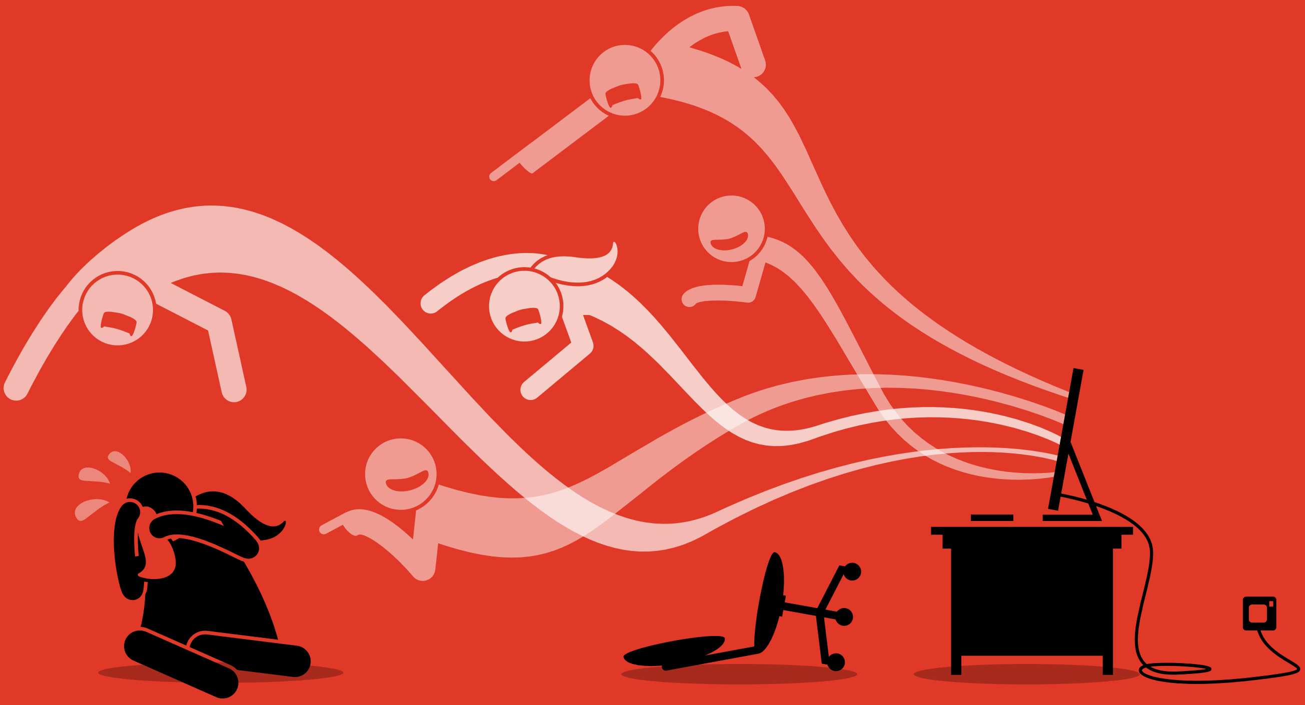
European Commission

Joint Research Centre

# Cyberbullying: Insights from science, policy and legislation

Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A., Lopez Cobo, M.

**2025**



This document is a publication by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

**Contact information**
Name: Daniel Villar-Onrubia
Email: daniel.villar-onrubia@ec.europa.eu

**The Joint Research Centre: EU Science Hub**
https://joint-research-centre.ec.europa.eu

JRC144335
EUR 40535

PDF ISBN 978-92-68-33760-8 ISSN 1831-9424 doi:10.2760/0941861 KJ-01-25-574-EN-N

Luxembourg: Publications Office of the European Union, 2025

Cover page illustration, © leremy / stock.adobe.com

How to cite this report: Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A. and Lopez Cobo, M., *Cyberbullying: Insights from science, policy and legislation,* Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/0941861, JRC144335.

## Contents

## Abstract

This report provides a comprehensive overview of key insights on cyberbullying drawn from scientific literature, policy documents and legislation. The prevalence of cyberbullying is growing worldwide and affects both individuals and societies. Although policymakers and researchers have worked to define and address it, no definition is currently universally accepted, impeding comparable research and coordinated policy action. We argue that a standard definition should be concise, comprehensive and informed by scientific evidence. Based on our analysis, a definition of cyberbullying should include the following elements: aggressive or hostile behaviour, use of digital technologies, imbalance of power, repeated exposure to harming experiences, harm resulting from intention to cause suffering or other motivations. These components should be approached in the light of some considerations: given the rapid pace of technology development and adoption, no specific types of technologies or practices should be mentioned; cyberbullying is a situated phenomenon shaped by social dynamics and norms; it is characterised by the targeting of specific individuals.

The report also summarises scientific findings on: the risk factors related to becoming a cyberbullying perpetrator, victim or both; protective factors; the characteristics of interventions against cyberbullying that are most effective; the uneven distribution of scientific knowledge on this phenomenon and the need for comparative data and EU-wide research.

Additionally, the report reviews policy initiatives and national legislation in the European Economic Area (EEA) relevant to behaviours associated with cyberbullying. This analysis reveals that whereas all countries already address cyberbullying at least to some extent, there is heterogeneity in the definitions found, terms used and legislative approaches to address cyberbullying.

Furthermore, the report outlines a set of policy recommendations that are directly relevant to the upcoming EU Action Plan against cyberbullying, the Better Internet for Kids strategy, the Commission’s broader 2024-2029 priorities to protect children online and the wider need for research on this topic.

## Acknowledgements

The authors would like to thank colleagues from the European Commission at the Directorate-Generals for Communications Networks, Content and Technology (CNECT), Education, Youth, Sport and Culture (EAC), Justice and Consumers (JUST), the Secretariat-General (SG) and the Joint Research Centre (JRC), for their generosity in taking time to review, comment and support this work. We also thank all representatives from the Member States who helped us validate the data collected for a preliminary version of country profiles.

### *Authors*

Daniel Villar Onrubia, Miguel Barreda Ángeles, Romina Cachia, Anastasia Economou, Montserrat López Cobo.

## Executive summary

Cyberbullying is a growing global concern, with roughly one in ten children being affected by it, according to UNESCO (2019). In the European context, about one in 20 youngsters aged between 9 to 16 report being bullied online at least once a month and the prevalence continues to rise despite a range of preventive initiatives, as revealed by the EU Kids Online study (Smahel et al., 2020). Data from studies based on representative samples of middle and high schools' students in the US reveal a steady increase from 33.6% in 2016 to 58.2% in 2025 (Patchin et al., 2025).

This report provides a comprehensive analysis of existing definitions of cyberbullying and how it differs from other harmful online behaviour, based on scientific literature, policy instruments and legislation; identifying a set of key elements that should be present in a standard definition able to support comparative research efforts and coordinated policy initiatives. Furthermore, it summarises key findings from scientific literature on cyberbullying to provide evidence-based recommendations.

### *Policy context*

This report supports the design of the upcoming EU Action Plan against cyberbullying, which is part of a broader effort to create a better, safer online world for children and young people, as part of the European Commission's 2024-2029 priorities to protect children. The wider set of complementary measures for the protection and empowerment of minors online also includes the Guidelines on the protection of minors under Article 28 of the Digital Services Act and enforcement actions, the blueprint for an age-verification solution, an inquiry on the impact of social media on mental health and the implementation of the Better Internet for Kids Strategy (BIK+).

### *Key conclusions*

Cyberbullying represents a complex and multidimensional phenomenon, distinguished by specific characteristics that set it apart from other forms of online violence, cyber aggression or even traditional bullying itself. While various definitions of cyberbullying exist, there is no agreement on a standardised definition. The establishment of a universally accepted definition of cyberbullying, incorporating these unique attributes, is essential for both scientific inquiry and policy development.

Such a definition would enable a foundational framework for different Member States to have a similar recognition of the same concept. Also, it would allow the development of standardised research instruments that would enable comparison of studies, data and the accumulation of evidence regarding effective interventions. In the absence of a shared definition, the development of reliable measures and appropriate strategies to address this phenomenon becomes challenging, thereby impeding advancements in our understanding and response to cyberbullying.

Academic research highlights the need for a specific definition of cyberbullying, since traditional bullying and other forms of online violence do not fully explain cyberbullying. Moreover, cyberbullying has been found to have unique relationships with specific outcome variables, such as risk and protective factors. This distinction is crucial for the formulation of targeted interventions and the enhancement of our collective understanding of effective strategies to combat cyberbullying.

Although not every country in the European Economic Area (EEA) has direct legislation specifically targeting cyberbullying, each country has laws addressing forms of violence that may intersect with this phenomenon. Illegal behaviours that qualify as cyberbullying can differ across jurisdictions, and it can sometimes be difficult — particularly for young individuals — to recognise that certain actions, such as posting content online, may not only be harmful but also illegal. Based on our analysis, we suggest that the fight against cyberbullying should combine specific legal instruments — ensuring that they are applied with caution to avoid the risk of criminalising children — with measures such as psycho-social interventions and educational or skill-development programmes aimed at preventing cyberbullying and equipping people with the required competences to be able to respond to this behaviour.

***Main findings***

Cyberbullying differs from other forms of violence in that perpetrators operate on the basis of some sort of power imbalance and victims are repeatedly exposed over time to harmful behaviour specifically targeted at them through the use of digital technology. Both cyberbullying and traditional bullying are primarily associated with children and young people, whether in research or policy initiatives. However, the use of digital technologies distinguishes cyberbullying from traditional bullying in several ways. The reconfiguration of temporal and spatial boundaries in interactions mediated by digital technologies allows cyberbullying to occur anywhere and anytime, beyond traditional social spaces like the schoolyard. Consequently, cyberbullying can affect larger populations as victims, perpetrators, bystanders or a combination of these roles. The affordances of digital technologies allow cyberbullies to distribute content across large networks, with content potentially becoming viral.

The sense of anonymity provided by digital technologies can alter the traditional power dynamics associated with bullying, sometimes allowing individuals to retaliate or engage in victimisation that might not have occurred without the technological mediation.

Scientific research on cyberbullying identifies several factors that may increase or decrease the likelihood of being affected by this phenomenon. Risk factors often include age, gender, sex, sexual orientation, and belonging to racial, ethnic, or religious minority groups, as well as individual characteristics like being a disabled or gifted student. Conversely, perceived social support from peers or teachers, physical activity within or outside the curriculum (e.g., sports), and certain family dynamics, (e.g., shared leisure activities, having dinner together) can reduce the risks of cyberbullying.

Studies on interventions designed to combat cyberbullying indicate that programs specifically targeting cyberbullying tend to achieve better outcomes, particularly those combining educational and skills development components. School-based interventions have proven effective, while online approaches can also be beneficial. The duration of the programs does not influence their effectiveness; however, shorter interventions tend to be more successful, especially when combined with active parental involvement. Active participation and inclusion of parents in interventions is suggested to potentially enhance outcomes.

EEA countries actively address and aim to combat cyberbullying through awareness programs and legal measures, supported by the EU's Better Internet for Kids strategy. All EU Member States participate in the Safer Internet Initiative. Criminal justice in all EEA countries covers behaviours that, under certain circumstances, can constitute or be related to cyberbullying, often linked to online harassment and violence. Additionally, some have enacted specific articles or adopted ad hoc legislation on cyberbullying.

### *Related and future JRC work*

This report is part of a strand of research at the JRC on the implications of digital technology for wellbeing and mental health, with particular attention to younger populations and digital education. Preliminary findings of this report were synthetised in a policy brief released in August 2025 (Cachia et al., 2025). Previous JRC work also explored the impact of school bullying, including cyberbullying on learning (Karpiński, 2023). Analysis of the impact of social media on well-being and mental health has led to various studies: the impact of social media on loneliness (Blasko et al., 2022); an umbrella review that review risks and opportunities associated with social media (Sala et al., 2024); an analysis of 40,000 students on the time they spent on social media and its impact of anxiety and depression an analysis of 40,000 students (Bertoni et al., 2025).An upcoming report on wellbeing in digital education will offer a model that follows a whole-school perspective.

