
- Incentivise platforms to adopt and adhere to a code of conduct on combating gender-based cyber violence that is developed in cooperation with civil society and equality bodies.

Set stronger standards for safer platform design and proactive risk mitigation.

- Promote the creation of stronger platform standards that take into account the real-life harms women and girls face online and include requirements for:
- safe product and algorithmic design that reduces the amplification of harmful content and prevents re-victimisation;
- sound risk assessment and safeguarding strategies, ensuring that platforms actively identify and address risks such as online harassment, deepfakes and image-based abuse.
- Require trauma-informed and victim-centred design principles to be used in moderation processes and interface design.
- Introduce mandatory gender impact assessments into the fundamental rights assessments required under the AI Act, including third-party audits to detect and correct algorithmic bias.
- Align platform age-verification, design and user-safety requirements with the European Commission's 2025 guidelines and prototype app for a safer online space for children.
- Ensure that these age-verification measures are implemented in a gender-sensitive way, recognising that girls face distinct risks in online settings.

Strengthen and ensure the enforcement of regulations on AI and emerging technologies.

- Ensure the enforcement of the AI Act.
- Ensure that existing EU AI governance instruments – including the ethics guidelines for trustworthy AI and Code of Practice on Marking and Labelling of AI-generated Content – are fully implemented and strengthened with binding accountability mechanisms.
- Advocate for the gender-related risks of generative AI, such as the production and dissemination of deepnudes, nudifying tools and other non-consensual synthetic imagery, to be listed as 'prohibited practices' under Article 5 of the AI Act.
- Ensure that the technical standards developed for AI providers include effective mechanisms for reporting complaints and following up on them, removing harmful content and informing victims of cyber violence about support services.
- Ensure that equality bodies and civil-society organisations working towards gender equality and fundamental rights at the national and EU levels are sufficiently equipped and financed to fulfil their role as consultative bodies under Article 77 of the AI Act.
- Ensure remedies and mechanisms are accessible to victims of AI-enabled violence.

Victim support and protection

Strengthen victim-centred support services and reporting mechanisms.

- Ensure that all Member States create reporting and support services for victims of cyber violence in line with existing obligations under the Istanbul Convention (Articles 20–22), the Victims' Rights Directive (2012/29/EU) and the EU Violence against Women Directive linked to rapid responses and specialised support services.
- Ensure that specialised support services focusing on violence against women are sufficiently equipped and financed to provide specialised, trauma-informed support, including technical support, mental health services and legal assistance.
- Ensure that specialised support for victims of cyber violence is tailored to different age groups of women and girls, based on their experiences and needs.
- Develop age-appropriate perpetrator intervention programmes specifically tailored to minors, recognising their developmental stage and the different accountability mechanisms that may apply.

Strengthen professionals' capacity to respond effectively.

- Provide mandatory training for frontline professionals (teachers, social workers, police, healthcare workers) on the gendered nature of cyber violence and platform-specific patterns.
- Establish national technical assistance points that allow practitioners to access cybersecurity expertise from public institutions or specialised civil-society organisations.
- Ensure sustainable funding for civil-society organisations conducting school interventions and for organisations specialising in digital and gender-equality awareness work for young people to prevent cyber violence and generative AI deepfakes.

Support families, caregivers and educators in early interventions and responses.

- Provide parents and caregivers with practical guidance on digital parenting, including tools and resources to help them detect and address online abuse early.
- Require schools and other educational institutions to establish clear policies and protocols on what to do in cases of technology-facilitated abuse to protect victims.
- Require schools and other educational institutions to define and communicate clear consequences for perpetrators of cyber violence (e.g. disciplinary records, notes on school reports, temporary or permanent expulsion and what is proposed in these cases).
- Raise awareness among parents and caregivers of civil legal avenues for victims to seek accountability and civil remedies.

Foster multistakeholder collaboration and innovation.

- Facilitate cooperation between governments, civil society, researchers, schools and other education centres, and technology companies by promoting the sharing of evidence and best practices across stakeholders to improve prevention and response.
- Introduce EU-level multistakeholder response protocols for schools and youth settings, clarifying the roles of educators, police, social services, platforms and cybersecurity bodies.
- Support the development of innovative technological solutions tailored to the rapidly evolving nature of cyber violence.

Monitoring and evaluation

Establish a harmonised EU monitoring and accountability framework.

- Ensure that national action plans are used to systematically track Member States' implementation of the Violence against Women Directive, including its provisions on prevention, protection, access to justice and cyber violence.
- Ensure the regular evaluation of Member State compliance to guarantee harmonised standards, identify enforcement gaps and support corrective action where obligations under the directive are not met.
- Advocate for the European Commission to issue periodic monitoring reports on cyber violence that are based on Member State data collection obligations under the Violence against Women Directive and the DSA.

Ensure data collection reflects the diversity of victims' experiences.

- In collaboration with relevant institutions at the EU and national levels, collect data on all forms of gender-based violence, including cyber violence, that can be disaggregated by sex, age, ethnicity, disability and socioeconomic status.
- Ensure that the specific experiences of groups facing intersecting forms of discrimination are captured in research and during data collection.
- Ensure that cyber violence and other forms of technology-facilitated violence against women are integrated in future EU-wide victimisation surveys.

Invest in long-term, evidence-based research on impacts and trends.

- In line with Article 44 of the Violence against Women Directive, ensure adequate budget allocation for specific research on cyber violence under the current and future multiannual financial framework.
- Support longitudinal research into understanding the long-term psychological impacts of cyber violence.
- Investigate the social and economic consequences of cyber violence over time.

References

- Adam, A. (2002), 'Cyberstalking and internet pornography: Gender and the gaze', Ethics and Information Technology, Vol. 4, Issue 2, pp. 133–142, https://doi.org/10.1023/A:1019967504762.
- Afrouz, R. and Vassos, S. (2024), 'Adolescents' experiences of cyber-dating abuse and the pattern of abuse through technology, a scoping review', Trauma, Violence, & Abuse, Vol. 25, Issue 4, pp. 2814–2828, https://doi.org/10.1177/15248380241227457.
- Allison, K. R. and Bussey, K. (2016), 'Cyber-bystanding in context: A review of the literature on witnesses' responses to cyberbullying', Children and Youth Services Review, Vol. 65, pp. 183–194, https://doi.org/10.1016/j.childyouth.2016.03.026.
- Assemblée nationale (2019), Loi No 2020-766 du mercredi 24 juin 2020 visant à lutter contre les contenus haineux sur internet, https://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.
- Azzarito, L., Simon, M. and Marttinen, R. (2017), '"Up against whiteness": Rethinking race and the body in a global era', Sport, Education and Society, Vol. 22, Issue 5, pp. 635–657, https://doi.org/10.1080/13573322.2015.1136612.
- Baas, N., de Jong, M. D. T. and Drossaert, C. H. C. (2013), 'Children's perspectives on cyberbullying: Insights based on participatory research', Cyberpsychology, Behavior, and Social Networking, Vol. 16, Issue 4, pp. 248–253, https://doi.org/10.1089/cyber.2012.0079.
- Backe, E. L., Lilleston, P. and McCleary-Sills, J. (2018), 'Networked individuals, gendered violence: A literature review of cyberviolence', Violence and Gender, Vol. 5, Issue 3, pp. 135–146, https://doi.org/10.1089/vio.2017.0056.
- Barlińska, J., Szuster, A. and Winiewski, M. (2013), 'Cyberbullying among adolescent bystanders: Role of the communication medium, form of violence, and empathy', Journal of Community & Applied Social Psychology, Vol. 23, Issue 1, pp. 37–51, https://doi.org/10.1002/casp.2137.
- Chawki, M., Basu, S. and Choi, K. (2024), 'Redefining boundaries in the metaverse: Navigating the challenges of virtual harm and user safety', Laws, Vol. 13, No 3, https://www.mdpi.com/2075-471X/13/3/33.
- Chiang, J., Chang, F. and Lee, K. (2021), 'Transitions in aggression among children: Effects of gender and exposure to online violence', Aggressive Behavior, Vol. 47, Issue 3, pp. 310–319, https://doi.org/10.1002/ab.21944.

- Connell, R. W. (2005), Masculinities, 2nd edition, Polity Press, Cambridge.
- Cosma, A., Molcho, M. and Pickett, W. (2024), A focus on adolescent peer violence and bullying in Europe, central Asia and Canada – Health Behaviour in School-aged Children: International report from the 2021/2022 survey, Volume 2, WHO Regional Office for Europe, Copenhagen, https://www.who.int/europe/publications/i/item/9789289060929.
- Council of Europe (2001), 'Convention on Cybercrime', European Treaty Series, No 185, Budapest, 23 November, https://rm.coe.int/1680081561.
- Council of Europe (2007), 'Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse', Council of Europe Treaty Series, No 201, 25 October, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201.
- Council of Europe (2011), 'Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence', Council of Europe Treaty Series, No 210, https://rm.coe.int/168008482e.
- Council of Europe (2018), Mapping Study on Cyberviolence: With recommendations adopted by the T-CY on 9 July 2018, Cybercrime Convention Committee, Strasbourg, https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914.
- Council of Europe (2020), Handbook for policy makers on the rights of the child in the digital environment, Strasbourg.
- Council of Europe (2023), Risks and Opportunities of the Metaverse.
- Cybersafe (2020), Cyber Violence against Women & Girls – Report, University of Ljubljana.
- DeKeseredy, W. S. and Schwartz, M. D. (2013), Male Peer Support and Violence against Women: The history and verification of a theory, Northeastern University Press, Boston, MA.
- De Vido, S. (2024), 'Deep fake as AI-generated violence against women', speech at the Global Conference on AI and Human Rights, Ljubljana, 13 and 14 June.
- Domínguez-Hernández, F., Bonell, L. and Martínez-González, A. (2018), 'A systematic literature review of factors that moderate bystanders' actions in cyberbullying', Cyberpsychology: Journal of Psychosocial Research on Cyberspace, Vol. 12, No 4, https://doi.org/10.5817/CP2018-4-1.
- Dunn, S. (2020), 'Technology-facilitated Gender-based Violence: An overview', Supporting a Safer Internet Papers, No 1, Centre for International Governance Innovation, Waterloo, Canada, https://www.jstor.org/stable/resrep27513.
- EIGE (2021), Artificial Intelligence, Platform Work and Gender Equality, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2839/53252.
- EIGE (2022), Combating Cyber Violence against Women and Girls, Publications Office of the European Union, Luxembourg, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf.
- EIGE (2024), Tackling Cyber Violence against Women and Girls: The role of digital platforms, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2839/1955989.
- EIGE (2025) Perception to Policy: Dismantling gender stereotypes in the European Union, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2839/7052284.

- eSafety's Commissioner and the Australian Communications and Media Authority (ACMA), 2022. Annual report 2021-2022, https://www.esafety.gov.au/sites/default/files/2022-10/ACMA%20and%20eSafety%20annual%20report%202021-22.pdf?v=1776941478076
- European Parliament (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
- European Parliament (2021a), European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL)) (OJ C 251, 30.6.2022, p. 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_251_R_0002).
- European Parliament: Directorate-General for Parliamentary Research Services (2024), 'Cyberviolence against women in the EU', https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.
- Europol (European Union Agency for Law Enforcement Cooperation) (2017), Online sexual coercion and extortion as a form of crime affecting children – Law enforcement perspective, The Hague, online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.
- EWL (European Women's Lobby) (2017), #HerNetHerRights: Mapping the state of online violence against women & girls in Europe, Brussels.
- FEMM Committee (Committee on Women's Rights and Gender Equality) and van der Wilk, A. (2018), Cyber Violence and Hate Speech Online against Women.
- Foster A. (2023). Australian teenagers targeted by sick sextortion scams. News.com.au. https://www.news.com.au/technology/online/security/australian-teenagers-targeted-by-sick-sextortion-scams/news-story/ae6975b8308917f611b03fa99bd2b0d9
- FRA (European Union Agency for Fundamental Rights) (2015), Violence against Women – An EU-wide survey: Main results, Publications Office of the European Union, Luxembourg.
- FRA (2017), Second European Union Minorities and Discrimination Survey – Muslims: Selected findings, Publications Office of the European Union, Luxembourg, https://doi.org/10.2811/072254.
- Freed, D., Consolvo, S., Cosley, D., Kelley, P. G., Ricart, E. et al. (2025), 'Help-seeking and coping strategies for technology-facilitated abuse experienced by youth', Proceedings of the ACM on Human–Computer Interaction, Vol. 9, Issue 2, pp. 1–25, https://doi.org/10.1145/3710992.
- Gámez-Guadix, M., Sorrel, M. A. and Martínez-Bacaico, J. (2022), 'Technology-facilitated sexual violence perpetration and victimization among adolescents: A network analysis', Sexuality Research and Social Policy, Vol. 20, pp. 1000–1012, https://doi.org/10.1007/s13178-022-00775-y.
- Gius, C. (2023), '(Re)thinking gender in cyber-violence. Insights from awareness-raising campaigns on online violence against women and girls in Italy', Media Education, Vol. 14. No 2, pp. 95–106, https://doi.org/10.36253/me-14896.
- Government of Belgium (2021), Plan d'action national de lutte contre les violences basées sur le genre
- Gilen, A., Van Damme, E., Walrave, M., Giacometti, M., Ponnet, K., & Hardyns, W. (2025). Les violences numériques dans le contexte du dating et des relations entre partenaires en Belgique. Institut pour l'égalité des femmes et des hommes, https://igvm-iefh.belgium.be/fr/documentation/les-violences-numeriques-dans-le-contexte-du-dating-et-des-relations-entre-ex
- GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence) (2021), GREVIO General Recommendation No. 1 on the digital dimension of violence against women – Adopted

on 20 October 2021, Council of Europe, Strasbourg, https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

- Gurumurthy, A. and Menon, N. (2009), 'Violence against women via cyberspace', Economic and Political Weekly, Vol. 44, No 40, pp. 19–21, https://www.jstor.org/stable/25663650.
- Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV), Institute of Development Studies, https://doi.org/10.19088/K4D.2021.140.
- Janickyj, M. and Tanczer, L. M. (2025), 'Tech abuse personas: Exploring help-seeking behaviours and support needs of victim/survivors of technology-facilitated abuse', Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, 509, pp. 1–11, https://doi.org/10.1145/3706599.3719986.
- Koukopoulos, N., Janickyj, M. and Tanczer, L. M. (2025), 'Defining and conceptualizing technology-facilitated abuse (''tech abuse''): Findings of a global Delphi study', Journal of Interpersonal Violence, Vol. 41, Issue 1–2, https://doi.org/10.1177/08862605241310465.
- Leonhardt, M. and Overå, S. (2021), 'Are there differences in video gaming and use of social media among boys and girls? – A mixed methods approach', International Journal of Environmental Research and Public Health, Vol. 18, No 11, https://doi.org/10.3390/ijerph18116085.
- López-Castro, L. and Priegue, D. (2019), 'Influence of family variables on cyberbullying perpetration and victimization: A systematic literature review', Social Sciences, Vol. 8, No 3, 98, https://doi.org/10.3390/socsci8030098.
- López-Castro, L., Smith, P. K., Robinson, S. and Görzig, A. (2023), 'Age differences in bullying victimisation and perpetration: Evidence from cross-cultural surveys', Aggression and Violent Behavior, Vol. 73, 101888, https://doi.org/10.1016/j.avb.2023.101888.
- Lu, Y., Van Ouytsel, J. and Temple, J. R. (2021), 'In-person and cyber dating abuse: A longitudinal investigation', Journal of Social and Personal Relationships, Vol. 38, Issue 12, pp. 3713–3731, https://doi.org/10.1177/02654075211065202.
- Machado, B., Caridade, S., Araújo, I. and Lobato Faria, P. (2022), 'Mapping the cyber interpersonal violence among young populations: A scoping review', Social Sciences, Vol. 11, No 5, 207, https://doi.org/10.3390/socsci11050207.
- McGraw, D. K. (1995), 'Sexual harassment in cyberspace: The problem of unwelcome e-mail', Rutgers Computer and Technology Law Journal, Vol. 21, pp. 491–518, https://api.semanticscholar.org/CorpusID:64276291.
- Mclocklin, G., Kellezi, B., Stevenson, C. and Mackay, J. (2024), 'Disclosure decisions and help-seeking experiences amongst victim-survivors of non-consensual intimate image distribution', Victims & Offenders, Vol. 20, Issue 7, pp. 1258–1284, https://doi.org/10.1080/15564886.2024.2329107.
- Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei, A., Sadiq, A. S. et al. (2024), 'The roots of digital aggression: Exploring cyber-violence through a systematic literature review', International Journal of Information Management Data Insights, Vol. 4, Issue 2, 100281, https://doi.org/10.1016/j.jjimei.2024.100281.
- Murphy, C. (2024), 'Cyberbullying among young people: Laws and policies in selected Member States', European Parliamentary Research Service Briefing, PE 7662.331, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI(2024)762331_EN.pdf.
- National Academies of Sciences, Engineering, and Medicine (2024), 'The relation between social media and health', in: Social Media and Adolescent Health, National Academies Press, Washington, DC, pp. 91–136.
- Nixon, C. L. (2014) 'Current perspectives: The impact of cyberbullying on adolescent health', Adolescent Health, Medicine and Therapeutics, 5, pp. 143–158, https://doi.org/10.2147/AHMT.S36456.