### *Quick guide*

This science for policy report is organised into seven chapters. **Chapter 1** sets the EU policy context, referring to the Better Internet for Kids (BIK+) strategy, the Digital Services Act (Article 28) and the forthcoming EU Action Plan against cyberbullying, and explains why a common, standard definition is needed. **Chapter 2** outlines the methodological approaches underpinning each of the chapters that present findings. **Chapter 3** offers an introduction of relevant terms in the wider semantic field around online violence and cyber-aggression, looking at the usage in everyday language. **Chapter 4** presents the results of a bibliometric analysis based on data extracted from two databases of scientific documents, namely Scopus and Web of Science. It identifies patterns related to where research of cyberbullying is being produced, influential works, funding, key populations, contexts and practices that are most often studied in connection with this phenomenon. **Chapter 5** summarises the state-of-the-art of scientific research on cyberbullying, looking at the main definitions, findings and conclusions reported in systematic reviews on this topic. **Chapter 6** reviews a set of definitions purposively selected from the academic literature and other influential reports and publications to explore the main components of a cyberbullying definition. **Chapter 7** looks at how international organisation have addressed cyberbullying, as well as at the ways in which national legislation and policies across the European Economic Areas deal with this phenomenon. **Chapter 8** discusses the main findings of the study, outlines key conclusions, and offers a set of policy recommendations in relation to the main elements that should underpin a comprehensive definition of cyberbullying and evidence-based considerations to inform policy actions aimed at fighting this phenomenon.

# 1. Introduction

## 1.1. Background

The European Commission is undertaking various actions to create a safer digital environment for all citizens in Europe, with special attention to children and young people. These efforts encompass the mitigation of online abusive behaviour online by means of an Action Plan against cyberbullying and a social media enquiry, as indicated in the President's Political Guidelines 2024-2029 (von der Leyen, 2024a) and in the mission letters to Commissioners Micallef, Várhelyi and Virkkunen (von der Leyen, 2024b, 2024c, 2024d). In the annual State of the Union speech in September 2025, President von der Leyen (2025) indicated that an expert group would be established to assess whether the European Union (EU) should set up a minimum age for access to social media.

Cyberbullying is a significant concern worldwide, which not only comes with serious consequences for the mental health and wellbeing of victims but also has a broader detrimental impact on society. The potential effect of online violence or aggressive behaviour on minors is particularly worrying. The widespread increase in the use of digital devices and online services — especially social media and video gaming — by young people and children offers an array of opportunities for socialising, creation of content, and learning. However, it simultaneously increases risks such as cyberbullying, which continues to evolve and proliferate. Cyberbullying is linked to adverse effects on wellbeing and mental health, including anxiety, stress, and loneliness, particularly among adolescents and young adults (Dennehy et al., 2020; Kasturiratna et al., 2025; Kowalski et al., 2014).

The pressing nature of cyberbullying is now widely recognised by authorities at national, regional and international levels globally, as reflected in several United Nations (UN) resolutions; including the one on 'Countering cyberbullying' adopted by the Human Rights Council, which recognises that it:

> *"has a negative impact on the fulfilment of human rights, including the rights of the child, and is among children's main concerns, affecting a high percentage of children and compromising their health, emotional well-being and academic work, and acknowledging the need to prevent and eliminate bullying among and of children" (UN General Assembly, 2024, p. 2).*

In the European context, the Better Internet for Kids (BIK+) strategy (EC, 2022), first launched in 2012 and updated in 2022, underscores cyberbullying as a critical threat to children's online safety. Cyberbullying has been consistently the predominant reason for contacting Safer Internet helplines over the past five years across Europe, with 14% of 54,000 calls received in 2024 reporting cyberbullying incidents (European Schoolnet, 2024).

To date, there is a diversity of definitions of cyberbullying and the concept has been operationalised in different ways among researchers and international organisations. While some advocate for its consideration as an extension of traditional bullying, others argue it constitutes a distinct phenomenon. Moreover, the increase of diversity of online behaviours has also prompted new avenues and types of online harassment, some of which can be classified as cyberbullying.

## 1.2. Research objectives

The goal of this report is to inform the upcoming Action Plan against cyberbullying, which will be implemented in close cooperation with Member States, national and local authorities, education institutions, industry and civil society (EC: DG CNECT, 2025b). The report aims to:

- analyse existing definitions of cyberbullying to identify its main components, in particular the specificities of cyberbullying as compared to a) traditional bullying b) other forms of violence;
- summarise key findings from systematic literature reviews, on protective and risk factors, as well as on the effective intervention programmes;
- examine national legislation, policies and initiatives to provide an overview of how cyberbullying is being tackled.

## 1.3. Policy context

Over the last few years, the EU has taken various actions to ensure safe digital environments for all, with particular attention to the protection of children and young people. Most notably, the European Commission has launched a set of complementary measures designed to protect and empower children and young people.

Apart from the already mentioned Action Plan against cyberbullying, the set of measures include the *Guidelines on the protection of minors* (EC, 2025b) under Article 28 of the Digital Services Act (DSA) and enforcement actions, the blueprint for an age-verification solution (EC, 2025a), and an inquiry on the impact of social media on mental health, as well as the implementation of the Better Internet for Kids Strategy BIK+ (EC, 2022). Table 1 provides a summary of the main actions undertaken by the EU to ensure safer digital environment in Europe.

**Table 1.** Actions taken by the EU to ensure safer digital environments

| Year | Action | Description |
|---|---|---|
| **2022** | European strategy for a better internet for kids - BIK+ (EC, 2022) | Aims to ensure that children are protected, respected and empowered online in the new Digital Decade, in line with the EU Strategy on the Rights of the Child (EC, 2021). |
| **2022** | Council conclusions on supporting wellbeing in digital education<br>(Council of the European Union, 2022) | Acknowledge cyberbullying as one of the factors impacting negatively wellbeing in education, as well as the need for digital competence to support anti-bullying policies. |
| **2022** | Digital Services Act (Regulation (EU) 2022/2065 (Digital Services Act), 2022) | Addresses the need to regulate accountability and transparency of online platforms and intermediaries to safeguard users, by placing obligations on providers to address illegal content and harmful activities online. To assist online platforms in ensuring they comply with the DSA's requirement and more specifically *Article 28 – Online protection of minors*, the Commission also provides guidelines to support the protection of minors online under a high level of privacy, safety and security and to ensure a harmonised implementation of the rules in all EU countries. |

| | | |
|---|---|---|
| **2023** | Communication on a comprehensive approach to mental health (EC, 2023) | Bullying prevention programmes in schools are listed as measures to support the psychological wellbeing of children and young people |
| **2024** | Directive (EU) 2024/1385 on combating violence against women and domestic violence, 2024 | This directive is the first comprehensive legal framework aiming to combat violence against women and domestic violence. It calls for minimum rules against cyber-harassment. |
| **2024** | Guidelines on well-being and mental health at school (EC: DG EAC, 2024a, 2024b) | Two sets of guidelines: one for education policy makers and one for school leaders, teachers and educators addressing well-being and mental health at school, whereby (cyber) bullying is also covered. |
| **2024** | Commission Recommendation on developing and strengthening integrated children protection systems in the best interests of the child (EC, 2024) | Recommendations aimed at supporting EU Member States in strengthening their child protection systems. This covers the protection of children's integrity and mental health and helping prevent and fight (cyber) bullying by encouraging Member States to develop national health strategies, whereby children is the priority target group |
| **2025** | Council conclusions on promoting and protecting mental health of children and adolescents in the digital era (Council of the European Union, 2025) | Measures that ensure children and adolescents can use digital technologies in a safe and healthy way. Cyberbullying is one of the potential threats listed that impact young people's mental health. |
| **2025** | Age-verification blueprint (EC, 2025a) | Provides a secure method for users to confirm they are 18 or older when accessing restricted adult material while keeping their personal information private. |
| **2025** | The Union of Skills (EC, 2025d) | A plan to improve skills through high quality education, training and lifelong learning. It aims to ensure that citizens become more digitally competent in relation to wellbeing. |

*Source: Information compiled by JRC*

## 1.4. Relevance of the topic

Bullying is a longstanding issue that has plagued societies throughout history and across the globe. With the advent of electronic and digital information and communication technologies (ICT) — such as the Internet, smartphones, social media and online video games — new potential contexts for the proliferation of this type of aggressive or hostile behaviour have emerged. The term cyberbullying has gained ground as way of referring to manifestations of bullying carried out through digital technologies. Cyberbullying and traditional bullying are often interlinked, with victims simultaneously experiencing both types of aggressive or hostile behaviour (Gefen et al., 2025; Tural Hesapcioglu et al., 2017; WHO, 2022b). However, there is scientific evidence indicating that traditional bullying victimisation and perpetration do not fully explain cyberbullying, which means that cyberbullying must be addressed as a distinct phenomenon requiring separate consideration from traditional bullying (Barlett et al., 2024).

Numerous studies indicate that a growing proportion of minors are subjected to cyberbullying as a regular aspect of their daily lives, underscoring the need for concerted efforts to address the negative effects of this phenomenon on individuals and society at large. The Health Behaviour in School-aged Children (HBSC) study conducted in 2017-2018 shows that 11% of adolescents (11-15 years old) reported problematic social media use associated with cyberbullying (Craig et al., 2020). The same study conducted in 2021-2022 found that around 16% of adolescents reported being cyberbullied in the past couple of months (15% of boy and 16% of girls), while on average 12% had cyberbullied others (Cosma et al., 2024).

Cyberbullying affects 1 in 10 children with 10.1% having experienced cyberbullying through instant messaging, postings, emails and text messages and 8.2% through pictures taken and posted online (UNESCO, 2019). The EU Kids Online research findings published in 2020 showed that in 19 countries, one in 20 children aged 9–16 are bullied online at least every month, while the percentage of children who had experienced cyberbullying continue to increase in eight years despite various stakeholder initiatives (Smahel et al., 2020). In the same study, children reported being both a victim and an aggressor.

In 2022, almost half of United States (US) teens aged 13-17 (46%) reported experiencing cyberbullying. Out of six types of cyberbullying behaviours, name-calling, was the most frequent with 32% of teens reporting that they have been called an offensive name online or on their mobile[1]. Within this sample, older girls (15-17) experienced higher levels of cyberbullying and multiple types of harassment than boys (Pew Research Center, 2022).

Results from fifteen studies conducted by the Cyberbullying Research Centre from 2007 until 2025 using national samples of middle and high schools' students across the US show that while the rates of cyberbullying have varied over the years, there is clear trend showing a steady increase from 33.6% in 2016 to 58.2% in 2025 (Patchin et al., 2025).

The widespread use of digital technologies by young people, the long time spent on such devices and applications, and the new practices they facilitate are potential reasons why cyberbullying is on the increase. Moreover, the growing pervasiveness of Artificial Intelligence (AI), specifically generative AI (GenAI), and their integration in online applications and services, augments risk or even creates new ones related to cyberbullying (EC: JRC, 2025). For example, deepfakes can be typically used maliciously and can lead to cases of cyberbullying (Ofcom, 2024). Since their emergence, deep fakes have been on the increase and can go as far as sexual deepfake abuse (Rousay, 2023), introducing a new dimension of harm that not only damage reputation but like other cyberbullying acts could also potentially lead to psychological trauma (Alexander, 2025; Vaccari et al., 2020).