- OAS (Organization of American States) (2021), Online Gender-based Violence against Women and Girls: Guide of basic concepts, United States Department of State, Washington, DC.
- Odink, I. (2024), 'Combating child sexual abuse: Revising Directive (2011/93/EU) – recast', European Parliamentary Research Service Briefing, PE 762.374, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762374.
- Pichel, R., Foody, M., O'Higgins Norman, J., Feijóo, S., Varela, J. et al. (2021), 'Bullying, cyberbullying and the overlap: What does age have to do with it?', Sustainability, Vol. 13, No 15, https://doi.org/10.3390/su13158527.
- PLAN International (2020), State of the World's Girls 2020: Free to be online? Girls' and young women's experiences of online harassment, Woking.
- Powell, A. and Henry, N. (2017), Sexual Violence in a Digital Age, Palgrave Macmillan, London.
- Project deSHAME (Digital Exploitation and Sexual Harassment Among Minors in Europe) (2017), Young People's Experiences of Online Sexual Harassment: A cross-country report, London.
- Ratajczak, M. and Galzignato, E. (2019), 'Migrant children and cyber-violence. The problem of hate speech in Italy and Poland', Peace Human Rights Governance, Vol. 3, Issue 3, pp. 365–388.
- Ray, A. and Henry, N. (2024), 'Sextortion: A scoping review', Trauma, Violence, & Abuse, Vol. 26, Issue 1, https://doi.org/10.1177/15248380241277271.
- Rudnicki, K., Vandebosch, H., Voué, P. and Poels, K. (2023), 'Systematic review of determinants and consequences of bystander interventions in online hate and cyberbullying among adults', Behaviour & Information Technology, Vol. 42, Issue 5, pp. 527–544, https://doi.org/10.1080/0144929X.2022.2027013.
- Sala, A., Porcaro, L. and Gómez, E. (2024), 'Social media use and adolescents' mental health and well-being: An umbrella review', Computers in Human Behavior Reports, Vol. 14, https://doi.org/10.1016/j.chbr.2024.100404.
- Salazar, M., Raj, A., Silverman, J. G., Rusch, M. L. A., and Reed, E. (2023), 'Cyber sexual harassment among adolescent girls: A qualitative analysis', Adolescents, Vol. 3, No 1, pp. 84–91, https://doi.org/10.3390/adolescents3010007.
- Schittenhelm, C., Kops, M., Moosburner, M., Fischer, M. S. and Wachs, S. (2024), 'Cybergrooming victimization among young people: A systematic review of prevalence rates, risk factors, and outcomes', Adolescent Research Review, Vol. 10, pp. 169–200, https://doi.org/10.1007/s40894-024-00248-w.
- Sciacca, B., Mazzone, A., Loftsson, M., O'Higgins Norman, J. and Foody, M. (2023), 'Nonconsensual dissemination of sexual images among adolescents: Associations with depression and self-esteem', Journal of Interpersonal Violence, Vol. 38, Issue 15–16, pp. 9438–9464, https://doi.org/10.1177/08862605231165777.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E. et al. (2020), EU Kids Online 2020: Survey results from 19 countries, EU kids online, https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf.
- Smith, D. (2023), 'How deception plays a role in online dating and dating apps', Canadian Journal of Family and Youth, Vol. 15, No 2, pp. 23–32, https://doi.org/10.29173/cjfy29869.
- Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T. et al. (2010) 'Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study', Archives of General Psychiatry, Vol. 67, No 7, pp. 720–728, https://doi.org/10.1001/archgenpsychiatry.2010.79.
- Šulc, A., Vehovar, V., Brečko, B., Rucman, A. B. and Krainer, A. (2024), 'Differences in cyberbullying victimisation and perpetration according to age and locality in Slovenia', Revija za kriminalistiko in kriminologijo, Vol. 72, Issue 4, pp. 337–349, http://www.dlib.si/?URN=URN:NBN:SI:doc-F7LDTW5D.

- Sutton, S. and Finkelhor, D. (2023), 'Perpetrators' identity in online crimes against children: A meta-analysis', Trauma, Violence, & Abuse, Vol. 25, Issue 3, pp. 1756–1768, https://doi.org/10.1177/15248380231194072.
- Thorn. (2024). New Research from Thorn: Financial Sextortion on the Rise, Targeting Teen Boys. https://www.thorn.org/blog/new-research-from-thorn-financial-sextortion-on-the-rise-tar geting-teen-boys/
- UN Women and WHO (World Health Organization) (2023), Technology-facilitated Violence against Women: Taking stock of evidence and data collection, https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection.
- UN Women (2024b), Youth Guide to End Online Gender-based Violence, Version 3.
- United Nations (2018), A/HRC/38/47: Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, Office of the United Nations High Commissioner for Human Rights, Geneva, 18 June, https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.
- USAID (United States Agency for International Development) (2023), DRG Learning Digest – Combatting technology-facilitated gender-based violence in politics, March, https://content.govdelivery.com/accounts/USAIDHQ/bulletins/34c7e57.
- Van Ouytsel, J., Ponnet, K. and Walrave, M. (2020), 'Cyber dating abuse: Investigating digital monitoring behaviors among adolescents from a social learning perspective', Journal of Interpersonal Violence, Vol. 35, Issue 23–24, pp. 5157–5178, https://doi.org/10.1177/0886260517719538.
- Vogels, E. A. (2022), Teens and Cyberbullying 2022, Pew Research Center, 15 December, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
- Vogler, S., Kappel, R. and Mumford, E. (2023), 'Experiences of technology-facilitated abuse among sexual and gender minorities', Journal of Interpersonal Violence, Vol. 38, Issue 19–20, 11290–11313, https://doi.org/10.1177/08862605231179724.
- Wajcman, J. (2004), TechnoFeminism, Polity Press, Cambridge.
- Wajcman, J. (2010), 'Feminist theories of technology', Cambridge Journal of Economics, Vol. 34, Issue, 1, pp. 143–152, https://doi.org/10.1093/cje/ben057.
- Wajcman, J. (2015), Pressed for Time: The acceleration of life in digital capitalism, University of Chicago Press, Chicago.
- Wallace, A., Langevin, R. and Hébert, M. (2023), 'An analysis of risk and protective factors associated with cyber-dating violence victimization of adolescent girls: An ecological perspective', Journal of Child & Adolescent Trauma, Vol. 16, No 4, pp. 1017–1029, https://doi.org/10.1007/s40653-023-00558-6.
- WeProtect Global Alliance (2016), Preventing and Tackling Child Sexual Exploitation and Abuse: A model national response, London.
- WeProtect Global Alliance (2021), Child 'Self-generated' Sexual Material Online: Children and young people's perspectives, London.
- WeProtect Global Alliance (2024), World's first estimate of the scale of online child sexual exploitation and abuse,'' Available: https://www.weprotect.org/blog/worlds-first-estimate-of-the-scale-ofonline-child-sexual-exploitation-and-abuse/
- Zweig, J. M., Lachman, P., Yahner, J. and Dank, M. (2014), 'Correlates of cyber dating abuse among teens', Journal of Youth and Adolescence, Vol. 43, No 8, pp. 1306–1321, https://doi.org/10.1007/s10964-013-0047-x.

- Office of the Government of the Czech Republic (2021), Gender Equality Strategy for 2021–2030: Updated version, Prague, https://vlada.gov.cz/assets/ppov/rovne-prilezitosti-zen-a-muzu/dokumenty/Updated-Gender-Equality-Strategy-2021-2030---Condensed-Version.pdf.
- Olenik-Shemesh, D., Heiman, T. and Eden, S. (2017), 'Bystanders' behavior in cyberbullying episodes: Active and passive patterns in the context of personal–socio-emotional factors', Journal of Interpersonal Violence, Vol. 32, Issue 1, pp. 23–48, https://doi.org/10.1177/0886260515585531.
- Penado-Abilleira, M. and Rodicio-García, M. L. (2018), 'Development and validation of an adolescent gender-based violence scale (ESVIGA)', Anuario de Psicología Jurídica, Vol. 28, No 1, pp. 49–57, https://doi.org/10.5093/apj2018a10.
- Pichel, R., Foody, M., O'Higgins Norman, J., Feijóo, S., Varela, J. et al. (2021), 'Bullying, cyberbullying and the overlap: What does age have to do with it?', Sustainability, Vol. 13, No 15, https://doi.org/10.3390/su13158527.
- Pietkiewicz, M. and Treder, M. (2018), 'Cyberstalking in social media – Polish view', Journal of Modern Science, Vol. 38, pp. 29–40, https://doi.org/10.13166/jms/99217.
- PLAN International (2020), State of the World's Girls 2020: Free to be online? Girls' and young women's experiences of online harassment, Woking.
- Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K. and Aboulez, N. (2021), The Chilling: Global trends in online violence against women journalists, UNESCO, Paris.
- Powell, A. and Henry, N. (2017), Sexual Violence in a Digital Age, Palgrave Macmillan, London.
- Pozza, V. D. (2024), Report on Cyber Violence against Women – Policy overview and recommendations, European Women's Lobby, Brussels.
- Project deSHAME (Digital Exploitation and Sexual Harassment Among Minors in Europe) (2017), Young People's Experiences of Online Sexual Harassment: A cross-country report, London.
- Ratajczak, M. and Galzignato, E. (2019), 'Migrant children and cyber-violence. The problem of hate speech in Italy and Poland', Peace Human Rights Governance, Vol. 3, Issue 3, pp. 365–388.
- Ray, A. and Henry, N. (2024), 'Sextortion: A scoping review', Trauma, Violence, & Abuse, Vol. 26, Issue 1, https://doi.org/10.1177/15248380241277271.
- Rigotti, C. and Malgieri, G. (2024), Sexual Violence and Harassment in the Metaverse: A new manifestation of gender-based harms, Alliance for Universal Digital Rights, Equality Now and Vulnera (International Observatory on Vulnerable People in Data Protection).
- Rodríguez Ramos, M. S. and Zarzalejos, J. (2024) 'Revision of the victims' rights acquis', https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-revision-of-the-victims-rights-acquis.
- Rudnicki, K., Vandebosch, H., Voué, P. and Poels, K. (2023), 'Systematic review of determinants and consequences of bystander interventions in online hate and cyberbullying among adults', Behaviour & Information Technology, Vol. 42, Issue 5, pp. 527–544, https://doi.org/10.1080/0144929X.2022.2027013.
- Safer Internet Centre Lithuania (2019), Safer Internet Centre Lithuania: Public report January 2019–December 2020, National Agency of Education, Vilnius, https://www.draugiskasinternetas.lt/wp-content/uploads/2021/03/English_2019-2020.pdf.
- Sala, A., Porcaro, L. and Gómez, E. (2024), 'Social media use and adolescents' mental health and well-being: An umbrella review', Computers in Human Behavior Reports, Vol. 14, https://doi.org/10.1016/j.chbr.2024.100404.

- Salazar, M., Raj, A., Silverman, J. G., Rusch, M. L. A., and Reed, E. (2023), 'Cyber sexual harassment among adolescent girls: A qualitative analysis', Adolescents, Vol. 3, No 1, pp. 84–91, https://doi.org/10.3390/adolescents3010007.
- Sales, N. J. (2024), 'A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future?', The Guardian, 5 January, https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta.
- Sánchez-Jiménez, V., Rodríguez-deArriba, M. and Muñoz-Fernández, N. (2022), 'Is this WhatsApp conversation aggressive? Adolescents' perception of cyber dating aggression', Journal of Interpersonal Violence, Vol. 37, Issue 19–20, pp. NP17369–NP17393, https://doi.org/10.1177/08862605211028011.
- Schittenhelm, C., Kops, M., Moosburner, M., Fischer, M. S. and Wachs, S. (2024), 'Cybergrooming victimization among young people: A systematic review of prevalence rates, risk factors, and outcomes', Adolescent Research Review, Vol. 10, pp. 169–200, https://doi.org/10.1007/s40894-024-00248-w.
- Sciacca, B., Mazzone, A., Loftsson, M., O'Higgins Norman, J. and Foody, M. (2023), 'Nonconsensual dissemination of sexual images among adolescents: Associations with depression and self-esteem', Journal of Interpersonal Violence, Vol. 38, Issue 15–16, pp. 9438–9464, https://doi.org/10.1177/08862605231165777.
- Scott, A., Semmens, L. and Willoughby, L. (2001), 'Women and the internet: The natural history of a research project', in: Adam, A. and Green, E. (eds), Virtual Gender: Technology, consumption and identity matters, Routledge, Abingdon.
- Secretariat of the Lanzarote Committee (2018), Guidelines for Implementation of Child Participation, https://rm.coe.int/guidelines-for-implementation-of-child-participation/1680790571.
- Singh, P., Smith, M. V., Raba, C. M. and Keller, J. (2016), 'Cyber-intimate partner violence and mental health outcomes in a sample of high school girls', MedCrave Online Journal of Public Health, Vol. 4, Issue 3, pp. 67–70, https://doi.org/10.15406/mojph.2016.04.00078.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E. et al. (2020), EU Kids Online 2020: Survey results from 19 countries, EU kids online, https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf.
- Smith, A. (2024), 'Rape in virtual reality: How to police the metaverse', Context website, 24 January, https://www.context.news/digital-rights/sex-assault-claims-and-crime-raise-fears-of-new-virtual-wild-west.
- Smith, D. (2023), 'How deception plays a role in online dating and dating apps', Canadian Journal of Family and Youth, Vol. 15, No 2, pp. 23–32, https://doi.org/10.29173/cjfy29869.
- Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T. et al. (2010) 'Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study', Archives of General Psychiatry, Vol. 67, No 7, pp. 720–728, https://doi.org/10.1001/archgenpsychiatry.2010.79.
- Steinvik, H. R., Duffy, A. L. and Zimmer-Gembeck, M. J. (2023), 'Bystanders' responses to witnessing cyberbullying: The role of empathic distress, empathic anger, and compassion', International Journal of Bullying Prevention, Vol. 6, pp. 399–410, https://doi.org/10.1007/s42380-023-00164-y.
- Šulc, A., Vehovar, V., Brečko, B., Rucman, A. B. and Krainer, A. (2024), 'Differences in cyberbullying victimisation and perpetration according to age and locality in Slovenia', Revija za kriminalistiko in kriminologijo, Vol. 72, Issue 4, pp. 337–349, http://www.dlib.si/?URN=URN:NBN:SI:doc-F7LDTW5D.
- Sutton, S. and Finkelhor, D. (2023), 'Perpetrators' identity in online crimes against children: A meta-analysis', Trauma, Violence, & Abuse, Vol. 25, Issue 3, pp. 1756–1768, https://doi.org/10.1177/15248380231194072.

- Torek, B. (2025), 'Meta's new policies: How they Endanger LGBTQ+ communities and our tips for staying safe online', Human Rights Campaign website, 15 January, https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online.
- UN Women (United Nations Entity for Gender Equality and the Empowerment of Women) (2021), A guide for women and girls to prevent and respond to cyberviolence.
- UN Women (2022), Accelerating efforts to tackle online and technology facilitated violence against women and girls (VAWG), UN Women policy paper.
- UN Women and WHO (World Health Organization) (2023), Technology-facilitated Violence against Women: Taking stock of evidence and data collection, https://www.unwomen.org/en/digital-library/publications/2023/04technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection.
- UN Women (2024a), Technology-facilitated Gender-based Violence: Developing a shared research agenda, https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda.
- UN Women (2024b), Youth Guide to End Online Gender-based Violence, Version 3.
- UNESCO (United Nations Educational, Scientific and Cultural Organization) (2023), 'Your Opinion Doesn't Matter, Anyway': Exposing technology-facilitated gender-based violence in an era of generative AI, Paris.
- United Nations (2018), A/HRC/38/47: Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, Office of the United Nations High Commissioner for Human Rights, Geneva, 18 June, https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.
- United Nations (2024), 'Cyberviolence against women and girls: The growing threat of the digital age', United Nations Regional Information Centre for Western Europe website, 5 December, https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/.
- USAID (United States Agency for International Development) (2023), DRG Learning Digest – Combatting technology-facilitated gender-based violence in politics, March, https://content.govdelivery.com/accounts/USAIDHQ/bulletins/34c7e57.
- Vallance, C. (2024), 'Police investigate virtual sex assault on girl's avatar', BBC News website, 2 January, https://www.bbc.com/news/technology-67865327.
- Van Ouytsel, J., Ponnet, K. and Walrave, M. (2020), 'Cyber dating abuse: Investigating digital monitoring behaviors among adolescents from a social learning perspective', Journal of Interpersonal Violence, Vol. 35, Issue 23–24, pp. 5157–5178, https://doi.org/10.1177/0886260517719538.
- Vogels, E. A. (2022), Teens and Cyberbullying 2022, Pew Research Center, 15 December, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
- Vogler, S., Kappel, R. and Mumford, E. (2023), 'Experiences of technology-facilitated abuse among sexual and gender minorities', Journal of Interpersonal Violence, Vol. 38, Issue 19–20, 11290–11313, https://doi.org/10.1177/08862605231179724.
- Waasdorp, T. E. and Bradshaw, C. P. (2014), 'The overlap between cyberbullying and traditional bullying', Journal of Adolescent Health, Vol. 56, Issue 5, pp. 483–488, https://doi.org/10.1016/j.jadohealth.2014.12.00.
- Wajcman, J. (2004), TechnoFeminism, Polity Press, Cambridge.
- Wajcman, J. (2010), 'Feminist theories of technology', Cambridge Journal of Economics, Vol. 34, Issue, 1, pp. 143–152, https://doi.org/10.1093/cje/ben057.

- Wajcman, J. (2015), Pressed for Time: The acceleration of life in digital capitalism, University of Chicago Press, Chicago.
- Wallace, A., Langevin, R. and Hébert, M. (2023), 'An analysis of risk and protective factors associated with cyber-dating violence victimization of adolescent girls: An ecological perspective', Journal of Child & Adolescent Trauma, Vol. 16, No 4, pp. 1017–1029, https://doi.org/10.1007/s40653-023-00558-6.
- WeProtect Global Alliance (2016), Preventing and Tackling Child Sexual Exploitation and Abuse: A model national response, London.
- WeProtect Global Alliance (2021), Child 'Self-generated' Sexual Material Online: Children and young people's perspectives, London.
- WWWF (World Wide Web Foundation) (2024), Perpetrators of Gender-based Violence Online: Roadmap for investigations, Washington, DC.
- WWWF and World Association of Girl Guides and Girls Scouts (2020), Survey – Young people's experience of online harassment, Washington DC, https://ureport.in/opinion/3983/.
- Wright, M. F. (2017), 'Adolescents' perceptions of popularity-motivated behaviors, characteristics, and relationships in cyberspace and cyber aggression: The role of gender', Cyberpsychology, Behavior and Social Networking, Vol. 20, Issue 6, pp. 355–361, https://doi.org/10.1089/cyber.2016.0693.
- Wright, M. F. (2020), 'The role of technologies, behaviors, gender, and gender stereotype traits in adolescents' cyber aggression', Journal of Interpersonal Violence, Vol. 35, Issue 7–8, pp. 1719–1738, https://doi.org/10.1177/0886260517696858.
- Wright, M. F. and Wachs, S. (2020), 'Adolescents' cyber victimization: The influence of technologies, gender, and gender stereotype traits', International Journal of Environmental Research and Public Health, Vol. 17, No 4, 1293, https://doi.org/10.3390/ijerph17041293.
- Xu, Y. and Trzaskawka, P. (2021), 'Towards descriptive adequacy of cyberbullying: Interdisciplinary studies on features, cases and legislative concerns of cyberbullying', International Journal for the Semiotics of Law, Vol. 34, No 4, pp. 929–943, https://doi.org/10.1007/s11196-021-09856-4.
- Yoon, J. (2022), 'Can we do anything about sexual crimes in the metaverse?', Inside Compliance website, 6 October, https://blogs.luc.edu/compliance/?p=4849.
- Zamfir, I. and Murphy, C. (2024), 'Cyberviolence against women in the EU', European Parliamentary Research Service Briefing, PE 7677.146, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.
- Zweig, J. M., Lachman, P., Yahner, J. and Dank, M. (2014), 'Correlates of cyber dating abuse among teens', Journal of Youth and Adolescence, Vol. 43, No 8, pp. 1306–1321, https://doi.org/10.1007/s10964-013-0047-x.

Annex

Boxes

Box 8: Details of the methodological approach used for the study

Desk research and literature review

The first stage of the study consisted of systematic desk research and a literature review, which provided the conceptual and empirical grounding for the study. Key studies and policy documents were identified using databases such as Google Scholar and Semantic Scholar. While Google Scholar was used for broad initial screening, Semantic Scholar enabled a more targeted search with its AI-supported recommendations and citation analysis. Publication date (with priority given to 2019–2024) and relevance to the study's objectives were the key inclusion criteria. Earlier works were included when necessary to trace the evolution of debates or to provide historical depth.

The review encompassed a wide range of sources: peer-reviewed articles, academic books, reports produced by international and European institutions (e.g. EIGE, UN, the World Bank), studies from NGOs and EU-wide women's rights organisations (e.g. European Women's Lobby, WAVE) and reports, papers and other outputs from EU-funded research. Grey literature, including documents from associations, specialised journals and press articles, was also incorporated to capture ongoing debates and emerging concerns. The software Zotero was used to manage references and classify literature according to keywords and themes. Tags allowed us to group studies by specific research questions or methodological approaches, ensuring a well-structured and easily retrievable evidence base.

Mapping of policy measures and legal provisions

Building on the literature review, the study carried out a systematic mapping of relevant policy frameworks and legal provisions at the international, European and national levels. This mapping aimed to identify the regulatory architecture addressing cyber violence and to highlight convergences and divergences among Member States. The process drew on a wide range of official sources, including the European Court of Human Rights (HUDOC) database, GREVIO

monitoring reports, the Council of Europe's online library, EIGE's legal definitions repository and the European Forum of Official Gazettes.

Snowballing techniques further ensured that national laws and new policy measures were captured in addition to the initial sample of documents. This approach provided a comprehensive picture of the policy and legal landscape in the EU, emphasising both common trends and specific national approaches.

Statistical data analysis

Quantitative analysis helped contextualise the research by examining the prevalence and dynamics of cyber violence across Member States. At the EU level, the analysis drew on statistics from the EU-GBV Survey, the FRA–EIGE EU Gender-based Violence Survey and the HBSC Survey.

National surveys and data collected by NGOs and umbrella organisations were also examined. International comparative surveys (e.g. from Plan International and the Pew Research Center) added further perspectives, while EU-funded projects such as EU kids online provided detailed insights into children and adolescents' online behaviours. The triangulation of these sources allowed the study to quantify trends and situate its qualitative findings within wider structural dynamics.

Focus groups and qualitative design

The second pillar of the methodology was qualitative fieldwork, which was designed to capture the lived experiences of adolescents in their own voices. A total of 37 focus groups were conducted across 10 Member States (Belgium, Germany, Estonia, Ireland, Spain, Italy, Cyprus, Poland, Romania and Sweden), involving 133 girls aged 13–18 and 38 boys aged 15–18. The decision to use focus groups was grounded in feminist and participatory principles: participants were not treated merely as informants but as knowledge-holders capable of articulating the ways in which gendered power relations and social norms shape their experiences of online harm.

Group discussions were structured around tailored discussion guides adapted to different age groups. For younger participants (aged 13–15), the discussion guides included interactive activities (e.g. word clouds, games such as Kahoot) and a vignette about a fictional character experiencing cyber harassment, to encourage reflection without requiring personal disclosure. For older adolescents (aged 16–18), the discussion guides included more complex scenarios, such as pressure to share intimate images and subsequent online harassment, allowing for deeper engagement with the themes of digital consent and reputational harm. The focus groups with boys focused on social norms, masculinity, bystander behaviour and empathy. In line with the project's ethics and safeguarding policy, discussions with girls and boys also addressed the potential support mechanisms available after experiences of cyber violence. Recruitment strategies ensured diversity in socioeconomic background, ethnicity and educational settings, while prioritising psychological safety. Focus groups were held in youth-friendly and accessible venues such as schools, community centres and libraries. Informed parental consent and participant assent were obtained in all cases.

Data analyses and safeguarding measures

Data analysis was carried out using a combined thematic and synthesis approach. Focus group discussions were transcribed, coded and analysed using NVivo software. The coding categories included forms of cyber violence, perceived causes, impacts, coping strategies, barriers to reporting and institutional responses. Coding was both inductive, allowing new themes to emerge

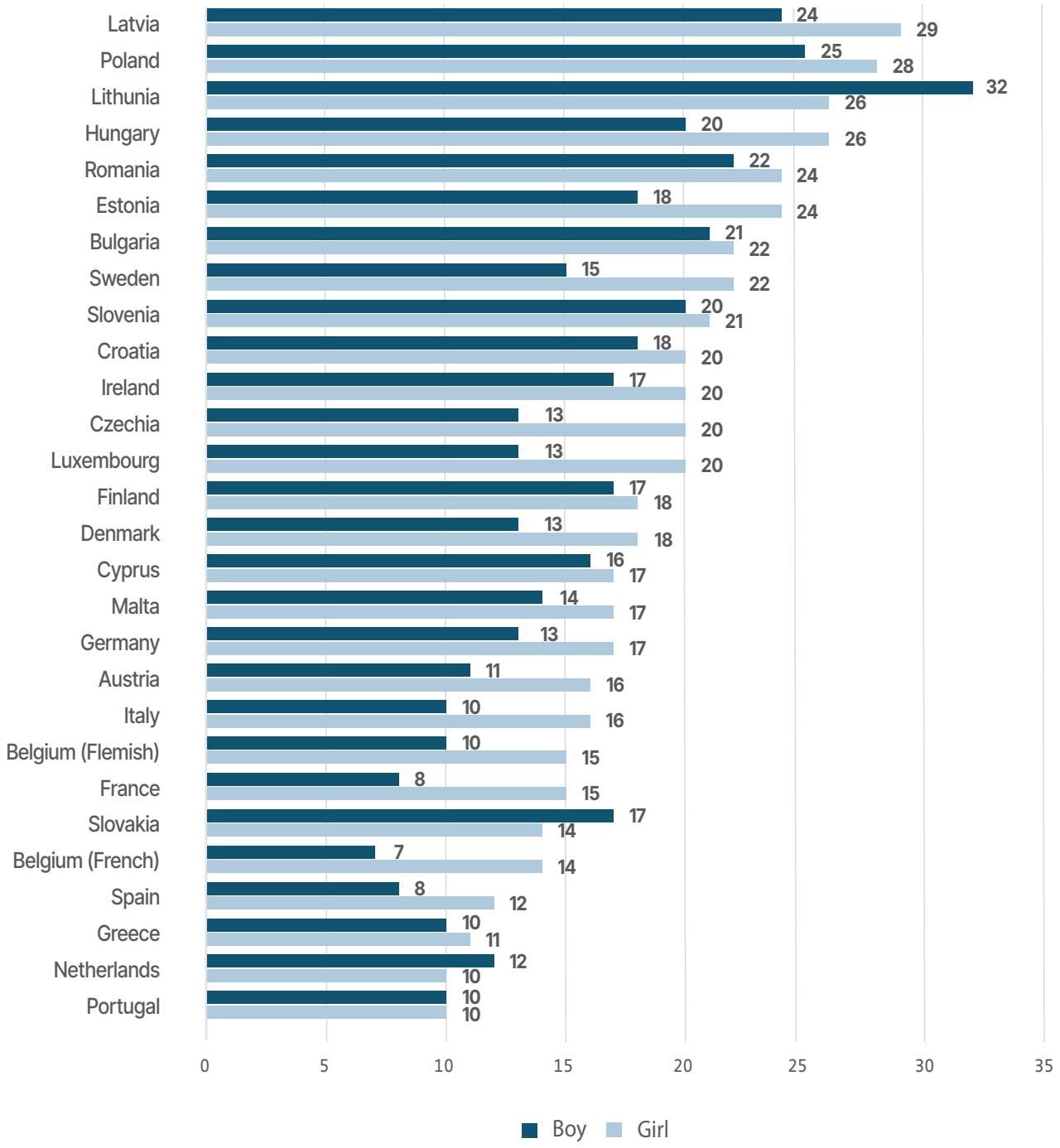
directly from the data, and deductive, guided by predefined research questions and the study's theoretical framework.