A universally accepted definition of cyberbullying is crucial for both science and policymaking, as it provides a common foundation for comparing studies and accumulating evidence on interventions, making it challenging to advance our understanding of cyberbullying (Bauman, Cross et al., 2013).

[1] This study measured cyberbullying of teens using six distinct behaviours, namely: (1) offensive name-calling; (2) spreading of false rumours about them; (3) receiving explicit images they did not ask; (4) physical treats; (5) constantly being asked where they are, what they are doing or who they're with by someone other than a parent; (6) having explicit images of them shared without their consent.

# 2. Methodology

In this chapter, we provide an overview of the methodology used for each of the analyses included in the report.

## 2.1. Cyberbullying terminology

The first analysis is based on establishing a foundation of key terms related to cyberbullying and the broader context of technology-mediated violence, drawing on dictionary definitions and web search data to help us understand how these terms are used in everyday life. To gain insight into the frequency and relationships between these terms, we utilised Google web search data,[2] which provides a unique window into the online behaviours and interests of individuals. Specifically, we analysed data from Google Trends,[3] a tool that offers a largely unfiltered sample of actual searches submitted to Google. This data enabled us to visualise interest in specific topics over time across the globe. While this data offers valuable insights into the usage patterns of relevant words, it is essential to acknowledge that Google Trends is not a scientific poll (Google, n.d.).

## 2.2. Bibliometric analysis

Next, we present a bibliometric analysis, which is a valuable method “for deciphering and mapping the cumulative scientific knowledge and evolutionary nuances of well-established fields by making sense of large volumes of unstructured data in rigorous ways” (Donthu et al., 2021). Our aim was to identify key trends and aspects that have defined the evolution of the body of scientific literature on this topic. Based on a structured analysis of two scientific databases, namely Scopus[4] and Web of Science,[5] we offer insights into the exponential growth of scientific literature on cyberbullying, identifying prominent authors, documents, and terms, as well as the countries and funding bodies that stand out due to their role in the production of research on this topic.

## 2.3. Rapid scoping umbrella literature review

Then, we examine the scientific literature by adopting a hybrid approach that combines elements from three typologies of reviews of literature: scoping review, umbrella review, and rapid review. As in a scoping review, our aim is to map and qualitatively describe a field of research rather than quantitatively synthesising evidence (Peters et al., 2021). As in an umbrella review (Aromataris et al., 2015), we include in our review only systematic reviews of the existing literature. And as in a rapid review, we make less stringent some of the parameters typically adopted in a traditional literature review, in order to accelerate the process (Garritty et al., 2021; Smela et al., 2023).. (Garritty et al., 2021; Peters et al., 2021; Smela et al., 2023)

[2] The choice of Google as a valuable source of search data is based on its status as a very large online search engine under the DSA (Regulation (EU) 2022/2065 (Digital Services Act), 2022), with a monthly average of 364 million active users as of September 2025 (EC, 2025c).

[3] https://trends.google.com/

[4] https://www.scopus.com/

[5] https://www.webofscience.com/

This way, we limited our review to systematic literature reviews, therefore excluding primary research articles. This choice was motivated by the fact that, given the extremely large number of published articles on cyberbullying, reviewing all of them would have been unfeasible within the limited time available for this work. By including only systematic literature reviews, we built on the evidence syntheses already conducted by other researchers, allowing us to identify the main aspects addressed in the scientific study of cyberbullying, namely those areas where abundant literature has led to the production of systematic reviews.

Therefore, this scoping umbrella review aimed to identify the main dimensions of the phenomenon as studied in scientific research, the state of the evidence regarding these dimensions, and the definitions of cyberbullying included in systematic literature reviews. In our case, adopting a rapid review approach involved consulting only one database (Web of Science), restricting the search to the last five years, and having one of the three reviewers involved in the process conduct the article selection and data extraction.

## 2.4. Review of cyberbullying definitions in the scientific literature

Third, we present a review of a narrower set of scientific publications of different kinds, purposively selected due to their relevance to the challenge of establishing a common definition of cyberbullying. To identify the main components that underpin the notion of cyberbullying in the scientific literature, we drew on highly influential journal articles identified in our bibliometric analysis and review of systematic reviews, while complementing these with insights from other relevant scientific publications, such as book chapters and reports.

## 2.5. Insights from policy and legislation

Mirroring the review process of selected cyberbullying definitions within the academic literature presented in the fourth chapter, in Chapter 5 we analysed documents by international organisations to gain insight into how this concept has been defined in the context of policy efforts aimed at fighting cyberbullying.

In addition, we examined the definitions provided in legislation within the EEA. Complementing previous research by the BIK+ initiative (EC: DG CNECT, 2025a), the European Parliamentary Research Service (Murphy, 2024), and the Council of Europe (2018), our analysis covered relevant legislation that addresses cyberbullying in a broad sense, either directly or indirectly. We look at criminal and civil law addressing cyberbullying and other related offenses that may be related to or apply to cyberbullying when committed through electronic means. We take stock of different terminology used to refer to cyberbullying or other forms of online violence in legislation (e.g., online harassment, digital bullying, stalking, obsessive harassment), as well as definitions provided. Finally, we present examples of initiatives and actions at national or regional level.

Legislation, definitions, and terms have been reviewed in English when translations are available from the original source; otherwise, machine translation from the national language has been used. As a result, there may be discrepancies between the translated definitions and terms and those in the original national language. For example, a term that corresponds to ‘cyberbullying’ in the original language might be translated as ‘online harassment’, and vice versa. Translated terms may not fully capture the underlying concepts. Additionally, our research may have inadvertently omitted relevant definitions due to the focus on legislation, and diversity in terminology and languages across the EU.

## 2.6. Digital tools

Apart from the platforms mentioned above as sources of data, we used several tools to support different processes throughout our research.

Zotero,[6] a tool to manage bibliographic references, was used to organise and annotate all the documents included in our review of scientific literature, policy documents and legislation.

Bibliometrix,[7] as science mapping tool (Aria et al., 2017), was used to performed more advanced analysis on some of the datasets extracted from bibliographic databases.

GPT@JRC, an in-house tool launched by the European Commission in 2023 to enable experimentation with GenAI across EU bodies, was employed to support analytical tasks during the review, as well as for text enhancement in the drafting of this report (Fernandez Machado et al., 2025). The tool was employed in line with the *Living guidelines on the responsible use of generative AI in research* (EC: DG RTD, 2025), meaning that the authors remain ultimately responsible for the scientific output.

[6] https://www.zotero.org/

[7] https://www.bibliometrix.org/

# 3. Cyberbullying terminology: key concepts and usage

This section offers a comprehensive overview of the key concepts, definitions, and terminology related to cyberbullying and related forms of cyber-aggression. It examines the language used to describe the various manifestations of these complex issues. Drawing on Google web search data, it reveals patterns and variations in the relative frequency of term usage. Furthermore, it expands the scope of discussion by introducing a broader range of terms that denote specific practices and types of behaviour that can be considered as manifestations of cyberbullying, thereby enhancing our understanding of this multifaceted phenomenon.

## 3.1. Introduction to the semantic field of online violence and cyber-aggression

According to the *Oxford English Dictionary* (OED), a bully is “a person who habitually seeks to harm, coerce, or intimidate those whom they perceive as vulnerable” (OED, 2024a), while **bullying** is currently understood as: “...the action or practice of seeking to harm, coerce, or intimidate someone perceived as vulnerable, esp. on a persistent or regular basis” (OED, 2024b). More specifically, the OED defines **cyber-bullying** as the “use of information technology to bully a person by sending or posting text or images of an intimidating or threatening nature” (OED, 2025a).

There is a considerable overlap between the term ‘cyberbullying’[8] and other compound words that refer to the use of digital technologies for abusive purposes. Terms related to digital technology — like ‘cyber’, ‘online’ or ‘Internet’ — are often combined with other words that denote aggressive or hostile behaviour, such as ‘stalking’, ‘victimisation’, ‘mobbing’ or ‘violence’.

In addition to the previous compound, another common term within this semantic field is **online harassment**, where ‘harassment’ refers to “unwarranted (and now esp. unlawful) speech or behaviour causing annoyance, alarm, distress, or intimidation, usually occurring persistently over a period of time”. (OED, 2023). While the OED does not have a separate entry for ‘online harassment’, when defining ‘harassment’ it highlights that it often comes with a modifying word (e.g., online, sexual, racial). PEN America treats the terms ‘online harassment’ and ‘online abuse’ as synonyms and defines them as “pervasive or severe targeting of an individual or group online through harmful behavior.” (PEN America, n.d.),

Other similar terms include ‘cyberstalking’ or ‘cyber-mobbing’, though they describe more specific types of abusive behaviour. Namely, to **cyberstalk** someone can be defined as the “action of intimidating or harassing a person online by persistently sending messages or images of an obsessive, threatening, or offensive nature” (OED, 2025b). The *Oxford English Dictionary* does not provide a definition for **cyber-mobbing**, suggesting that it is a relatively less established term. However, based on the entry for the main component (i.e., ‘mobbing’) of this compound word, it could be defined as the use of digital technology to facilitate the “action of a mob or group of people in attacking, harassing, [...] a person” (OED, 2025c).

[8] While the Oxford English Dictionary definition includes a hyphen, it is becoming increasingly common to combine the prefix and root word directly to form a single, cohesive term.

While the English terms ‘bullying’ and ‘cyberbullying’ are often adopted by other languages to describe these phenomena, many languages have native terms that either fully or partially overlap with these meanings. For example, the words ‘*acoso’* in Spanish or ‘*ijime’* in Japanese capture varying degrees of the elements characteristic of bullying (Smith et al., 2013).

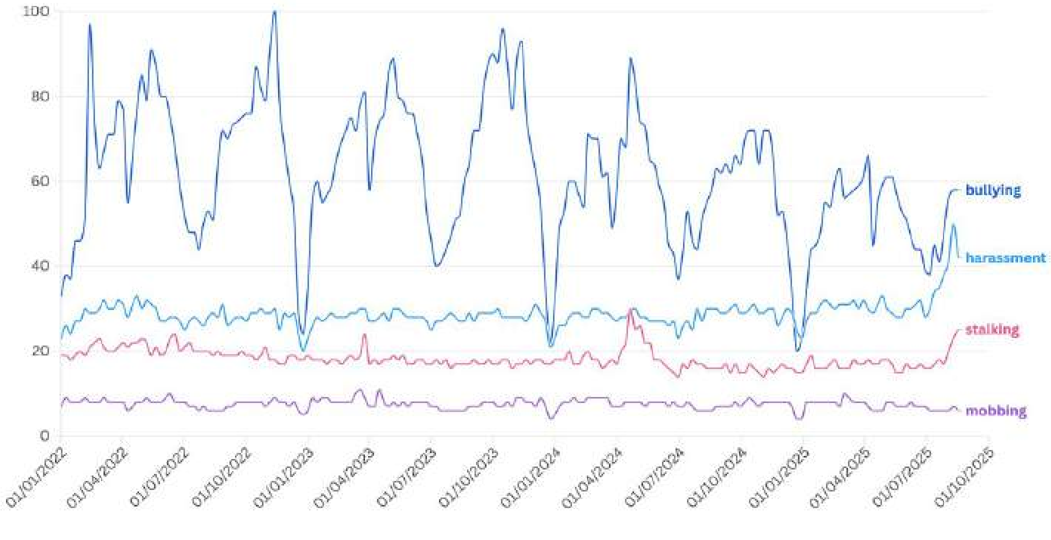
## 3.2. Frequency of use in online searches

Looking at how often certain keywords are submitted by Internet users to popular search engines can help us understand the popularity of terminology. Figure 1 shows the relative interest of several terms within the semantic field related to abusive behaviour, as indicated by the queries submitted worldwide to the search engine Google between January 2022 and August 2025.

If Figure 1 shows that ‘bullying’ is the most searched term among the four included words, Figure 2 indicates that when the focus is narrowed to abusive behaviours involving digital technology, ‘cyberbullying’ is even more frequently searched than the other related terms.

Considering that they generally refer to repeated acts of aggression towards specific individuals, rather than isolated incidents, ‘bullying’ and ‘harassment’ are often used interchangeably — with ‘cyberbullying’ and ‘online harassment’ overlapping in similar ways. However, the definitions discussed above suggest some distinctions between them, as ‘bullying’ is presented as a more general concept that encompasses a wide range of hostile behaviours that may not necessarily be illegal. In contrast, according to the lexicographical definition above, ‘harassment’ often involves actions that are more likely to be considered unlawful. Nevertheless, this nuanced interpretation does not appear to be reflected in the way this terminology is used in academic literature as discussed in the next section.

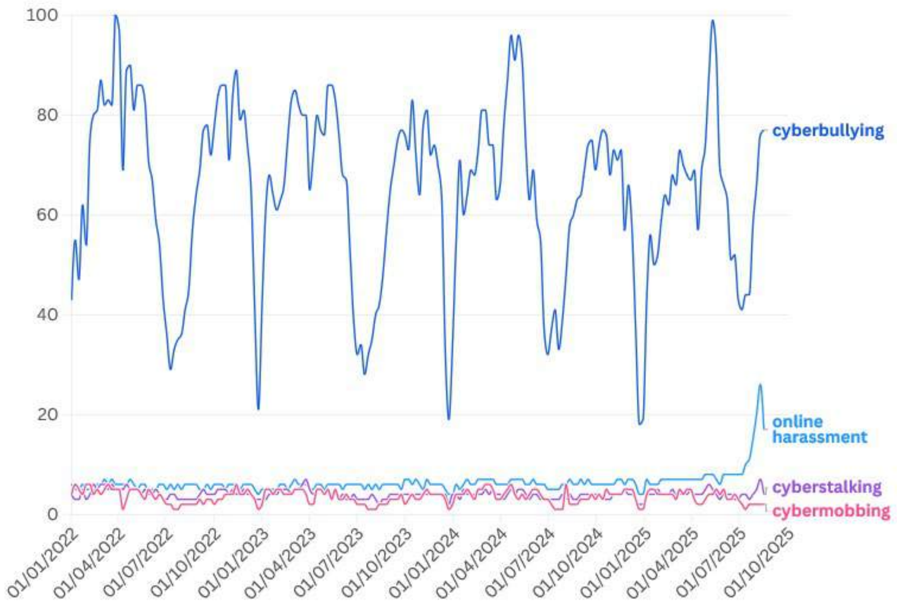
**Figure 1.** Interest over time on bullying and related terms from Google search users[1], 2022-2025



[1] Note: The numbers indicate search interest in relation to the peak point on the chart for the specified time period. A value of 100 signifies the term's maximum popularity. A value of 50 indicates that the term is half as popular.

*Source: JRC elaboration based on data exported from https://trends.google.com. Chart created with flourish.studio.*

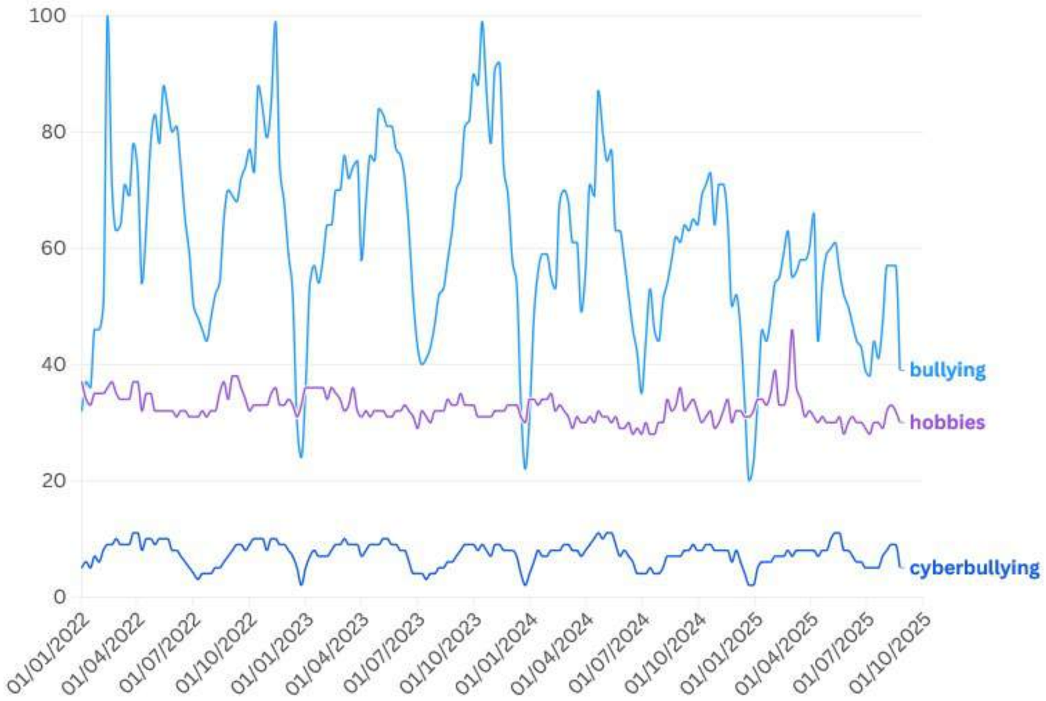
**Figure 2.** Interest over time on cyberbullying and related terms from Google search users[1], 2022-2025



[1] Note: The numbers indicate search interest in relation to the peak point on the chart for the specified time period. A value of 100 signifies the term's maximum popularity. A value of 50 indicates that the term is half as popular. Chart created with flourish.studio

*Source: JRC elaboration based on data exported from https://trends.google.com.*

**Figure 3.** Interest over time on bullying and related terms from Google search users[1], 2022-2025



[1] Note: The numbers indicate search interest in relation to the peak point on the chart for the specified time period. A value of 100 signifies the term's maximum popularity. A value of 50 indicates that the term is half as popular. Chart created with flourish.studio

*Source: JRC elaboration based on data exported from https://trends.google.com.*

Bullying and cyberbullying are often associated with children, young people and educational contexts. This association might explain the pronounced dropping in Google searches for both ‘bullying’ and ‘cyberbullying’ that consistently occurs around the winter and summer breaks in the academic year, as shown in Figure 1 and Figure 2. Suggesting that this is not just due to an overall reduction in searches of any type coinciding with those periods, Figure 3 compares the fluctuations with those of an unrelated random term (‘hobbies’) that is presumably not affected to the same extent by those variations.

## 3.3. Glossary of cyberbullying manifestations

Cyberbullying can be understood as a specific form of cyber-aggression, a broader term referring to “intentional behavior aimed at harming another person or persons through computers, cell phones, and other electronic devices, and perceived as aversive by the victim” (Schoffstall et al., 2011, p. 588). The specificities of cyberbullying as compared to more generic forms of technology-mediated aggressions will be discussed later in the report.

At the same time, cyberbullying is associated with a wide and rapidly expanding range of both colloquial expressions (i.e., lingo) and formal terms (i.e., jargon) that describe specific forms of abusive behaviour that, under certain circumstances, may be regarded as cyberbullying. Table 2 includes relevant vocabulary and definitions extracted from the literature. As the lingo associated with cyberbullying is in constant flux, it is essential to follow the coining of terms referring to both well-established and emerging abusive behaviours. While the prevalence of cyberbullying continues to grow, there is no consensus yet on a standardised definition. The next sections of this report provide an overview of this topic as addressed in research and policymaking, including key considerations regarding how the concept is being defined in both arenas.

**Table 2.** Glossary of terms denoting behaviours and practices that are somehow related to cyberbullying.

| Term[1] | Description | Source |
|---|---|---|
| **Catfishing** | “steal[ing] someone’s identity and information to cheat others with a fake profile.” | Teng et al. (2024, p. 5) |
| **Cyber-Mob Attacks, also known as Dogpiling (cyber-mobbing)** | “when a large group of abusers collectively attacks a target through a barrage of threats, slurs, insults, and other abusive tactics.” | PEN America (n.d.) |
| **Cyberstalking** | “sending electronic content, such as messages or photos, to annoy, threaten and scare an individual.” | Teng et al. (2024, p. 5) |
| **Deepfake cyberbullying** | “hyper-realistic, fabricated content, depicting students in harmful or compromising scenarios they never participated in, leading to severe reputational damage and emotional trauma” | Alexander (2025) |
| **(online) Denigration** | “gossiping or spreading fake rumors about an individual to spoil an individual’s reputation” | Teng et al. (2024, p. 5) |
| **Dissing** | “posting information to damage an individual’s public image”. | Teng et al. (2024, p. 5) |

| Term[1] | Description | Source |
|---|---|---|
| **Doxing** | “personal information on others is sought and released, thereby violating their privacy and facilitating further harassment.” | Chen et al. (2019, p. 1) |
| **Flaming (roasting)** | “starting online fighting with anger, usually with upper case letters to indicate such emotion” | Teng et al. (2024, p. 4) |
| **Flooding** | “sending bullying content to an individual limitlessly” | Teng et al. (2024, p. 5) |
| **Hateful speech** | “Expression that attacks a specific aspect of a person’s identity, such as their race, ethnicity, gender identity, religion, sexual orientation, disability, etc. Hateful speech online often takes the form of ad hominem attacks, which invoke prejudicial feelings over intellectual arguments in order to avoid discussion of the topic at hand by attacking a person’s character or attributes.” | PEN America (n.d.) |
| **(cyber) (online) Grooming (Internet predation)** | “this is generally limited to adults using technology to solicit and recruit children into online or offline sexual encounters or to obtain sexual images or videos. Online grooming offences can be perpetrated by adults encountered online and adults already known to the child from offline venues (49–51). Canadian police statistics find 61% of online grooming offenders are offline acquaintances or friends.” | WHO (2022, p. 5) |
| **(cyber) (online) Harassment** | “involves sending insulting and abusive messages repeatedly and continually toward an individual. The behavior of discriminating against an individual by appearance, gender, and race falls in this type.” | Teng et al. (2024, p. 4) |
| **(online) Impersonation (fraping)** | “Creation of a hoax social media account, often using the target’s name and/or photo, to post offensive or inflammatory statements to defame, discredit, or instigate further abuse. A harasser can also impersonate someone the target knows in order to cause harm.” | Pen America (n.d.) |
| **Masquerading** | “involves pretending to be someone else to send something to an individual by hiding his identity” | Teng et al. (2024, p. 5) |
| **Nonconsensual sexting (revenge porn)** | “distributing sexual images of someone without the consent of the victim)” | Gámez-Guadix et al., 2022, p. 790) |
| **Outing** | “sharing information that encompasses private or personal content with the public” | Teng et al. (2024, p. 5) |
| **Pulling a pig** | “sending messages to seduce girls considered not pretty and fat and making fun of it by publicly posting the conversation” | Teng et al. (2024, p. 5) |
| **(online) Solicitation** | [solicitation for sexual activities] “may come from a wide variety of solicitors, including many peer solicitations that are unwanted, frightening and harassing” | WHO (2022, p. 5) |

| Term[1] | Description | Source |
|---|---|---|
| **(online) Racism** | "posting something to discriminate against an individual due to different aspects of ethnicity, nationality, religion, and race." | Teng et al. (2024, p. 5) |
| **Sextortion** | "threatening with distributing sexual images to pressure the victim into doing something" | Gámez-Guadix et al., (2022, p. 290) |
| **Social exclusion (ostracism)** | "excluding an individual from a social group or making an individual feel outcast. For instance, this occurs in the chat room or online discussion group by removing or unfriending an individual from the list" | Teng et al. (2024, p. 5) |
| **Trickery (deception)** | "tricking an individual into getting his trust but later exposing his information to the public." | Teng et al. (2024, p. 5) |
| **(online) Trolling** | "posting controversial content in online spaces [...] as a form of entertaining activity for both trolls and (some) bystanders at the behest of the victims." | Scriven (2025, pp. 284–285) |

[1] Note: Within brackets equivalent terms and common qualifiers denoting the technology-mediated nature of aggressions, added by the authors.