The thematic analysis was complemented by a synthesis analysis to compare findings across age groups and Member States, enabling the identification of shared patterns and contextual variations. Triangulation with quantitative data and policy findings further reinforced the robustness of the analysis. This multilayered framework ensured that adolescents' subjective accounts were interpreted against the backdrop of structural evidence.

Given the sensitive nature of the research and the participation of minors, strong ethical safeguards were applied. The study was conducted in compliance with WHO guidelines and institutional child protection frameworks. Informed consent and assent procedures were central to the design: guardians received detailed information on the study's objectives and procedures, while adolescents were given the agency to assent or withdraw at any point. Safeguarding measures included trained facilitators, confidentiality guarantees and the continuous monitoring of participants' well-being before, during and after the sessions.

Figures

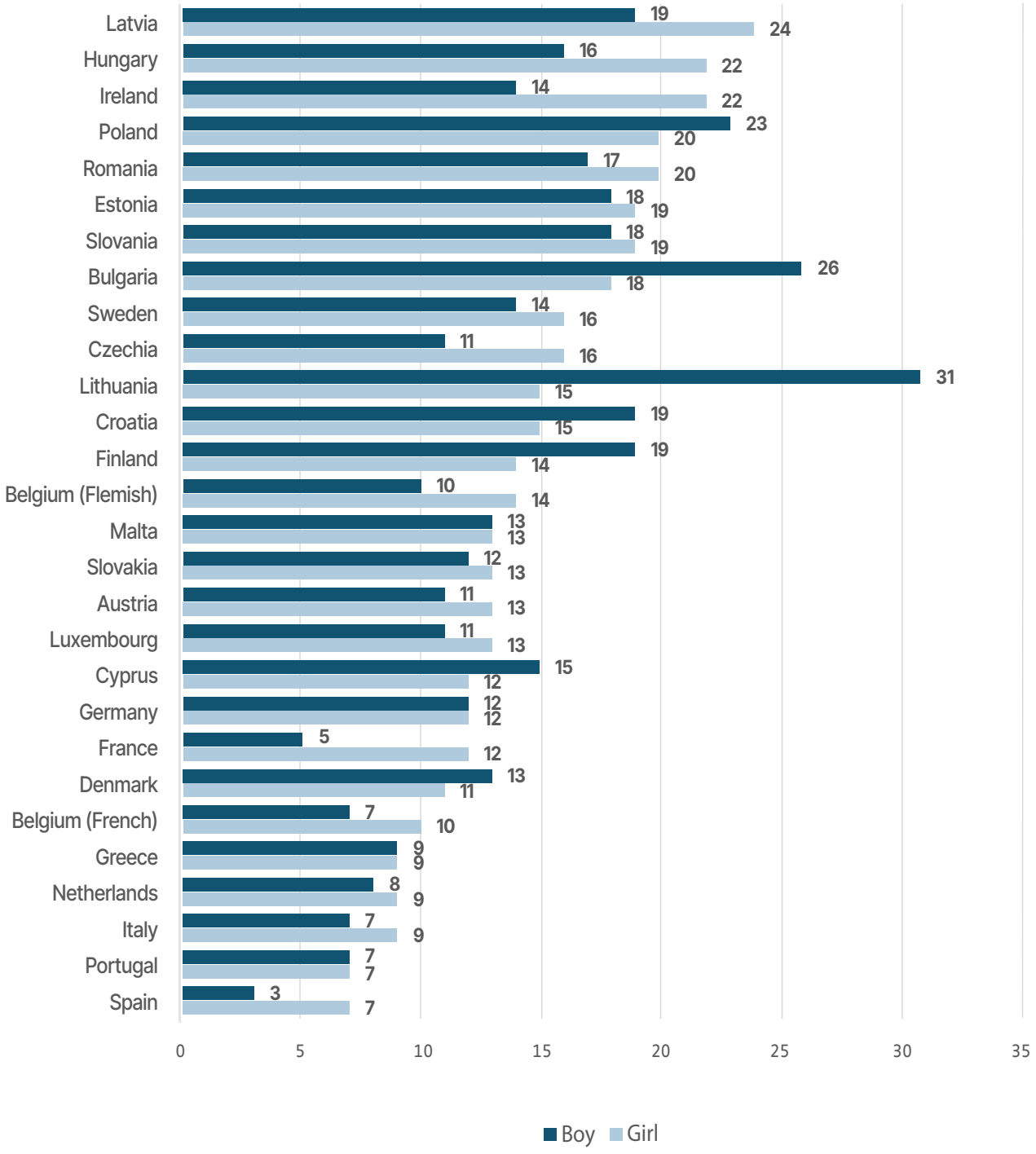
FIGURE A1 | Thirteen-year-olds who have been cyberbullied at least once in the past couple of months, by sex and Member State (%, 2021–2022)



NB: Young people were asked how often they had experienced cyberbullying (e.g. anyone sending mean instant messages, wall postings or emails or someone posting or sharing photos or videos online without their permission). Response options ranged from 'I have not been cyberbullied in the past couple of months' to 'Several times a week'. The findings presented here show the percentage of young people who had experienced cyberbullying at least once in the past couple of months.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

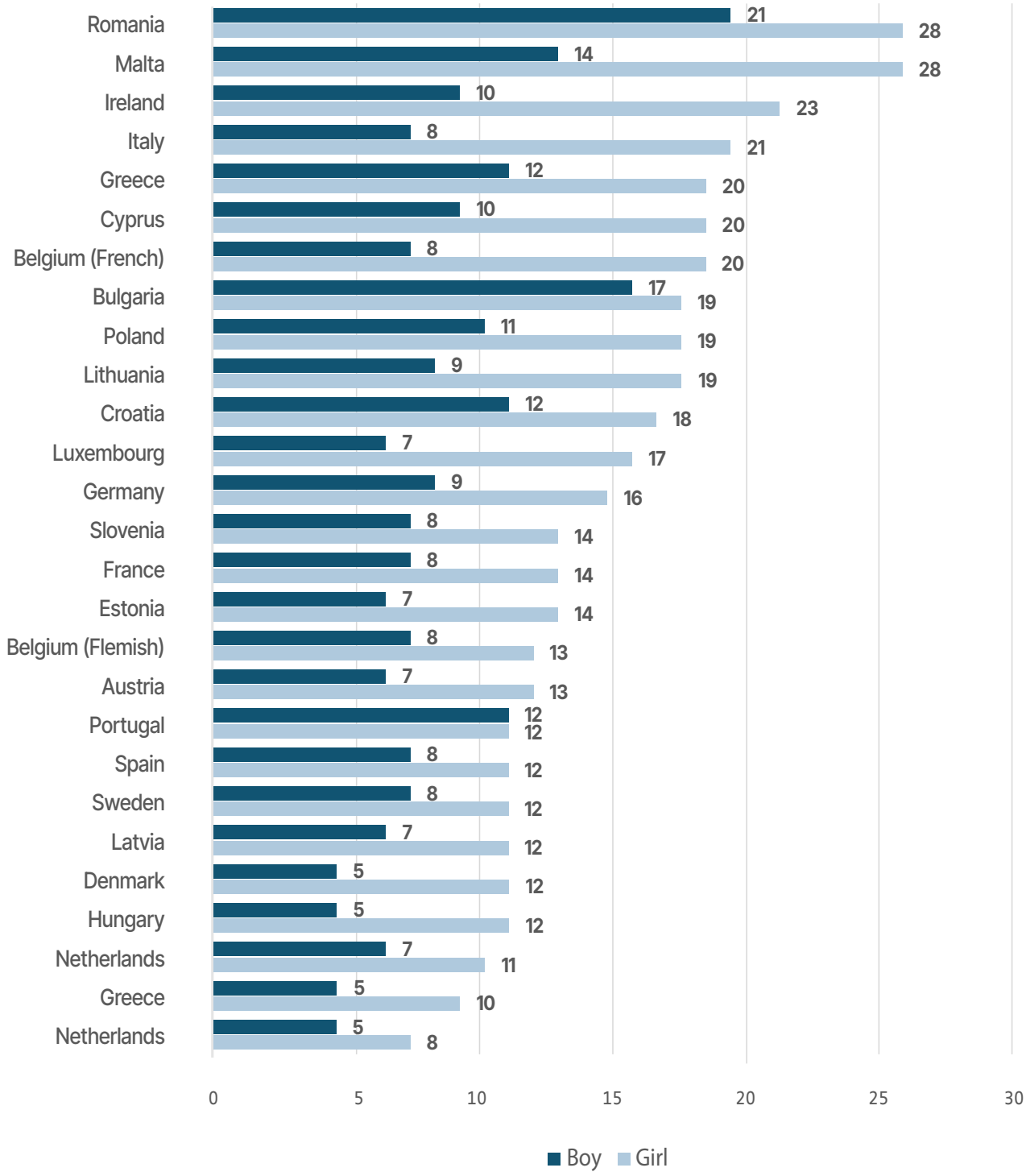
FIGURE A2 | Fifteen-year-olds who have been cyberbullied at least once in the past couple of months, by sex and Member State (%, 2021–2022)



NB: Young people were asked how often they had experienced cyberbullying (e.g. anyone sending mean instant messages, wall postings or emails or someone posting or sharing photos or videos online without their permission). Response options ranged from 'I have not been cyberbullied in the past couple of months' to 'Several times a week'. The findings presented here show the percentage of young people who had experienced cyberbullying at least once in the past couple of months.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

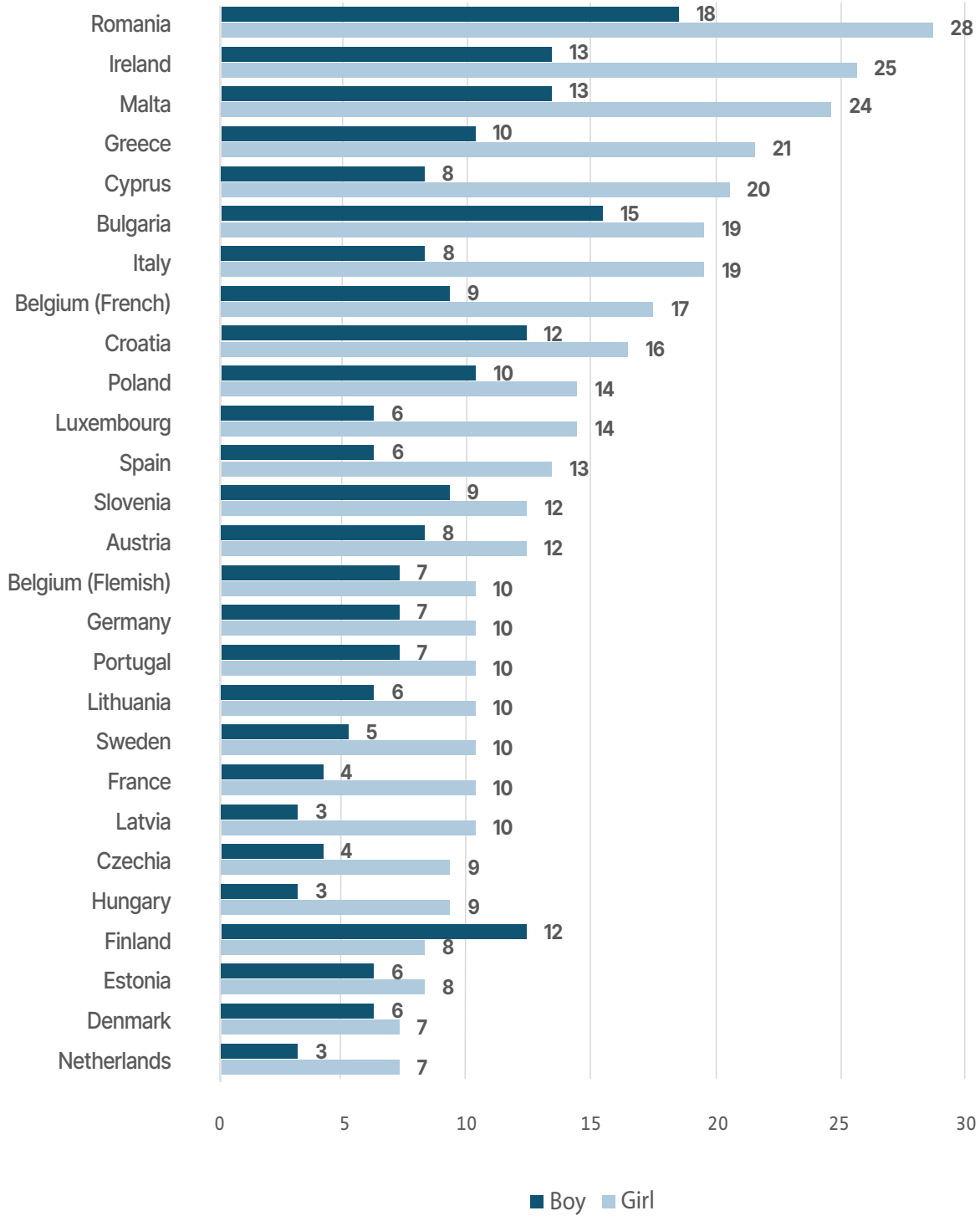
FIGURE A3 | Thirteen-year-olds who report problematic social media use, by sex and Member State (% 2021–2022)



NB: Young people were asked to report symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale, a nine-item measure to which respondents answered each question with a 'yes' or 'no'. The findings presented here show the percentage of young people who answered 'yes' to six or more questions and were therefore categorised as problematic social media users.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

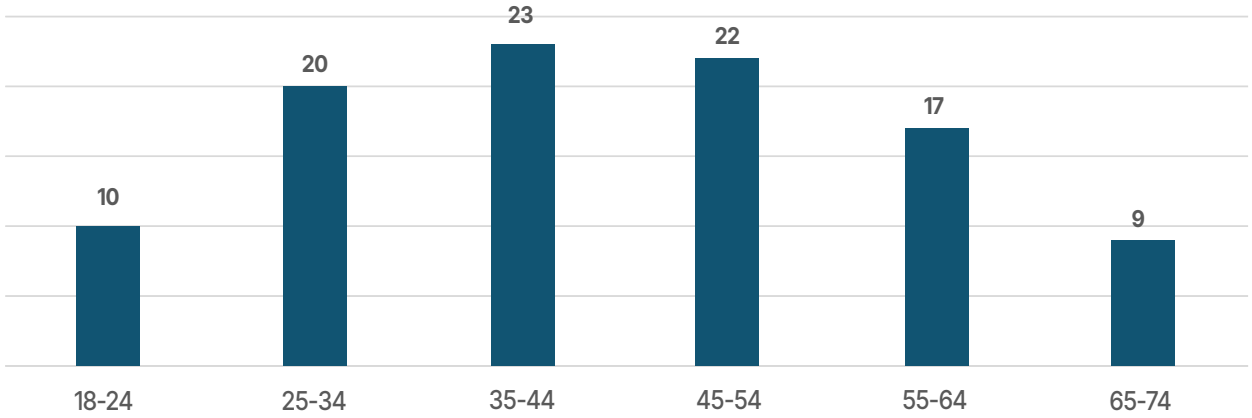
FIGURE A4 | Fifteen-year-olds reporting problematic social media use, by sex and Member State (%20 21–2022)