*Source: Extracted by JRC researchers from diverse sources, as indicated in the third column.*

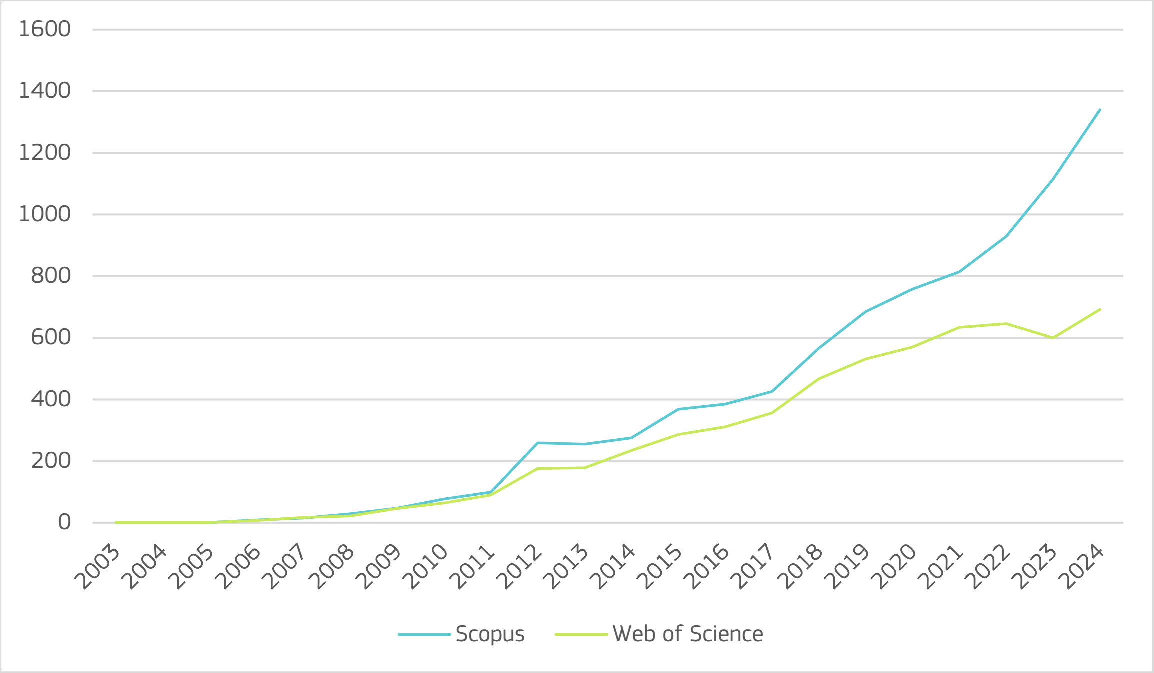
# 4. Bibliometrics analysis on cyberbullying research

This chapter presents the results of a bibliometric analysis based on data extracted from two databases of scientific documents, namely Scopus and Web of Science. It identifies patterns related to where research of cyberbullying is being produced, influential works, funding, key populations, contexts and practices that are most often studied in connection with this phenomenon.

## 4.1. Overview

Research on cyberbullying has grown exponentially over the last two decades. According to the Web of Science[9] and Scopus[10] databases, the number of documents — including journal articles, conference papers, book chapters, etc. — mentioning this term increased exponentially from 2003 to 2024 (see Figure 4). In total, Web of Science indexed 6,441 scientific documents between 2003 and September 2025,[11] while Scopus had 9,447 indexed during that period.

**Figure 4.** Scientific documents on cyberbullying[1], 2003-2024



[1] Note: Documents that mention “cyberbullying”, “cyber-bullying” or “cyber bullying” in their titles, abstracts or keywords.

*Source: JRC elaboration based on data from Scopus and Web of Science.*

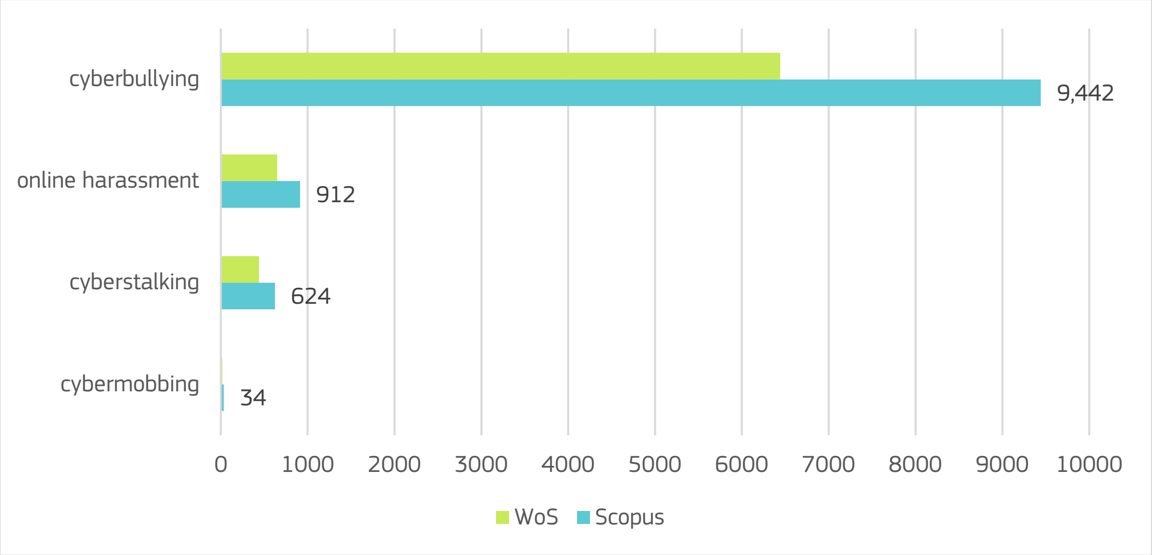
[9] Documents retrieved by means of the following query: TS=(cyberbullying OR cyber-bullying OR "cyber bullying")

[10] Documents retrieved by means of the following query: TITLE-ABS-KEY ( cyberbullying OR cyber-bullying OR "cyber bullying" )

[11] Search conducted on 25 September 2025.

As shown in Figure 5, the term ‘cyberbullying’ stands out prominently compared to other terms describing technology-mediated abusive behaviours, with frequencies that mirror those of Google searches presented earlier (Figure 2).

**Figure 5.** Number of scientific documents that mention ‘cyberbullying’ and other terms denoting technology-mediated abuse[1], 2003-2025



[1] Note: Documents that mention the relevant terms in titles, abstracts or keywords.

*Source: JRC elaboration based on data retrieved from Scopus and Web of Science in September 2025.*

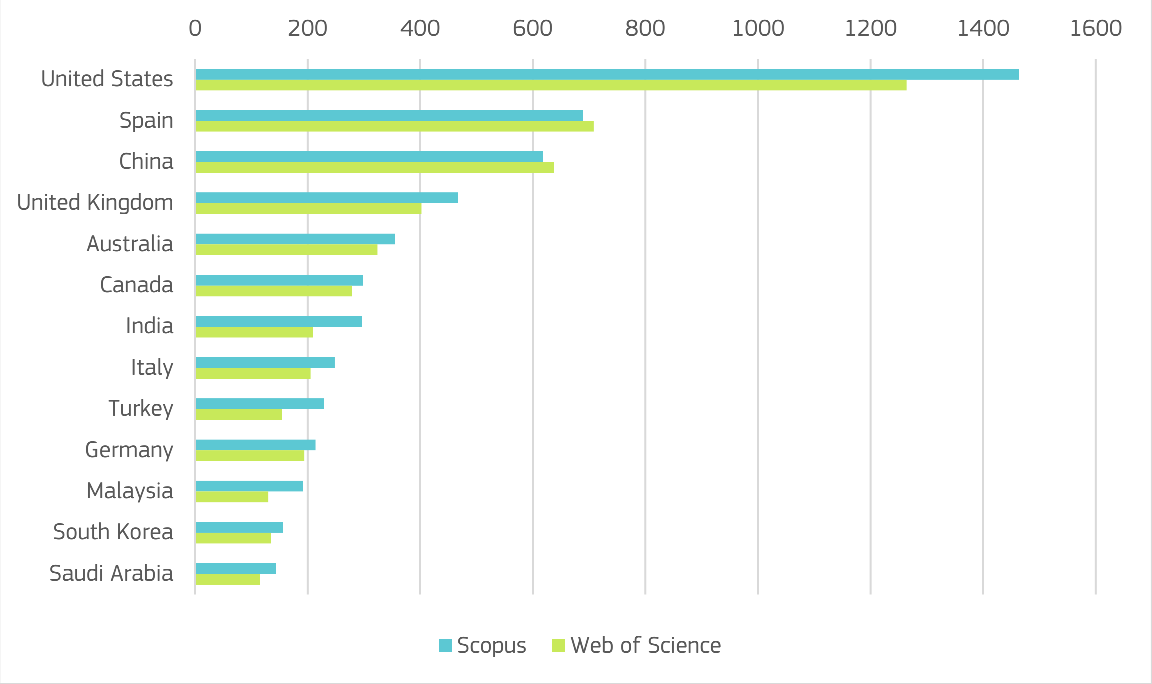
## 4.2. Territorial distribution, funding and languages

As shown in Figure 6, the production of scientific articles on cyberbullying is largely concentrated in the United States (US), followed by Spain and China.[12] A more thorough look at these data shows that articles on this topic have increased steadily in the US, Spain, the UK and Australia, while rocketing in China over the last few years. All countries in the EU have contributed to the production of scientific knowledge on cyberbullying. Over 2,000 articles in total indexed in the Web of Science database have been produced by researchers affiliated with research institutions in EU Member States. After excluding the three most active EU Member States (i.e., Spain, Germany and Italy), the average number of articles on cyberbullying indexed in that database per remaining MS is 37.8, with a standard deviation of 31.1. Approximately one-third of EU MSs produced fewer than 20 articles each, with a handful producing fewer than 5 articles.

Certain higher institutions stand out as knowledge hubs for the study of cyberbullying. As shown in Figure 7, five universities from the UK, the US, Canada and Spain have been particularly active in this field, with the number of articles their researchers have published on this phenomenon consistently growing over the last 15 years.

[12] It should be noted that the country refers to country of authors’ affiliation. with all authors being accounted for (i.e., a publication with several authors are counted once per author).