NB: Young people were asked to report symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale, a nine-item measure to which respondents answered each question with a 'yes' or 'no'. The findings presented here show the percentage of young people who answered 'yes' to six or more questions and were therefore categorised as problematic social media users.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

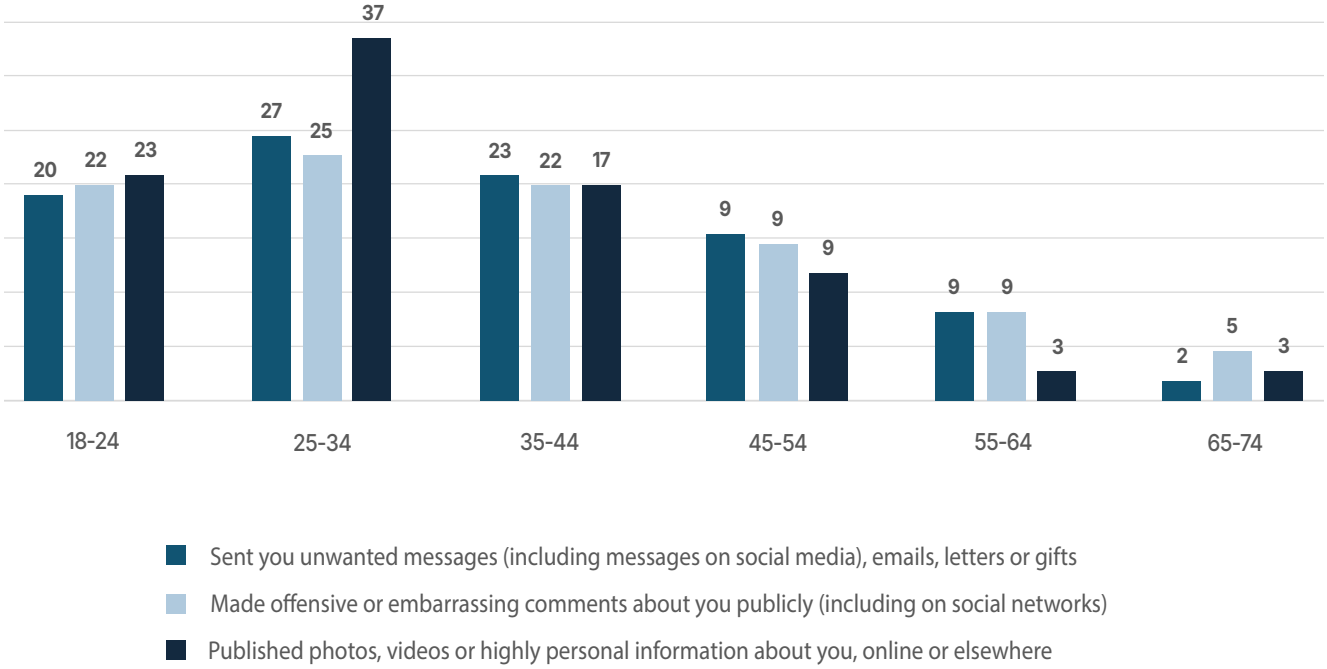
FIGURE A5 | Women who have experienced controlling behaviour from partners who insist on knowing their whereabouts, by age group (%, 18–74-year-olds, EU, 2021)



NB: Respondents were asked whether any of their current and previous partners had ever insisted on knowing where they were in a controlling way or tracking them via GPS, phone, social network, etc. (EU-GBV Survey question F1.) The findings presented here show the proportion of respondents who reported such experiences, broken down by age. This is based on the population estimate derived from the sample and has been appropriately weighted. The target population of the EU-GBV Survey is defined as individuals aged 18–74 living in private households, with a focus on women.

Source: Authors, based on data from the EU-GBV Survey (2021 wave).

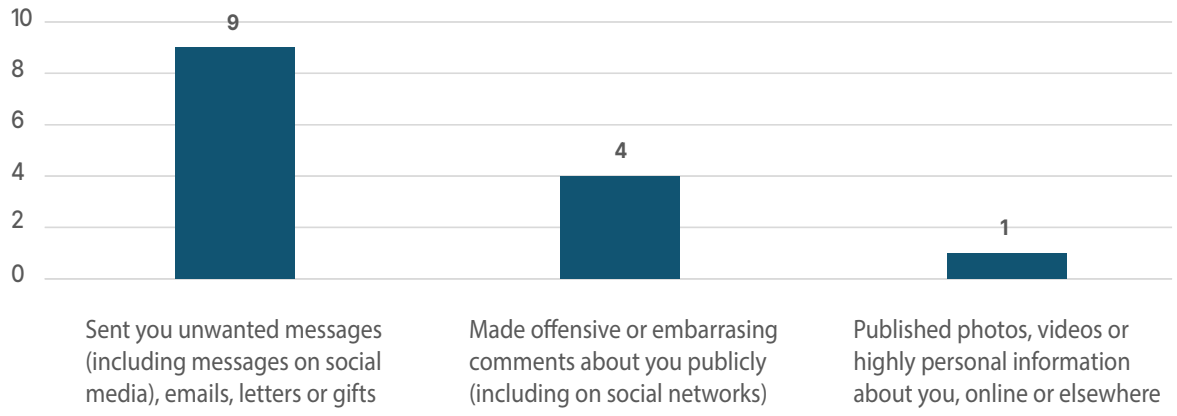
FIGURE A6 | Women who have experienced cyber violence, by type of violence and age group (%, 18–74-year-olds, EU, 2021)



NB: Respondents were asked whether, during their lifetime, the same person had repeatedly (more than once) carried out one or more of the following actions in a way that caused fear, alarm or distress. The items considered are related to issues linked (though not limited) to different types of cyber violence, specifically: 'Sent you unwanted messages (including messages on social media), emails, letters or gifts'; 'Made offensive or embarrassing comments about you publicly (including on social networks)'; and 'Published photos, videos or highly personal information about you, online or elsewhere.' (EU-GBV Survey question N1. Survey variables: ST_GIFTS, ST_COMMENT, ST_PUBLISH.) The findings presented here show the proportion of respondents who reported such experiences, broken down by age. This is based on the population estimate derived from the sample and has been appropriately weighted. The target population of the EU-GBV Survey is defined as individuals aged 18–74 living in private households, with a focus on women.

Source: Authors, based on data from the EU-GBV Survey (2021 wave).

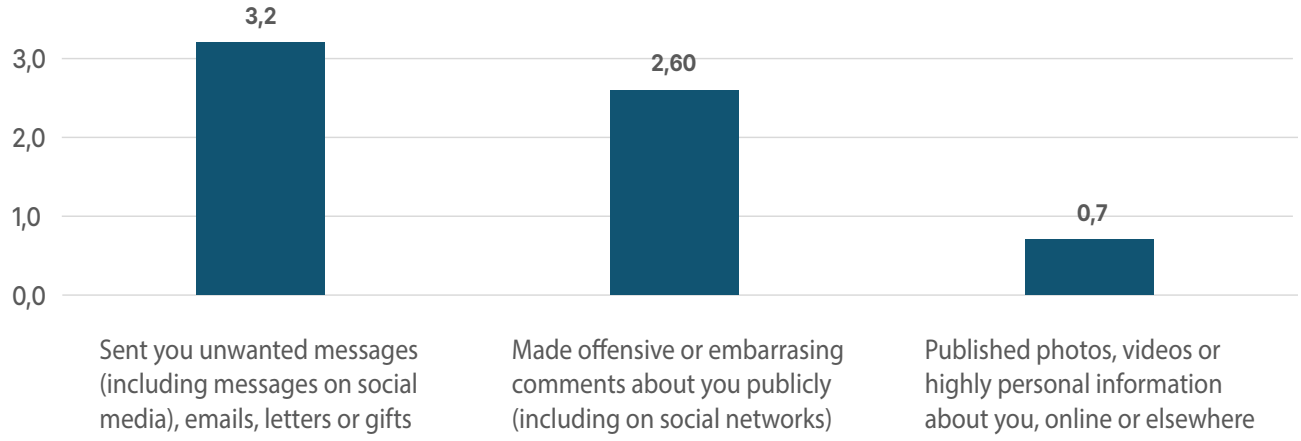
FIGURE A7 | Women who experienced cyber violence, by form of violence (%, EU, 18–74-year-olds, 2021)



NB: Respondents were asked whether, during their lifetime, the same person had repeatedly (more than once) carried out one or more of the following actions in a way that caused fear, alarm or distress. The items considered are related to issues linked (though not limited) to different types of cyber violence, specifically: 'Sent you unwanted messages (including messages on social media), emails, letters or gifts'; 'Made offensive or embarrassing comments about you publicly (including on social networks)'; and 'Published photos, videos or highly personal information about you, online or elsewhere.' (EU-GBV Survey question N1. Survey variables: ST_GIFTS, ST_COMMENT, ST_PUBLISH.) The findings presented here show the proportion of respondents who reported such experiences. This is based on the population estimate derived from the sample and has been appropriately weighted. The target population of the EU-GBV Survey is defined as individuals aged 18–74 living in private households, with a focus on women

Source: Authors, based on data from the EU-GBV Survey (2021 wave).

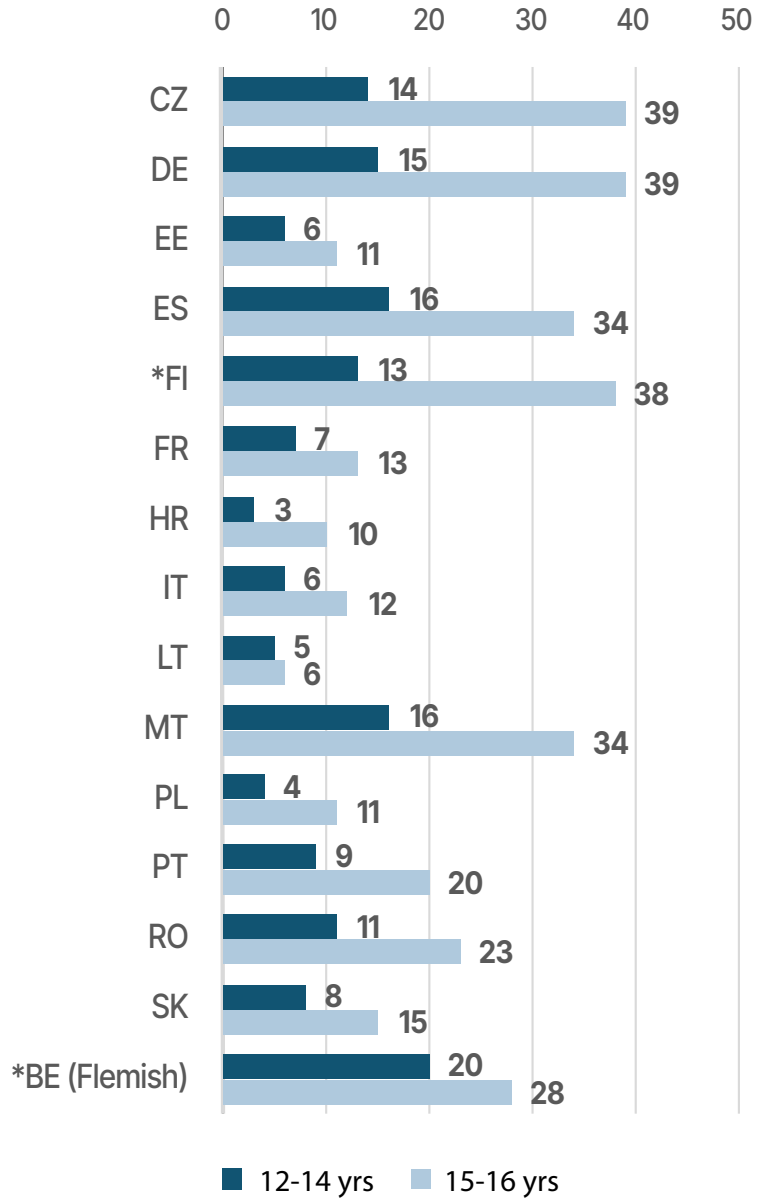
FIGURE A8 | Women whose experiences of cyber violence occurred before the age of 15 (%, EU, 18–74-year-olds, 2021)



NB: Respondents were asked whether the violent episode they experienced happened before the age of 15. The findings reported here correspond to those respondents who – among those who stated that they had experienced cyber violence in answer to question N1 – answered that, of the situations they had indicated experiencing in N1, 'all of them' occurred before the age of 15 (EU-GBV Survey question N6). The findings presented are based on the population estimate derived from the sample and have been appropriately weighted. The target population of the EU-GBV Survey is defined as individuals aged 18–74 living in private households, with a focus on women.

Source: Authors, based on data from the EU-GBV survey (2021 wave).

FIGURE A9 | Adolescents who have received unwanted sexual requests, by age group and Member State (%,12–16-year-olds, 2020)

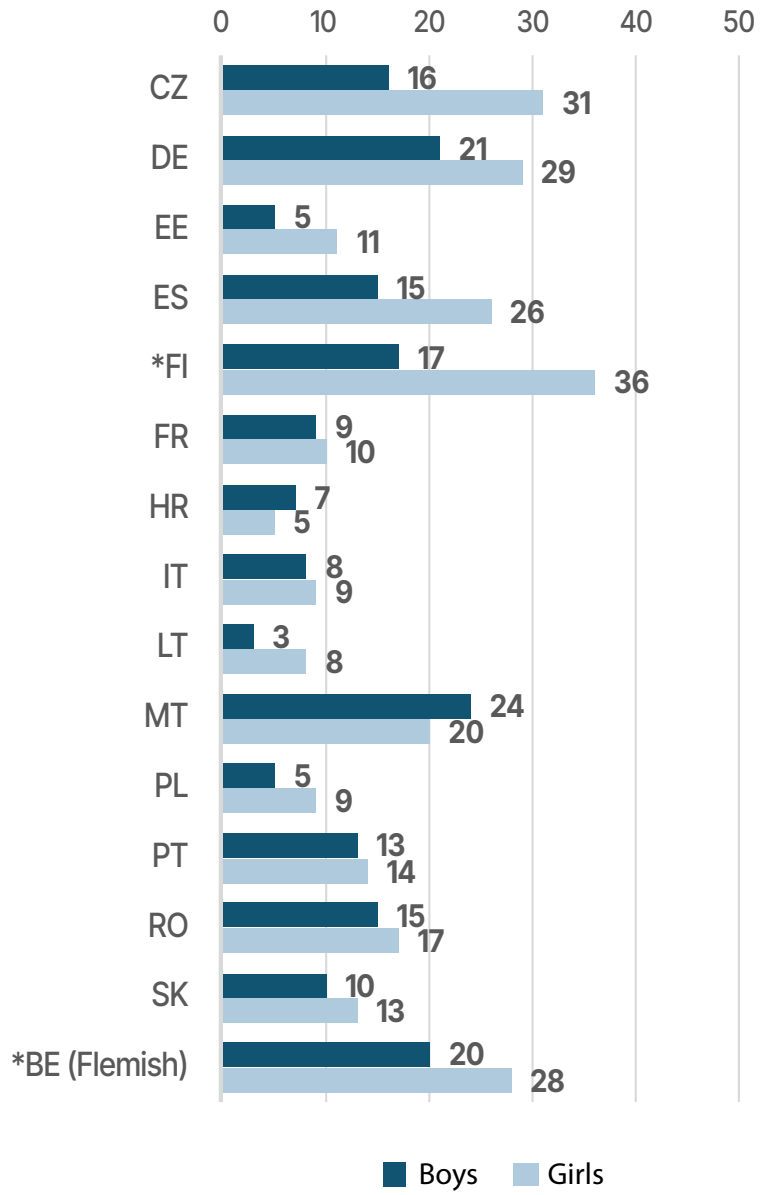


(*) data not weighted

NB: Based on the following question from a survey conducted as part of the EU kids online project (QF47). 'In the PAST YEAR, how often, if ever, have you been asked by someone on the internet for sexual information (words, pictures or videos) about yourself when you did not want to answer such questions?' Percentage of children who answered 'a few times', 'at least monthly' or 'daily or almost daily'.

Source: Smahel et al., 2020.

FIGURE A10 | Adolescents who have received unwanted sexual requests, by sex and Member State (%, 12–16-year-olds, 2020)

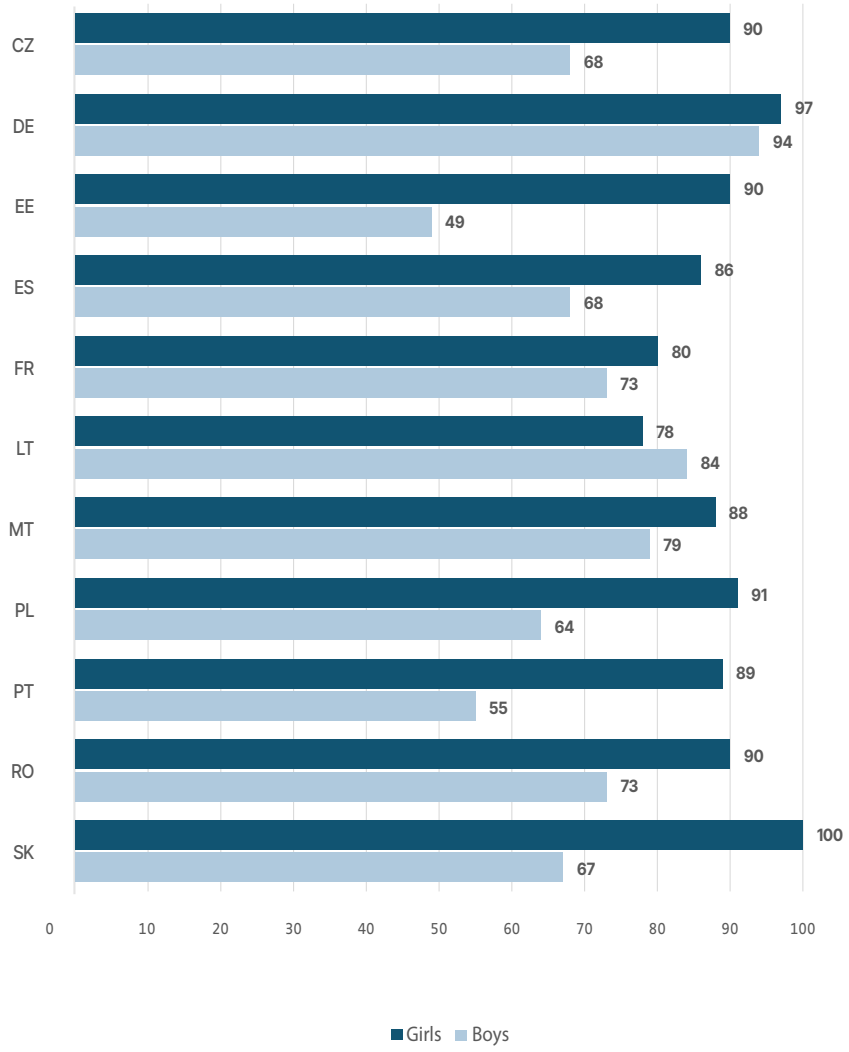


(*) data not weighted

NB: Based on the following question from the EU kids online project survey (QF47). 'In the PAST YEAR, how often, if ever, have you been asked by someone on the internet for sexual information (words, pictures or videos) about yourself when you did not want to answer such questions?' Percentage of children who answered 'a few times', 'at least monthly' or 'daily or almost daily' of all children aged 9–16 who use the internet.

Source: Smahel et al., 2020.

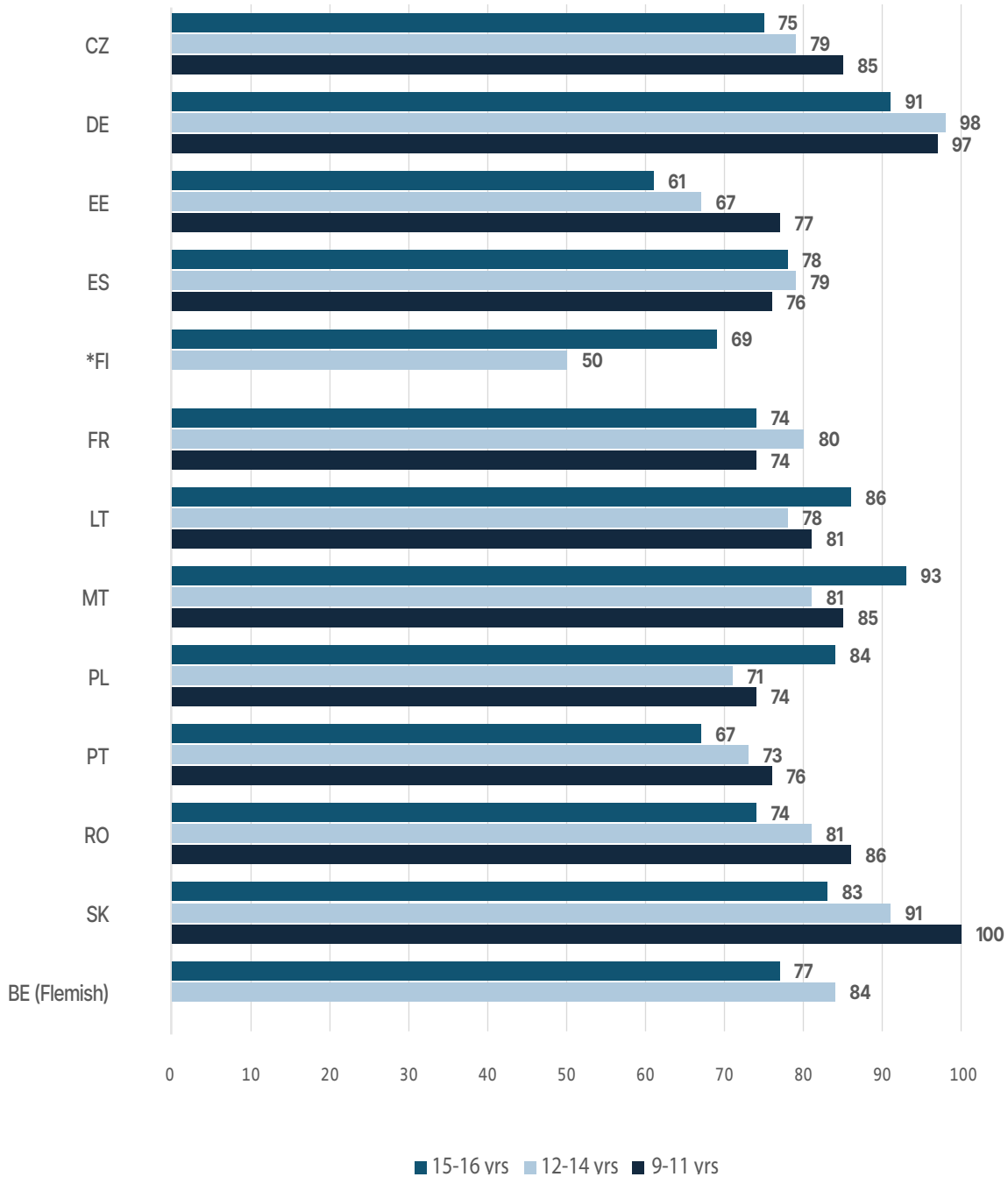
FIGURE A11 | Children who have experienced harm from online victimisation (to the degree of being at least a bit upset), by sex and Member State (%, 9–16-year-olds, 2020)



NB: In the Flemish Region of Belgium and Finland the full age range was not available; in Hungary and Italy the question was not asked. The question (QF24) was as follows: 'Thinking of the LAST TIME someone treated you in a hurtful or nasty way ONLINE, how did you feel?' Results include percentage of children who answered 'I was a little upset', 'I was fairly upset' or 'I was very upset' of all children aged 9–16 who use the internet and who reported being victimised online at least a few times.

Source: Smahel et al., 2020.

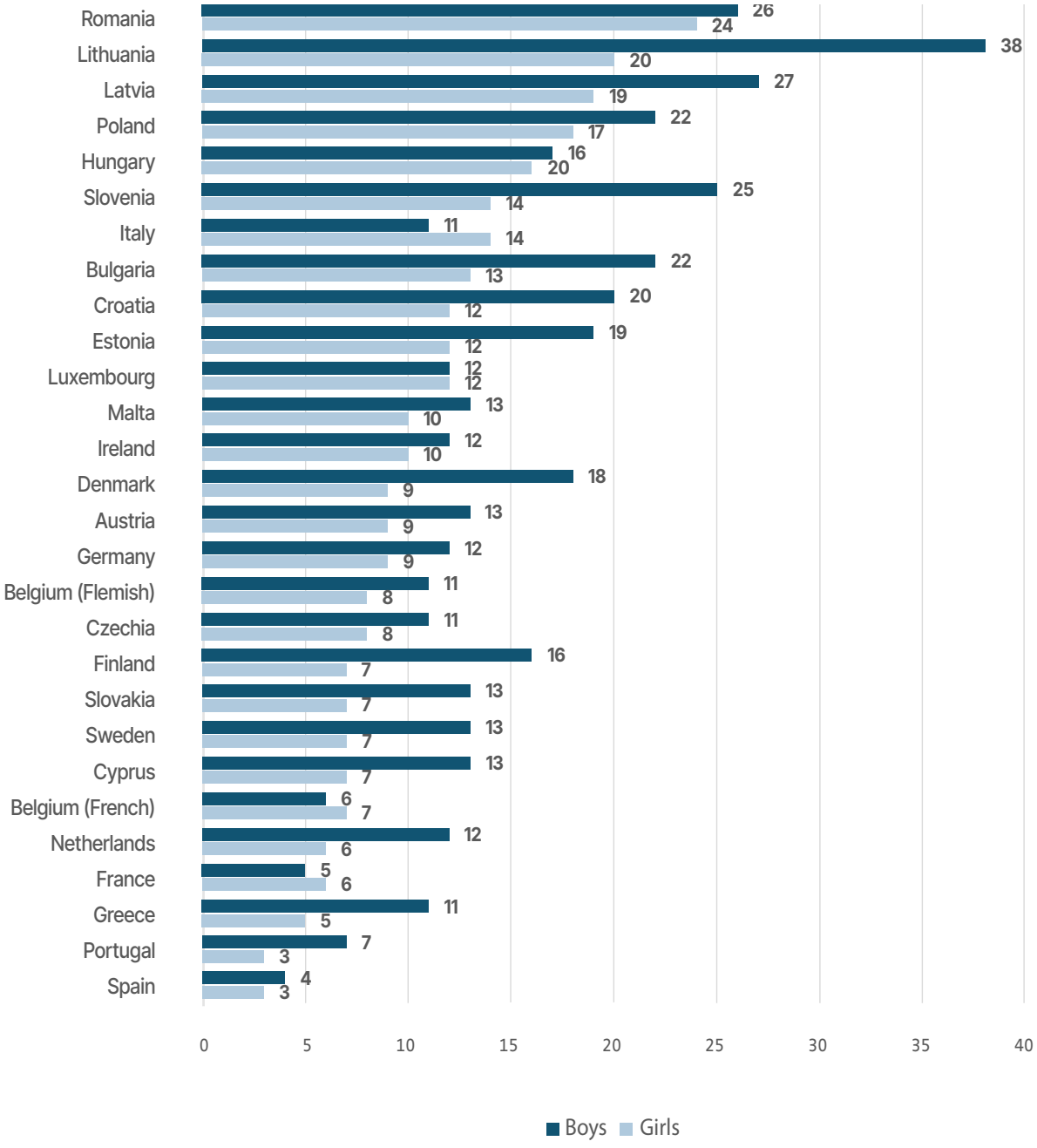
FIGURE A12 | Children reporting harm from online victimisation (at least a bit upset), by age group and Member State (%, 9–16-year-olds, 2020)



NB: In the Flemish Region of Belgium and Finland the full age range was not available; in Hungary and Italy the question was not asked. The question (QF24) was as follows: 'Thinking of the LAST TIME someone treated you in a hurtful or nasty way ONLINE, how did you feel?' Results include percentage of children who answered 'I was a little upset', 'I was fairly upset' or 'I was very upset' of all children aged 9–16 who use the internet and who reported being victimised online at least a few times.

Source: Smahel et al., 2020.