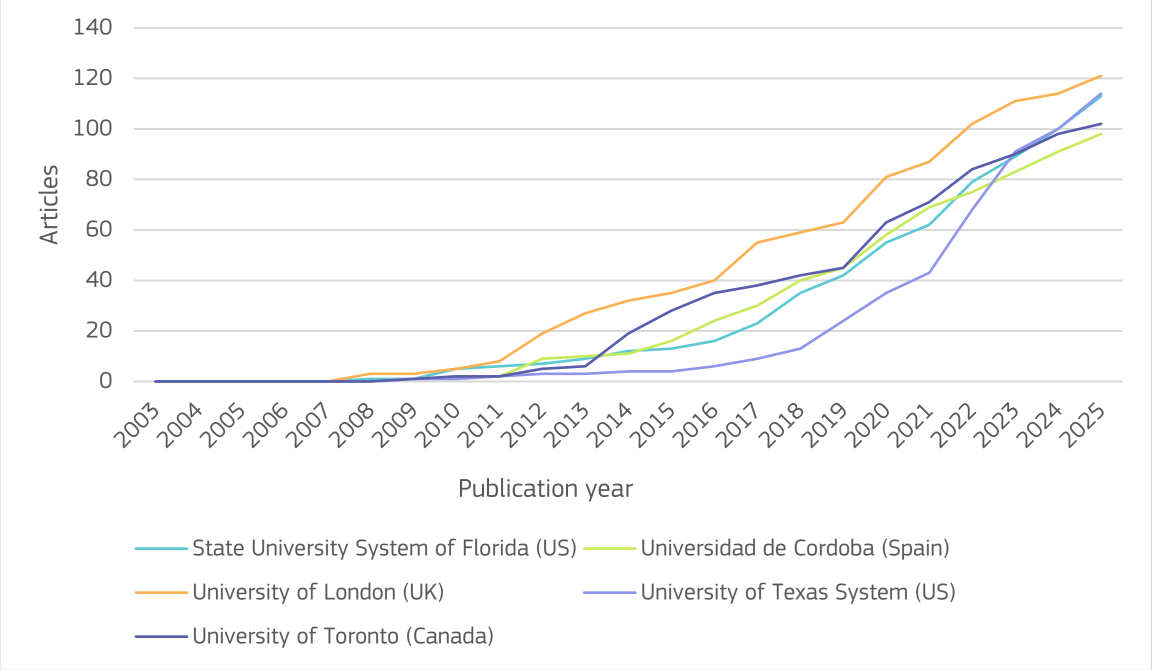
**Figure 6.** Scientific articles on cyberbullying in Scopus and Web of Science by authors' affiliation country[1], 2003-2025



[1] Note: publications are associated to countries based on authors' affiliations and therefore one article might be included in more than one country.

*Source: JRC own elaboration, based on data retrieved in September 2025 from the Scopus and Web of Science databases.*

**Figure 7.** Cumulative number of scientific articles on cyberbullying by university, 2003-2025



*Source: JRC own elaboration, based on data from Web of Science.*

The main funders supporting the publication of scientific research on cyberbullying as indexed in both databases include institutions and funding programmes in the EU (e.g., Horizon, Erasmus, European Regional Development Fund, European Research Council) and the governments of the US (e.g. Department of Health Human Services, National Science Foundation), China (e.g., National Natural Science Foundation, National Social Science Fund of China), Spain (e.g., Ministry of Science and Innovation), Canada (e.g., Social Sciences Humanities Research Council, Canadian Institutes of Health Research) and the United Kingdom (e.g., UK Research Innovation, Economic and Social Research Council).

Apart from English, there are other European languages actively used in the publication of scientific articles on this topic, most notably Spanish, German, Portuguese, French and Italian (Table 3).

**Table 3.** Scientific articles, including reviews, on cyberbullying in Scopus and Web of Science by language, 2003-2025

| Language | Scopus | Web of Science |
|---|---|---|
| English | 5,717 | 4,931 |
| Spanish | 275 | 239 |
| German | 40 | 38 |
| Portuguese | 47 | 34 |
| Russian | 48 | 34 |
| Turkish | 26 | 19 |
| French | 33 | 15 |
| Italian | 30 | 9 |
| Croatian | 9 | 5 |
| Chinese | 51 | 4 |

*Source: JRC own elaboration, based on data from the Scopus and Web of Science databases.*

## 4.3. Influential works and authors

When mapping the scientific literature on a particular topic, looking at the most widely cited articles can help to identify the authors, findings and ideas that are driving forward that body of knowledge by shaping the work of others. Scopus and Web of Science yield an identical top-seven list, with each article appearing in the same rank position in both databases, as listed in Table 4.

**Table 4.** Top 10 most cited articles on cyberbullying in the period 2003-2025

| Article | Citations in Scopus | Citations in Web of Science |
|---|---|---|
| Cyberbullying: its nature and impact in secondary school pupils (Smith et al., 2008) | 2,579 | 1,982 |
| Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth (Kowalski et al., 2014) | 2,155 | 1,760 |
| Following you home from school: A critical review and synthesis of research on cyberbullying victimization (Tokunaga, 2010) | 1,817 | 1,437 |
| School Bullying Among Adolescents in the United States: Physical, Verbal, Relational, and Cyber (J. Wang et al., 2009) | 1,468 | 1,211 |
| Bullying, cyberbullying, and suicide (Hinduja et al., 2010) | 1,420 | 1,100 |
| Clinical Report-The Impact of Social Media on Children, Adolescents, and Families (O'Keeffe et al., 2011) | 1,316 | 996 |
| Cyberbullying: Another main type of bullying? (Slonje et al., 2008) | 1,252 | 952 |

*Source: JRC own elaboration, based on data from the Scopus and Web of Science databases.*

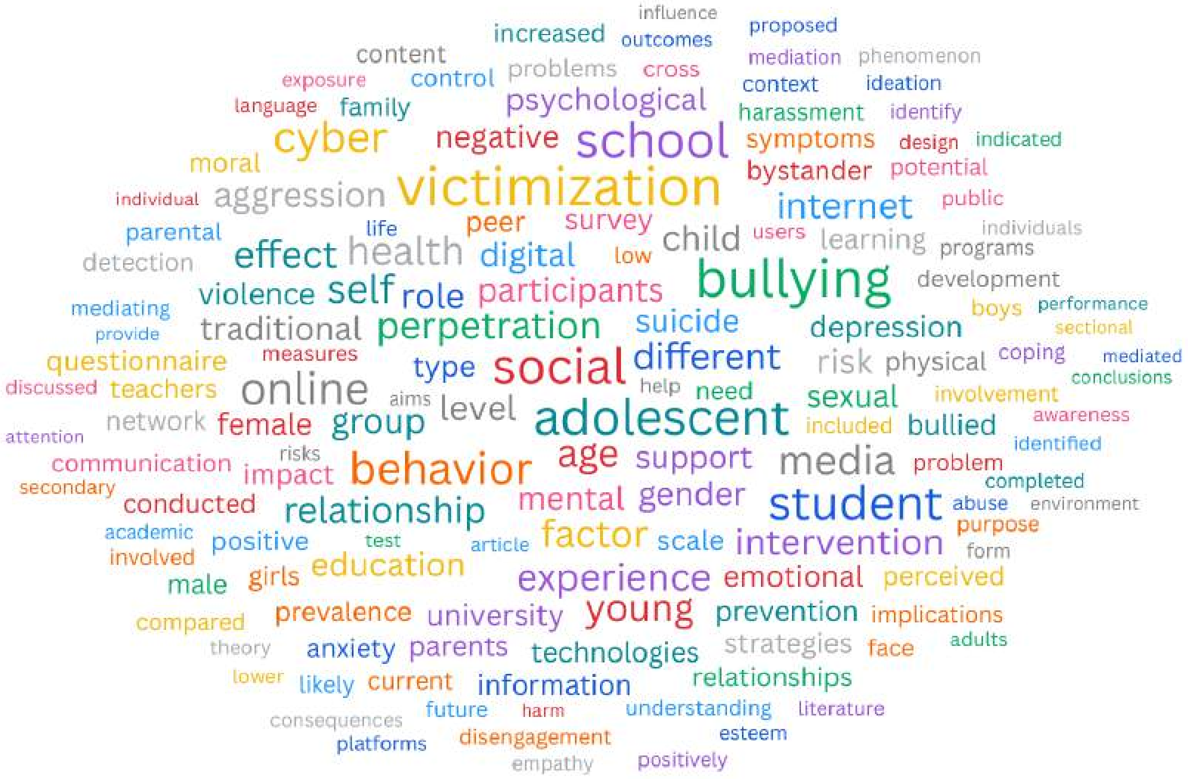
## 4.4. Analysis of key terms

Identifying the words most frequently used within the abstracts of scientific articles on cyberbullying (Figure 8) can provide valuable insights into key aspects and dimensions that define the body of literature on this topic. For example, by revealing the populations and social contexts (e.g., adolescents, schools) or the consequences (e.g., depression, anxiety, suicide) that are most often studied in connection with this phenomenon.

Table 5 shows how often certain terms are mentioned across the abstracts of scientific articles. These data reveal that cyberbullying is often discussed in relation to the broader phenomenon of bullying and tends to be characterised as a form of victimisation, aggression, violence, harassment, or abuse. Scientific articles on this topic are largely concerned with young people, as indicated by the frequent mentioning of adolescents, children, youth, girls or boys.

Likewise, the phenomenon is often approached in connection with educational contexts, as suggested by the reference to schools, students, universities or colleges. Regarding the actors involved in cyberbullying, scientific articles seem to be particularly focused on the victims, while also paying attention to other stakeholders that can play an important role, such as parents, peers, teachers and bystanders.

**Figure 8.** Top 200 words[1] most frequently mentioned across the abstracts of scientific articles on cyberbullying in Scopus and Web of Science, 2003-2025



[1] Note: Terms stemming from the same root are considered as one word (e.g., 'school' and 'schools', 'aggressive' and 'aggressor'. Common words that are not relevant were excluded (e.g., research, results, findings)

*Source: JRC own elaboration, based on a dataset of 7,700 abstracts extracted from Web of Science and Scopus, processed with voyant-tools.org. Chart created with flourish.studio.*

**Table 5**. Words most frequently used in the abstracts of scientific articles on cyberbullying by semantic field, 2003-2025

| Semantic field | Stems and single words | Wordcount | Aggregated terms |
|---|---|---|---|
| Aggressive behaviour | bull* | 13961 | 'bullying', 'bully', 'bullied', etc. |
| Aggressive behaviour | victimi* | 7428 | 'victimization', 'victimisation', 'victimized', etc. |
| Aggressive behaviour | aggress* | 3086 | 'aggression', aggressive', 'aggressor', etc. |
| Aggressive behaviour | violen* | 2093 | 'violence', 'violent', etc. |
| Aggressive behaviour | harass* | 1250 | 'harassment', 'harass', 'harassed', etc. |
| Aggressive behaviour | abus* | 1043 | 'abuse', 'abusive', etc. |
| Technology | online | 5952 | |
| Technology | "social media" | 3269 | |
| Technology | Internet | 3123 | |