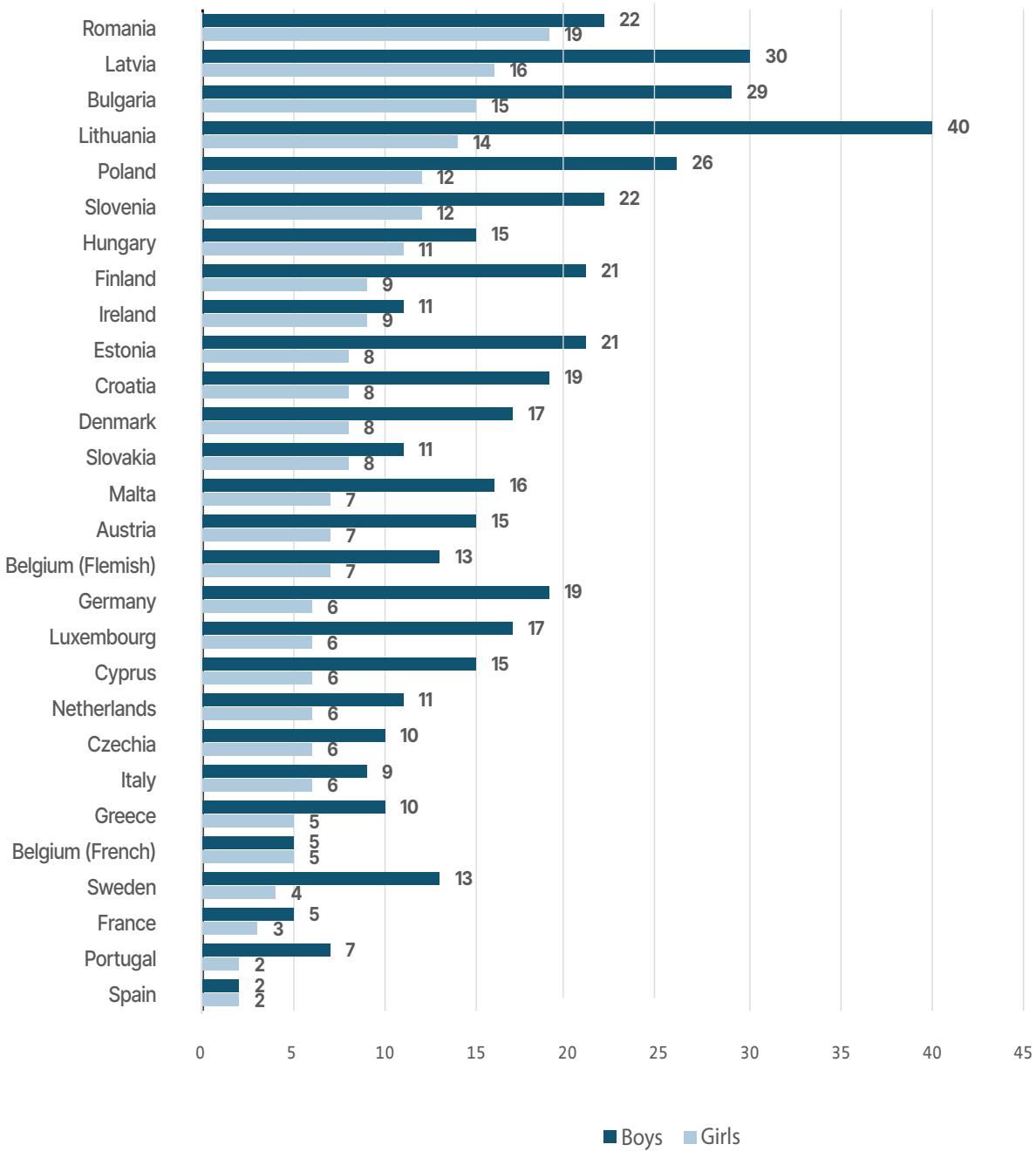
Figure A13 | Thirteen-year-olds who have cyberbullied others at least once in the past couple of months, by sex and Member State (%, 2021–2022)



NB: Young people were asked whether they had taken part in cyberbullying (e.g. sending mean instant messages, wall posts or emails or posting or sharing photos or videos online without permission). The response options ranged from 'I have not cyberbullied another person in the past couple of months' to 'Several times a week'. The findings presented here show the percentage of young people who had cyberbullied others at least one in the past couple of months.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

Figure A14 | Fifteen-year-olds who have cyberbullied others at least once in the past couple of months, by sex and Member State (%, 2021–2022)



NB: Young people were asked whether they had taken part in cyberbullying (e.g. sending mean instant messages, wall posts or emails or posting or sharing photos or videos online without permission). The response options ranged from 'I have not cyberbullied another person in the past couple of months' to 'Several times a week'. The findings presented here show the percentage of young people who had cyberbullied others at least one in the past couple of months.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey) – https://data-browser.hbsc.org.

Tables

Table A1: Examples of international policy and legal documents addressing cyber violence

Instrument	Year and body	Scope and main provisions	Cyber violence dimension	Relevance for EU action
UN Women and WHO research paper on technology-facilitated violence against women	2023, UN Women and WHO	Highlights gaps in data collection; offers methodologies for obtaining better evidence.	Calls for inclusion of diverse experiences in policymaking.	Supports EU's emphasis on data-driven policymaking and intersectional approaches.
GREVIO General Recommendation No. 1 on the digital dimension of violence against women	2021, Council of Europe	Provides guidance on the implementation of the Istanbul Convention in the digital context.	Emphasises national action plans, digital literacy and the training of law enforcement.	Informs EU recommendations on training, prevention and digital literacy.
Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective	2018, UN	Identifies forms of cyber violence such as cyberstalking, harassment and non-consensual image sharing; recommends legal reform and systemic change.	Strong focus on victim-centred remedies and education for digital literacy.	Provides human rights framing used in European Parliament debates and documents.
Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention)	2011, Council of Europe	Is a comprehensive treaty against violence against women; requires states to criminalise multiple forms of abuse.	Explicitly includes online abuse (cyberstalking, harassment, non-consensual images).	Basis on which the EU calls on Member States to ratify and implement legislation against violence against women; aligned with Directive (EU) 2024/1385.

Instrument	Year and body	Scope and main provisions	Cyber violence dimension	Relevance for EU action
Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse	2007, Council of Europe	Protects children from sexual exploitation and abuse.	Includes digital exploitation; Lanzarote Committee guidelines (2017, 2022) stress the importance of educating children about digital safety, promoting age-appropriate content moderation, ensuring platform accountability and improving cross-sector collaboration among governments, tech companies, NGOs and law enforcement.	Reinforces EU child protection strategies (e.g. Regulation (EU) 2021/1232; the better internet for kids strategy).
Budapest Convention on Cybercrime and its Second Additional Protocol	2001–2022, Council of Europe	First binding international treaty on cybercrime; establishes cross-border cooperation and platform accountability.	Covers cyberstalking, grooming, non-consensual images and online exploitation.	Provides legal and operational tools for Member States to prosecute cross-border cybercrime.

Table A2: Examples of EU regulatory developments on gender-based (cyber) violence

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance/ Added value
Strengthening legal protections amid emerging challenges	EU Violence against Women Directive	2024	Makes a significant legislative commitment to combating cyber violence against women and girls, as it obliges Member States to act against specific forms of cyber violence.	Provides common definitions for the four main forms of cyber violence. Sets minimum standards for criminalisation and mandates data collection.	Addresses the long-standing issues of diverse and multiple definitions and a fragmented approach to criminalisation. Sets up a framework for harmonised data collection likely to improve research and monitoring.
	EU AI Act (Regulation 2024/1689)	2024	World's first AI law; establishes obligations for high-risk AI and content transparency.	Requires labelling of AI-generated deepfake content.	Acts as a direct response to deepnudes / non-consensual synthetic intimate imagery; strengthens transparency and accountability.
	DSA	2022	Imposes strict content moderation rules for large online platforms.	Requires proactive moderation of illegal and harmful content, including child sexual abuse material and non-consensual intimate images.	Is the key enforcement tool for platform accountability. Directive (EU) 2024/1385 aligns with the DSA's enforcement mechanisms.
	Audiovisual Media Services Directive (2018/1808)	2018	Regulates media services across Member States.	Includes provisions against online hate speech and harmful content.	Extends protection to online platforms; enables an intersectional approach to vulnerable groups.
	GDPR	2018	Strengthens rights over personal data; establishes safeguards against misuse.	Enables removal of harmful or non-consensual personal content online.	Provides privacy-based protection frequently used by victims of cyber violence.

	Instrument	Year	Scope and main provisions	Cyber violence dimension	Relevance/ Added value
Expanding support systems for victims	Victims' Rights Directive (2012/29/EU, revision proposed in 2023)	2012 / revision ongoing	Establishes minimum standards for victims' rights and support.	Provides access to counselling, reporting and legal aid; its proposals include stronger digital protections for vulnerable groups.	Forms a cornerstone of the EU victim-centred approach; aligned with Directive (EU) 2024/1385, which enhances victim support by introducing anonymous online reporting mechanisms, specialised counselling and mental health services and prevention initiatives (e.g. Article 34.5 of Directive (EU) 2024/1385 supports the creation of preventive measures for men).
Monitoring and evaluation through collaboration	EU Code of Conduct on Countering Illegal Hate Speech Online	2016 (integrated into the DSA in 2025)	Promotes collaboration with major platforms to remove hate speech.	Tackles online hate speech; now reinforced via DSA provisions.	Is an instrument for public–private cooperation; ensures quicker content removal and accountability online.
Measures to protect children and address gender-specific risks	Regulation (EU) 2021/1232	2021	Allows the detection and removal of child sexual abuse material while ensuring compliance with EU privacy and data protection safeguards.	Protects children from online sexual exploitation, including young girls.	Strengthens compliance with privacy standards while combating child sexual abuse material.
	Better internet for kids strategy	2022	Promotes digital literacy and online safety across Member States.	Addresses cyber violence explicitly via cyberbullying, harmful content, harassment, exposure to sexual abuse content, violent content, self-harm risks, etc. Also aims to prevent and respond to harmful conduct among minors online.	Provides a holistic, child-centred framework that links legal/regulatory measures (like the DSA) with awareness, education and the direct participation of children.
	EU strategies: 2020–2025 gender equality strategy; 2020–2025 victims' rights strategy; 2020–2025 strategy for a more effective fight against child sexual abuse	2020-2025	Present policy roadmaps for equality, victim protection and child safety.	Emphasise online gender-based violence prevention, digital literacy, platform accountability and child protection.	Provide significant guidance on gender-based violence that aligns with binding directives.

Table A3: Examples of specific case-law related to cyber violence

Member State	Judgment number	Description
Italy	Supreme Court Judgment No 3989/2019 ([59])	In this case, the defendant was convicted of stalking through WhatsApp messages. The defendant argued that private messaging between two users should not be considered an electronic means under the law. However, the Italian Supreme Court rejected this argument, affirming that communication via WhatsApp constitutes the use of electronic or telematic means, thereby aggravating the crime of stalking. The court ruled that the defendant was to receive a six-month prison sentence, judging such messaging platforms to fall within the purview of Article 612-bis.
	Supreme Court Judgment No 33230/2024 ([60])	This ruling addressed the distinction between stalking (Article 612-bis) and the unlawful dissemination of sexually explicit images (Article 612-ter, known as 'revenge porn'). The defendant was convicted of both offences after sending offensive messages and distributing intimate images of his ex-partner via electronic means. The Italian Supreme Court highlighted that the unauthorised sharing of explicit images constitutes a separate offence from stalking, underscoring the legal system's recognition of a range of ICT-related behaviours as criminal acts.
Romania	European Court of Human Rights judgment No 56867/15 (Buturugă v. Romania) ([61])	In this case, the European Court of Human Rights found that Romanian authorities failed to properly investigate both domestic violence and cyberbullying allegations. The applicant reported her former husband's violent behaviour and claimed he had accessed her private electronic accounts without consent. However, the courts dismissed her complaints, arguing that online privacy violations were unrelated to the case. The court ruled that cyber violations, including unauthorised access to electronic correspondence, are a form of domestic violence and require thorough examination. Romania was found to have violated Articles 3 and 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and the applicant was awarded EUR 10 000 in non-pecuniary damages.
	European Court of Human Rights No 28935/21 (M. Ș. D. v. Romania) ([62])	The case involves the national authorities' handling of the applicant's complaint about alleged online harassment by her former partner, reportedly motivated by revenge, which included the non-consensual public sharing of her intimate photographs. The court determined that Romania infringed upon a woman's right to privacy and family life by not providing protection against cyber violence.

Source: Authors.

59 'Stalking by WhatsApp' – VGS Family Lawyers.
60 'Supreme Court ruling: The boundary between stalking and revenge porn' – Studio Legale Bianucci.
61 Judgment of the European Court of Human Rights of 28 March 2024, Buturugă v. Romania, No 56867/15, ECLI:CE:ECHR:2020:0211JUD005686715.
62 Judgment of the European Court of Human Rights, M. Ș. D. v. Romania, No 28935/21, ECLI:CE:ECHR:2024:1203JUD002893521.

Table A4: Experiences of cyber violence among young people, by age and sex (%)

	Offensive name-calling	Spreading of false rumours about them	Receiving explicit images they didn't ask for	Constantly being asked where they are, what they're doing or who they're with by someone other than a parent	Physical threats	Having explicit images of them shared without their consent	Any cyberbullying
Boys	31	16	15	13	10	5	43
Girls	32	29	19	17	10	8	49
White	35	24	16	14	10	6	48
Black	29	17	21	9	11	10	40
Hispanic	29	21	19	21	10	7	47
Aged 13-14	29	20	11	12	10	4	42
Aged 15-17	34	24	22	17	10	8	49
Boys aged 13-14	31	15	11	12	10	3	41
Boys aged 15-17	32	16	18	13	10	7	44
Girls aged 13-14	25	24	10	12	9	5	41
Girls aged 15-17	36	33	25	20	10	9	54

NB: The numbers of White and Black young people are those who reported being only one race (and not Hispanic). Hispanic young people were those of any other race. Those who did not give an answer to this question are not shown. Young people were asked the following question: 'Thinking about your experiences online or on your cell phone, which of the following, if any, has ever happened to you personally?'

Source: Vogels, 2022; survey conducted from 14 April to 4 May 2022.