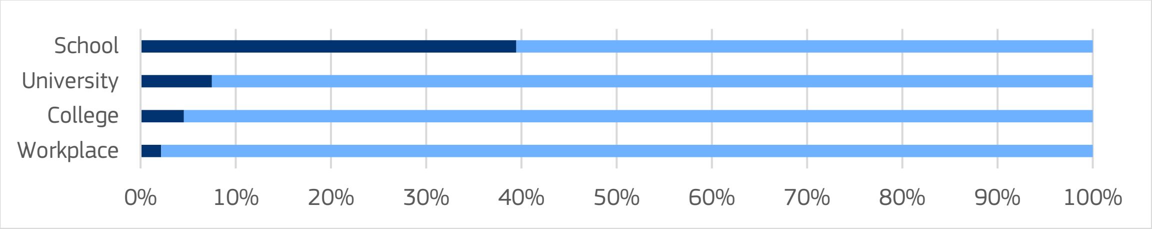
| Semantic field | Stems and single words | Wordcount | Aggregated terms |
|---|---|---|---|
| Technology | Digital* | 2291 | 'digitalization', digitally', etc. |
| Technology | technolog* | 1891 | 'technology', 'technological', etc. |
| Technology | electronic* | 465 | 'Electronic', 'electronically' |
| Technology | screen* | 386 | 'Screen', 'screens', etc. |
| Technology | computer* | 277 | 'computers', 'computerized' |
| Age groups | adolesc* | 8769 | 'adolescents', 'adolescent', 'adolescence', etc. |
| Age groups | child* | 3630 | 'children', 'child', 'childhood', etc. |
| Age groups | youth* | 2139 | 'youth', 'youths', etc. |
| Age groups | young* | 2139 | 'young', 'younger', 'youngster', etc. |
| Age groups | girls | 1384 | |
| Age groups | boys | 1035 | |
| Age groups | adult* | 1098 | |
| Education | student* | 8006 | 'students', 'student', etc. |
| Education | educat* | 2884 | 'education', 'educational', 'educator', etc. |
| Education | school* | 1809 | 'school', 'schools', 'schoolchildren', etc. |
| Education | university* | 1165 | 'university', 'universities', etc. |
| Education | college* | 812 | 'college', 'colleges' |
| Actors | 'victims' + 'victim' | 4747 | |
| Actors | parent* | 3499 | 'parents', 'parental', 'parenting', parent, etc. |
| Actors | teacher* | 1678 | 'teachers', 'teacher' |
| Actors | famil* | 1578 | 'family', 'families' |
| Actors | bystander* | 1368 | 'bystander', 'bystanders' |
| Actors | perpetrato* | 846 | 'perpetrator', 'perpetrators' |
| Actors | 'cyberbully' + 'cyberbullies' | 782 | |
| Actors | bullies | 493 | |
| Actors | aggressor* | 363 | 'aggressor, 'aggressors' |
| Gender | female* | 1805 | 'female', females' |
| Gender | male* | 1402 | 'male', 'males' |
| Gender | girls | 1429 | 'girl', girls' |

| Semantic field | Stems and single words | Wordcount | Aggregated terms |
|---|---|---|---|
| Gender | boy* | 1065 | 'boy', 'boys' |
| Gender | transgender | 105 | |
| Wellbeing | health* | 4093 | 'healthy', 'healthcare', etc. |
| Wellbeing | depress* | 2455 | 'depression', 'depressive' |
| Wellbeing | anxi* | 1447 | 'anxiety', 'anxious', etc. |
| Wellbeing | *steem | 847 | 'selfesteem' |

*Source: JRC own elaboration, based on data from the Scopus and Web of Science databases.*

In order to have a better understanding of the level of attention paid across this body of literature to, for example, particular subjects, practices or socio-technical contexts, it is useful to look at the number of articles that mention certain terms in their abstracts as compared to others. In this regard, we can observe in Figure 9 that schools stand out as a core organisational setting in relation to which cyberbullying is studied, being mentioned in almost 40% of abstracts. This is in stark contrast with workplaces, only mentioned in about 2% of them.

**Figure 9.** Abstracts mentioning terms[1] related to a selection of organisational settings (%), 2003-2025

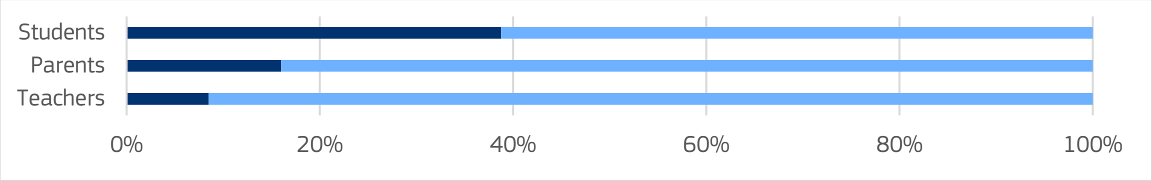


[1] Note: The searches made use of wildcard characters (*) to allow for the inclusion of multiple variations of a word, such as singular and plural: school*, universit*, college*, workplace*.

*Source: JRC own elaboration, based on data merged from the Scopus and Web of Science databases.*

Students are also mentioned in almost 40% of abstracts, which suggest that this is a key population for the study of cyberbullying. While parents and teachers can also play a central role in this phenomenon, they are only present in the abstracts of articles to a considerably much more limited extent, being mentioned in less than 16% and 9% respectively (Figure 10).

**Figure 10.** Abstracts mentioning key stakeholder groups[1] (%), 2003-2025

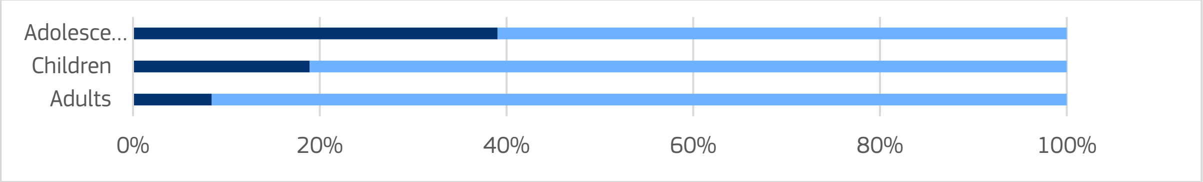


[1] Note: The searches made use of wildcard characters (*) to allow for the inclusion of multiple variations of a word, such as singular and plural: student*, parent*, teacher*

*Source: JRC own elaboration, based on data merged from the Scopus and Web of Science databases.*

Figure 11 shows the frequency of terms related to younger populations as compared to adults, suggesting that the scientific literature is particularly concerned with the study of cyberbullying in relation to minors.

**Figure 11.** Abstracts mentioning age groups[1] (%), 2003-2025

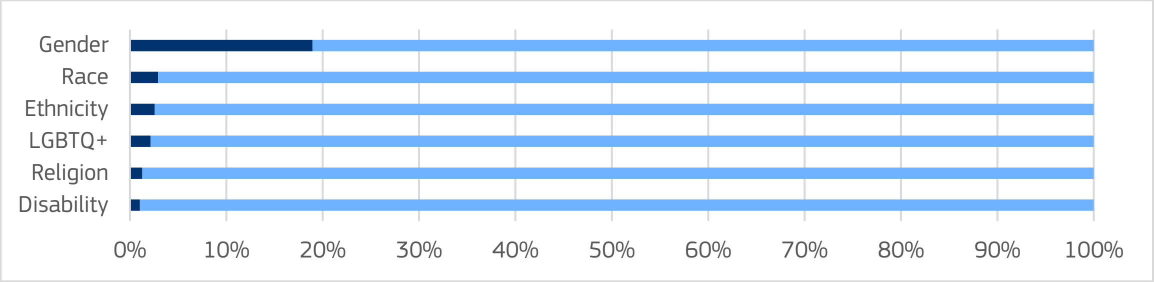


[1] Note: The searches made use of wildcard characters (*) to allow for the inclusion of multiple variations of a word, such as singular and plural: adolescen*, child*, adult*

*Source: JRC own elaboration, based on data merged from the Scopus and Web of Science databases.*

As shown in Figure 12, about 20% of abstracts are concerned with the gender dimension, whereas only a very small fraction make reference to particularly vulnerable populations, including characteristics such as race (2.9%), ethnicity (2.6%), sexual orientation or identity (2.1%), religion (1.3%) and disability (1%).

**Figure 12.** Abstracts concerned with gender and vulnerable populations[1] (%), 2003-2025



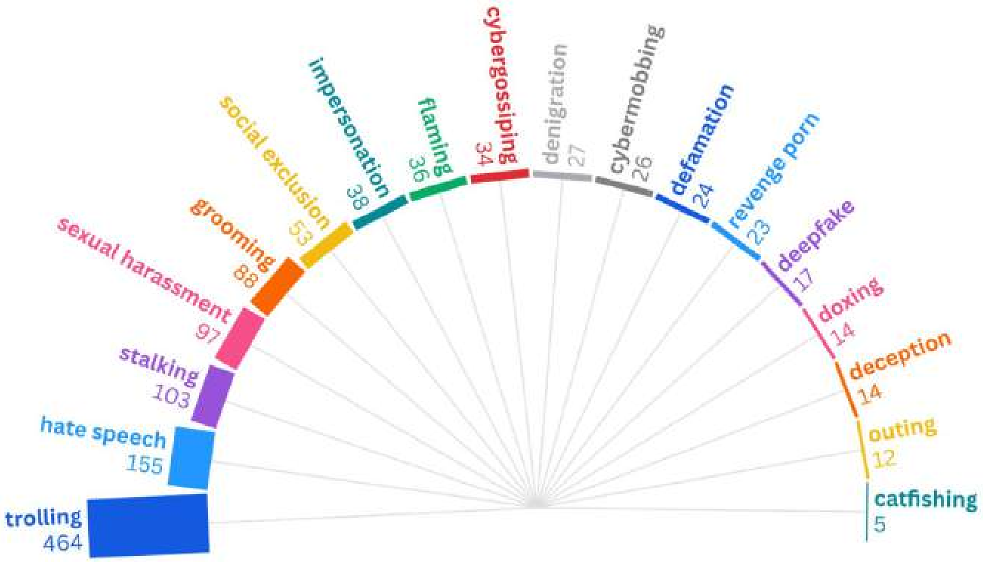
[1] Note: Some searches made use of wildcard characters (*) to allow for the inclusion of multiple variations of a word: gender, raci*, ethnic*, relig*, disab*

*Source: JRC own elaboration, based on data merged from the Scopus and Web of Science databases.*

As already noted in Chapter 3, there is a wide and rapidly expanding range of practices and types of behaviour that can be regarded as instances of cyberbullying. Figure 13 contains a selection of relevant terms that are mentioned in five or more abstracts. Building up on the analysis conducted for the policy brief preceding this work (Cachia et al., 2025), we have incorporated data from Web of Science in our analysis, to data from Scopus, to provide a more comprehensive understanding of the quantity of scholarly articles addressing specific forms of online harassment that tends to be related to cyberbullying.

Social media and online games have emerged as central environments for the proliferation of cyberbullying, with 1,350 abstracts mentioning the former and 230 the latter. Research on this phenomenon has paid particular attention to specific digital platforms such as Facebook, Twitter or Instagram, as shown in Figure 14.

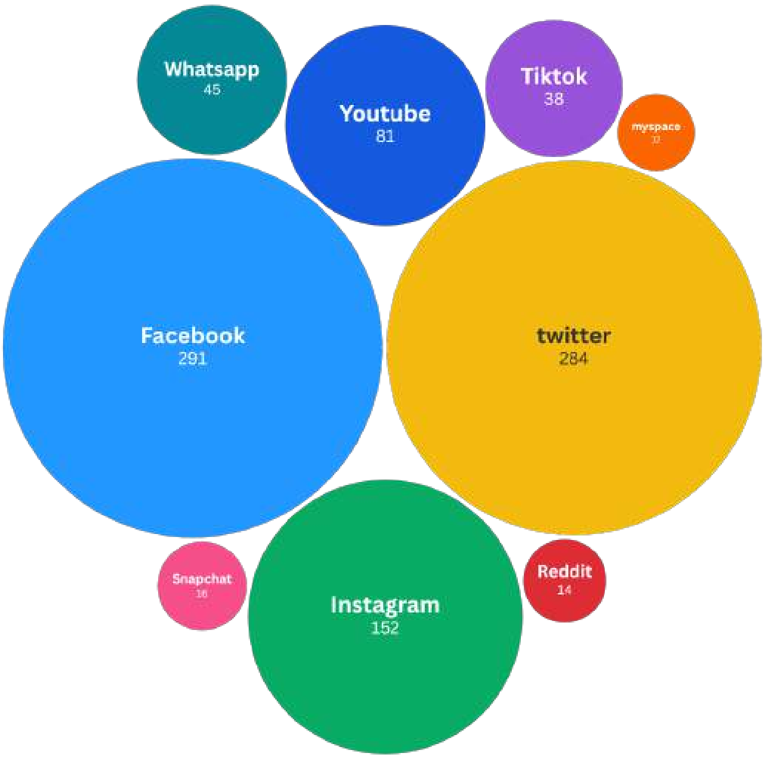
**Figure 13.** Number of journal articles by specific forms of online harassment[1] that could be related to cyberbullying, 2003-2025



[1] Note: Words mentioned in the abstracts. Some searches made use of wildcard characters (*) to allow for the inclusion of multiple variations of a word: troll*, hate* speech, *stalking, sexual harassment, *grooming, social exclusion, impersonation, flaming, *gossip*, denigration, *mobbing, defamation, revenge porn, deepfake, doxing, deception, outing, catfishing

*Source: JRC own elaboration, based on data merged from the Scopus and Web of Science databases.*

**Figure 14.** Number of journal articles on cyberbullying by specific online platforms mentioned in their abstracts



*Source: JRC own elaboration based on data merged from the Scopus and Web of Science databases.*

## 5. Exploring systematic literature reviews on cyberbullying through a rapid scoping review

To identify systematic literature reviews addressing cyberbullying published in scientific journals, we queried the Web of Science database with a search strategy specifically designed to retrieve articles that mention the words “cyberbullying” in their title and “systematic review’ in either their title or abstract,[13] while excluding other types of publications (e.g., conference papers). After limiting the search to only those systematic reviews published between 2020 and September 2025, we obtained a dataset with 64 articles.