Table A5: Types of cyber violence experienced or witnessed by female focus group participants (13–18-year-olds, focus groups conducted between March 2025 and June 2025)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
(Sexual) Cyber violence/ harassment	Includes unsolicited sexual messages or images, grooming, coercion for nudes, revenge porn, deepfakes and sexual threats.	Cyber harassment (including cyberbullying)	'And there's this app called Snapchat. And on this app this particular friend of mine was totally adding everyone who invited her to it. And it was just like, you'd go into these messages and every message was just a naked penis.' (Poland, 13–15) 'I was on this Omegle already with my friends on a sleepover [sleepover at a friend's house]. This is typical on sleepovers. I connected with a guy like that. I'm like ''hey'', ''where are you from'', a conversation, and suddenly I'm [like] ''wait, what are you doing?'', I'm like eww, he put out his [genitals]. It's all the time! Hello, hello, skip, skip, skip! And then some three some skips later it was the same thing.' (Poland, 13–15) 'I started joining some other servers later on and then I had such a literal rash of people writing to me and at some point I became friends with this dude. He said he was about the same age as me and so on and we wrote together for a very long time and then we started 'dating' [i.e. being a 'couple']. Obviously this kind of you know, nine-year-old me and some dude on discord. And then I found out, it was some long time later, because he used to say to me that ''well if you don't write back to me, am I going to kill myself'' and it was like he was, he was in a different time zone, so it often happened that I would stay up all night to talk to him, because I didn't want him to kill himself. And after a while he just, there was a conversation like: ''I need to tell you something''. ''Well, what do you need to tell me?'', ''I'm actually 19''. Not only was he 19, but it wasn't just one person, it was three people sharing one account and writing to underage kids on Discord as a character they had made up. And they were also scamming these kids with ''nudes'' and ''softs'' and stuff like that.' (Poland, 13–15) TikTok in some countries now has the possibility that you can just post pictures in the comments section and some people literally post porn in there, GIFs of some kind, something like that. It can be a photo, it can be a GIF of a few seconds and very often it can be porn. It can even be anything, maybe a joke, something funny, maybe you'll get comments like this, such a big [penis] and it's even moving.' (Poland, 13–15)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
			There was this person who, from his profile, seemed to be an older man who sent messages because this girl had an Instagram profile and he kept sending her various provocative messages, asking her to send him photos of herself in her underwear or even without [underwear], perhaps in certain positions, not the most appropriate. And every time she blocked him, he created other profiles and continued to write to her, so he didn't accept rejection.' (Italy, 13–15)
			Yes, or an account called "Horny in [city]" added you. That's not unusual either. Or "sending nudes"; not unusual either. Horny guy from [city], a lot of them. I can even go to my Snap[chat] now and there are several of them where they're just like "horny, looking for a pretty girl".' (Sweden, 13–15)
			'I was in a group with a very immature boy. He sent me a private message once and then it continued ... At least every three months, let's say ... and he would write to me, let's say – how can I put it – [to see] if I wanted to send him a message, if I wanted him to send me a message, if I wanted to have sex, this and that.' (Cyprus, 16–18)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
Cyberstalking	Persistent unwanted contact, tracking via fake accounts, emotional manipulation (e.g. suicide threats) and monitoring in relationships.	Cyberstalking	'It feels like the first thing a guy asks ... when you add him on Snap[chat] is about you, but then always a picture. It's always pictures ...' (Sweden, 16–18)
			'This guy would do anything to get her back, stalking her, sending her messages and trying to deprive her of everything ... but she was just a girl; I don't think she was even fifteen.' (Italy, 16–18)
			'After a while he became a bit possessive and when she broke up with him he tried to track him down through other accounts and through his friends, even resorting to blackmail, saying he would kill himself or stuff like that.' (Italy, 16–18)
			'But also like a girl in my class ... a guy in my class is obsessed with her. And we've tried for so long to get teachers and stuff to understand it, but he still sends pictures of when he's held knives to his arms and said, ''if you don't stay with me I'll kill myself''.' (Sweden, 13–15)
			'It was some guy who wrote something, and she replied ... then he started getting a little creepy. She blocked him, but he kept opening new accounts and writing to her. No matter how much she blocked him, he kept going – and she couldn't have known that [he would do something like this]'. You never know.' (Sweden, 16–18)
			They were online friends. And after a few months, we said, since we're so close, let's show each other our faces. Okay, we showed our faces, and because I was 12 at the time and a bit chubby, they started teasing me and kicked me out of the group.' (Cyprus, 16–18)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
Cyber harassment (including cyberbullying)	Hate messages, targeted group chats, exclusion, rumour spreading, mocking, verbal attacks, humiliation, spreading false stories and coordinated social shaming that impact mental well-being.	Cyber harassment; cyber incitement to hatred or violence	'I think we've all noticed, either on TikTok or Instagram, a girl who posted photos and now there are messages you can write to someone when they post a story, which are anonymous, and the things people write to her in those messages are very nasty and have very disgusting content.' (Cyprus, 16–18)
			'He started spreading rumours about me, as if to make me pay, and we got to the point where I had the whole class against me. Since my school was small, the rumours spread quickly to the other sections and various classes, and I couldn't take it ... spending eight hours at school with everyone staring at you and whispering jokes behind your back.' (Italy, 13–15)
			Some people from my old school had set up a group on Messenger. It was just there to just literally talk down on me and my like two friends. It was so very silly because they weren't posting, they were [forwarding some pictures from] different accounts on Instagram and then commenting on them to each other. Or there was also the fact that they started generating AI stories.' (Poland, 13–15)
			'So yes, you've noticed from the lower years that it's mainly this sending around naked pictures and starting rumours and stuff. There were definitely one or two cases in the lower years. I think everyone realised that too. And that's definitely also represented here at our school.' (Germany, 16–18)
			'I found out from this one girl that they just had a group where they would send each other pictures of me and this friend of us being together in certain places, that we were going to a bubble tea [shop], for example, and there was a picture of us going [taken] from behind. Or when we were at school and he was helping me because I didn't understand something in math and we were both bent over the notebook like that. It was also pictures like that that were just everywhere. And it didn't stop, it didn't stop, even when I left school.' (Poland, 13–15)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
			They decided that all of a sudden, they would start calling her names on her public account on Instagram. And they'd start writing really mean things about her. And now there are these threads on Instagram. And there they started writing her name and that she's stupid, for example, or 'fuck her'. And they've created something like a picture of a penis … from cars, and put it on the account, created pictures of her next to it, comparing her to that car from that video, and stuff like that,… [...] But I remember the worst thing is that these girls were doing it for no reason at all. Nothing had happened before, they had been very friendly with her before. And all of a sudden they jumped from such a friendship to very strange situations and it was still horrible.' (Poland, 16–18)
			'There are games like Valorant … where there's an option to enter a voice chat. And I can say … there's not a day where it doesn't happen … I'll say ''hello'', they hear it's a feminine voice and it just starts shouting. There's a lot of that ''go to the kitchen'' chatter. If I play badly, they say I play badly because I'm a woman. If I play well, they start arguing even more.' (Poland, 13–15)
			Me too, yes, I found out about this, about a person I don't know directly, whom I heard about, and she sent videos to her boyfriend, and these videos went around the whole school and everything.' (Italy, 13–15)

Type of cyber violence	Description	Relevance to forms of cyber violence covered by Directive (EU) 2024/1385	Example quotes
Image-based cyber violence	Secretly taking or manipulating images/ videos, sharing them without consent or creating sexualised deepfakes.	Non-consensual sharing of intimate images	In my class, in the first years of high school, there was a period when parents and teachers had to get involved because some boys photographed the private parts of another classmate and spread the photos around the school and the class, and it came to light.' (Italy, 13–15)
			'She didn't want to date him, be in a relationship, and he literally made a deepfake of her, and he started just sending it around school. Then he hacked her account and her sister's Facebook account, and he started sending just these deepfakes from this friend of mine's account to literally all the contacts that they both had.' (Poland, 13–15)
			'I was with a guy who I later found out had taken a picture of me when we had sex. It hasn't been shared but I'm still like this: ''he can keep it, he can keep it''. It's unsafe to know that it's there, because even if he deleted it, he could still have it on his phone.' (Sweden, 13–15)
			Then he probably started sending my videos, our videos – we made videos. Sending our videos and my pictures and then ... And I know it's kind of wrong, but I just find it sad because I just trusted him with my body like that. And then he sends it to everyone.' (Germany, 13–15)
			''Because, like, for example, I have my Instagram profile where I might only accept certain people. I share photos, including ones where my face and body are visible. I mean, yes, my profile is private, so only people who follow me can see my photos, but still... just knowing that at any moment someone might suddenly get the idea to take my photo and do whatever they want with it, it honestly gives me chills. Like, it makes me think: wait, maybe I should take it down'' (Italy, 13-15)

Table A6: Children who have been cyberbullied at least once in the past couple of months by Member State, sex and family affluence (%, 11–18-year-olds, 2021–2022)

		Low FAS score	High FAS score
Lithuania	Girls	22	23
	Boys	32	31
Latvia	Girls	28	24
	Boys	23	21
Poland	Girls	23	20
	Boys	23	29
Estonia	Girls	27	21
	Boys	22	16
Ireland	Girls	25	21
	Boys	21	15
Sweden	Girls	22	29
	Boys	13	18
Slovenia	Girls	20	18
	Boys	24	19
Hungary	Girls	24	18
	Boys	20	17

		Low FAS score	High FAS score
Bulgaria	Girls	22	16
	Boys	19	23
Romania	Girls	21	20
	Boys	28	18
Finland	Girls	17	19
	Boys	17	20
Croatia	Girls	18	18
	Boys	18	16
Czechia	Girls	19	20
	Boys	15	13
Denmark	Girls	19	20
	Boys	14	12
Cyprus	Girls	15	16
	Boys	15	15
Slovakia	Girls	19	13
	Boys	16	14

		Low FAS score	High FAS score
Luxembourg	Girls	19	14
	Boys	12	13
Belgium (Flemish Region)	Girls	21	15
	Boys	12	10
Malta	Girls	16	17
	Boys	13	12
Germany	Girls	16	13
	Boys	15	10
Italy	Girls	19	15
	Boys	11	8
Austria	Girls	16	13
	Boys	13	8
France	Girls	15	15
	Boys	9	11
Belgium (Walloon Region)	Girls	15	11
	Boys	10	7

		Low FAS score	High FAS score
Greece	Girls	11	10
	Boys	10	11
Portugal	Girls	10	8
	Boys	9	9
Spain	Girls	11	6
	Boys	5	4

NB: FAS – Family Affluence Scale. Bold indicates a significant difference in prevalence between affluence groups (at $p < 0.05$). Low- and high-affluence groups represent the lowest 20 % and highest 20 % of earners in each Member State / region. Countries are ordered in descending order of prevalence.

Young people were asked if they had experienced cyberbullying (e.g. anyone sending mean instant messages, wall postings or emails or someone posting or sharing photos or videos online without their permission). Response options ranged from 'I have not been cyberbullied in the past couple of months' to 'Several times a week'. The findings presented here show the percentage of young people who had experienced cyberbullying at least once in the past couple of months.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey), https://data-browser.hbsc.org.

Table A7: Prevalence of problematic social media use among children, by Member State, sex and family affluence

		Low FAS score	High FAS score
Romania	Girls	26	28
	Boys	16	18
Malta	Girls	21	25
	Boys	14	16
Ireland	Girls	23	17
	Boys	11	13
Italy	Girls	24	16
	Boys	10	10
Bulgaria	Girls	19	14
	Boys	12	13
Belgium (Walloon Region)	Girls	10	16
	Boys	10	20
Cyprus	Girls	17	17
	Boys	11	9
Greece	Girls	17	17
	Boys	7	11

		Low FAS score	High FAS score
Lithuania	Girls	18	14
	Boys	9	12
Croatia	Girls	11	14
	Boys	11	16
Poland	Girls	13	14
	Boys	9	9
Luxembourg	Girls	17	13
	Boys	7	7
Germania	Girls	16	11
	Boys	8	8
France	Girls	14	13
	Boys	6	8
Slovenia	Girls	12	11
	Boys	9	9
Belgium (Flemish Region)	Girls	14	9
	Boys	8	9

		Low FAS score	High FAS score
Austria	Girls	12	7
	Boys	11	9
Spain	Girls	16	11
	Boys	5	6
Portugal	Girls	10	10
	Boys	8	8
Estonia	Girls	14	9
	Boys	7	6
Czechia	Girls	11	11
	Boys	6	7
Finland	Girls	7	7
	Boys	9	11
Sweden	Girls	11	12
	Boys	3	7
Denmark	Girls	12	8
	Boys	8	6

		Low FAS score	High FAS score
Latvia	Girls	11	8
	Boys	4	6
Hungary	Girls	8	8
	Boys	7	5

NB: FAS – Family Affluence Scale. Bold indicates a significant difference in prevalence by family affluence group (at $p < 0.05$). Low- and high-affluence groups represent the lowest 20 % and highest 20 % of earners in each Member State / region. Countries are ordered in descending order of prevalence.Young people were asked to report symptoms of problematic (addictive-like) social media use using the Social Media Disorder Scale, a nine-item measure to which respondents answered each question with a 'yes' or 'no'. The findings presented here show the percentage of young people who answered 'yes' to six or more questions and were therefore categorised as problematic social media users.

Source: HBSC study data browser (findings from the 2021–2022 HBSC Survey), https://data-browser.hbsc.org.

Table A8: Common types of perpetrators of cyber violence

Type of perpetrator	Tactic	Means used
The troll / the cyber sexual harasser	Attacks women who assert their opinions online	Comments sections, forums, chat rooms
The creepshotter / the digital voyeur	Photographs women and girls without their consent and publishes the photos online	Offline public places, Reddit, dedicated websites, social networks
The revenge pornographer / the digital rapist	Posts private pictures or videos of a sexual nature to shame and humiliate the victim – an extension of intimate partner violence	Social networks
The online groomer / the child sexual abuser	Builds a relationship with a child via the internet to sexually abuse / traffic them	Social networks, forums
The cyberstalker / the obsessive abuser	Spies on, fixates on and compiles information about women online to scare them and blackmail them	Social networks
The masculinist / the woman hater	Negates and perpetuates systemic sexism by 'defending men's rights'	Dedicated websites, women's groups' websites, social networks
The cyberbully / the humiliator	Repeatedly sends hurtful messages and starts rumours to shame and humiliate	Social networks, communication apps
The dating website manipulator / the sexual predator	Seeks power and control over their victim by charming them online and luring them towards a dangerous situation	Dating websites, social networks, chat rooms, communication apps
The recruiter / the rape seller, aka the trafficker	Uses new technologies to lure victims in to traffic and sexually exploit them	Sales websites, dedicated platforms, social media, communication apps
The doxxer / the data thief and criminal shamer	Researches and publishes private information online to publicly expose, out and shame victims	Victim's social network profiles, Google searches
The malicious distributor / the dangerous defamatory	Uses new technologies and propaganda tools to promote violence against women or women's rights groups	Social networks
The hacker / the invader	Intercepts private information and communication (e.g. webcams)	Can be anywhere

Source: Authors, based on classification proposed by the European Women's Lobby.

Table A9: Factors influencing the behaviour of young bystanders (under 20 years of age) witnessing cyber violence

Category	Factor	Summary
Contextual	Friendship	Friendship influences bystander behaviour positively and negatively; positive relationships with victims encourage helping, while strong ties with offenders inhibit intervention.
	Social environment	Social norms and support systems influence behaviour positively and negatively. Positive environments encourage intervention, while norms supporting bullying or rejection discourage it.
	Bystander effect	The likelihood of intervention decreases as the number of bystanders increases (due to the diffusion of responsibility). Perceptions of other bystanders' actions also play a role.
	Incident severity	Severe incidents and visible distress in victims motivate bystanders to intervene.
	Action of other bystanders	The actions of other bystanders influence behaviour; if they support the bully this discourages intervention, but if they defend the victim this encourages support.
	Request for assistance	Direct requests for help motivate bystanders to intervene, as they highlight the seriousness of the situation.
	Evaluation of the situation	Ignorance of the situation or unclear circumstances hinder intervention, while perceived unfairness motivates it.
	Knowledge of strategies	Awareness of effective intervention strategies and support resources encourages positive interventions.
	Virtual environments	Online disinhibition and anonymity can encourage negative behaviour, while public communication channels can reduce it.
	Fear of retaliation	Fear of retaliation can discourage action, though strong friendships with victims can mitigate this fear.
Personal	Empathy	High empathy levels, especially cognitive empathy, encourage behaviours that support victims, while low empathy can lead to passive or negative actions.
	Moral disengagement	High moral disengagement leads to negative bystander behaviour, while low disengagement often results in helpful actions.
	Behavioural determinants	Factors like self-efficacy, a positive attitude and prosocial tendencies facilitate intervention, while impulsivity and social anxiety act as barriers to intervening.
	Previous experience	Past victims are more likely to help, while previous bullies are more likely to engage in negative bystander behaviours.
	Demographic data	In some cases, girls and younger individuals are more likely to intervene.

Source: Authors, based on the conclusions on factors from Dominguez-Hernandez et al. (2018).

European Institute for
Gender Equality

Publications Office
of the European Union
Law | Data | Publications

eige.europa.eu

European Institute for
Gender Equality

ISBN 978-92-9486-350-8 doi:10.2839/5514733

eige.europa.eu

European Institute for Gender Equality

MH-01-26-045-EN-N

FROM LIVED REALITY TO POLICY ACTION:

Combating cyber violence against girls in the EU

An EU Agency