After screening them, we excluded 12 in accordance with the inclusion criteria we applied (Table 6).

**Table 6**. Set of criteria for the selection of documents to be reviewed

| Criterium number | Inclusion criteria |
|---|---|
| 1 | Published after 2019 |
| 2 | Reviews of scientific literature on cyberbullying |
| 3 | Following a systematic review approach |
| 4 | Global geographic scope or focused on EU countries |
| 5 | Articles published in scientific journals |
| 6 | Written in English |

*Source: JRC own elaboration.*

The systematic reviews incorporated in our scoping review address cyberbullying as a complex and multifaceted phenomenon that manifests in diverse forms, impacts a wide range of populations, occurs across various digital environments, and has far-reaching global consequences. By synthetising key topics, findings and policy implications offered by these reviews, we aim to provide a comprehensive understanding of cyberbullying's prevalence, predictors — including both risk and protective factors —, consequences, and the effectiveness of interventions aimed at mitigating its impact.

Almost all the systematic reviews included in our analysis follow the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. They were primarily based on peer-reviewed journal articles indexed in well-established databases of scientific literature, although a few also included additional publications identified by other means (e.g., from cited references or relevant journals not indexed in the selected databases) or made use of less restrictive sources of academic literature (e.g., Google Scholar) in order to widen the scope. The most frequently used databases were Web of Science, Scopus and Pubmed.

Most of the reviews focused on quantitative studies, with some also offering a meta-analysis to look at combined effect sizes (Doty et al., 2022; Henares-Montiel et al., 2022; Huang et al., 2024;

[13] The exact query submitted to Web of Science was: TI=("cyberbullying") AND (TI=("systematic review") OR AB=("systematic review"))

Lan et al., 2022). Only very few reviews were specifically devoted to qualitative studies (Dennehy et al., 2020; Pardo-González et al., 2022; Teng et al., 2024).

Overall, the timespans of the systematic reviews varied, but many tended to cover medium to long periods to capture more comprehensive data and trends in the literature. Several reviews covered extensive periods, sometimes spanning two decades or even more (e.g., Dennehy et al., 2020; Lo Cricchio et al., 2021; Martínez-Monteagudo et al., 2023; Mills et al., 2024). Some covered medium-length periods, typically ranging from 5 to 10 years (e.g., Camerini et al., 2020; D. Zhang et al., 2025). A few focused on shorter periods, prioritising the most recent literature (e.g., Huang et al., 2024).

Whereas the reviews tended to focus on research published in English, some also included works in other languages, mainly Spanish (e.g., Anichitoae et al., 2025; Díaz-Esterri et al., 2025; Rusillo-Magdaleno et al., 2024) and Chinese (e.g., Huang et al., 2024; Li et al., 2024). Most reviews were authored by researchers based in the following countries: Spain, China, the United Kingdom and the United States. Apart from Spain, the other EU Member States where selected reviews were produced are Italy, Ireland, Germany, Romania, Portugal, Netherlands, Belgium, Sweden, Estonia and Lithuania.

## 5.1. Scope of the reviews

The selected reviews drew from foundational definitions of both bullying and cyberbullying, indicating a consensus on core elements such as repetition, intentionality and power imbalance. The most widely cited definitions of cyberbullying among the selected reviews are those proposed by Smith et. al (2008), Tokunaga (2010), and Hinduja and Patchin (2009).

With regard to the implications of digital technologies for bullying and the specificities of cyberbullying, the selected reviews highlighted how spatial and temporal boundaries are redefined. This not only means that victims may experience aggressions anywhere, anytime and for longer periods of time, but also that a wider population can potentially be involved or affected, as harmful content can be shared, forwarded and viewed by many people. This also entails that even in the case of isolated incidents, they can persist over time due to the fact that digital content can be continuously accessed, shared, and remain online indefinitely.

The reviews identified anonymity as a crucial aspect of cyberbullying, noting that digital platforms may enable perpetrators to conceal their identities, thereby heightening feelings of vulnerability and helplessness among victims. This dynamic significantly impacts the power imbalances traditionally associated with bullying, as anonymity can also empower victims of bullying or cyberbullying to retaliate and potentially become perpetrators themselves. Additionally, digital technologies further reshape power dynamics since digital skills and access to technology influence who can engage in cyberbullying. These differences highlight the unique challenges of addressing cyberbullying, as it extends the dynamics of traditional bullying into the digital realm, introducing new complexities in terms of prevention and intervention strategies.

The search strategies and queries employed in the systematic reviews encompassed a wide array of terms and keywords, including jargon and lingo related to aggressive behaviour, digital technology, and technology-mediated aggression (Table 7).

**Table 7.** Examples of terms[14] included in the search strategies of the systematic reviews

| Aggressive behaviour | Digital technology | Technology-enabled violence |
|---|---|---|
| Abuse | Blog | Doxing |
| Aggression | Chat | Cyber-aggression |
| Bullying | Cyber | Cyber-gossip |
| Delinquency | Discord | Cyber-harassment |
| Denigration | Electronic | Cyber-hate |
| Deviant | Facebook | Cyber stalking |
| Harassment | Gaming | Cyber-bullying |
| Hate | Internet | Cyber-victimization |
| Intimidation | LinkedIn | Digital harassment |
| Mobbing | Machine learning | Electronic harassment |
| Ragging | Massively Multiplayer Online Role-playing Games | Flaming |
| Toxic | Massively Multiplayer Online Games | Internet bully |
| Victim | Media | Internet harassment |
| Victimization | Mobile | Online aggression |
| | Multiplayer Online Battle Arenas | Online bully |
| | Online | Online harassment |
| | Pinterest | Online victimization |
| | Reddit | Online violence |
| | Snapchat | Revenge porn |
| | Social media | Video lynching |
| | Social network | |
| | TikTok | |
| | Twitter | |
| | Tumblr | |
| | Youtube | |

*Source: JRC own elaboration.*

[14] Most queries made use of asterisks as a wildcard character to represents any number of characters, allowing for the inclusion of multiple variations of a word or root word. For instance, "bully*" would capture "bully," "bullies," "bullying," etc. This technique is often used in database searches to broaden the search to include all possible word forms and derivations.

### 5.1.1. Focus

Most of the systematic reviews we examined offered insights into those factors that may either increase or minimise the risk of being affected by cyberbullying behaviours, mainly with regard to the likelihood of being victimised or, in some cases, of becoming an aggressor. Eleven reviews focused specifically on studies looking at programmes and strategies aimed at tackling cyberbullying, such as educational and family interventions or technical approaches for the detection of cyberbullying (e.g., Doty et al., 2022; Nee et al., 2023; Tozzo et al., 2022). A smaller set of reviews were specifically concerned with methodological aspects (e.g., Chun et al., 2020; W. Zhang et al., 2022) or perceptions and conceptualizations of this phenomenon from the perspective of key stakeholders (Dennehy et al., 2020; Pardo-González et al., 2022; Tang et al., 2023).

Eleven reviews conducted a meta-analysis of quantitative studies (e.g., Huang et al., 2024; Mills et al., 2024; Polanin et al., 2022) and three focused exclusively on reviewing longitudinal studies (Camerini et al., 2020; Morales-Arjona et al., 2024; D. Zhang et al., 2025). Additionally, Kasturiratna et al. (2025) conducted an umbrella review of meta-analyses, which is a type of systematic review that compiles data from multiple meta-analyses to provide a broad synthesis of evidence, allowing for the identification of patterns, strengths and gaps in the literature.

### 5.1.2. Types of cyberbullying

While most systematic reviews treated cyberbullying as a general form of online violence, a few focused specifically on particular forms of aggression. For instance, Bussu et al. (2025) distinguished between 'cyberbullying' and 'cyberstalking,' defining the latter as a form of online harassment often linked to ex-partners and romantic relationships, which tends to involve persistent and unwanted electronic communication intended to harass or intimidate victims or monitoring victims' behaviour.

Fulantelli et al. (2022) reviewed 24 articles on ‘cyberbullying’ and ‘cyberhate’ to investigate whether, and to what extent, the connection between these two phenomena is explicitly made, and if overlapping factors can be identified in their descriptions. The findings reveal that adolescent spreading of hateful material by means of digital media is less explored than cyberbullying, with most studies focusing on one of these phenomena not addressing the other. Nonetheless, upon comparing the predictors and outcomes of both, overlaps become apparent. These include the influence of the parent-child relationship in minimising cyber-aggression risk; the association between sexuality and cyber-attacks; the protective role of families and strong friendships; the impact of both cyberbullying and cyberhate on adolescents' well-being and emotions; and significant similarities in the coping mechanisms used by victims of both cyberbullying and cyberhate.

While some manifestations of cyberbullying involve direct threats or aggressions, others consist of hostile practices that aim to harm victims in a different way. Two reviews looked specifically at studies on cyberbullying and social exclusion, where victims are isolated from a group. Ademiluyi et al. (2022) examined 34 research articles on how social media contributes to ostracism as a form of cyberbullying. They identified several recurring causes of cyberbullying perpetration and victimisation, including social pressures (peer grouping, social success), web-based behaviour (security awareness, social tendencies), self-concept (identity development, social status, educational status), public perception (perceived appearance, nonverbal interactions), and familial issues (marital status, home environment, parental relationships).

Mills et al. (2024) examined 29 studies that employ electroencephalography (EEG) to investigate the impact of cyberbullying-related social exclusion on brain activity. The findings showed associations between cyberbullying, social exclusion and irregularities in EEG measures, especially in children and adolescents. However, the authors highlighted limitations in the literature, noting that many studies had small sample sizes and lacked long-term insights into the effects of repeated ostracism on brain function.

### 5.1.3. Socio-technical environments

While cyberbullying may take place through diverse information and communication technologies (e.g., email, SMS), social media emerged as a prominent space for online aggressions, with systematic reviews including studies on platforms such as Twitter, Instagram, Facebook or Myspace (e.g., Nee et al., 2023; Salawu et al., 2020; Shahzad et al., 2024).

More specifically, one of the reviews (Hu et al., 2025) focused on the relevance, characteristics and predictors of cyberbullying behaviour in multiplayer online games, concluding that it is associated with gaming frequency, with men more likely to be both victims and perpetrators, while women face disproportionate levels of sexual harassment in these online environments. Factors such as competition, anonymity, and normalisation contribute to these behaviours. Despite concerns regarding violent video game content, its ability to predict cyberbullying is uncertain. The findings of this review indicate that behaviour is sustained by in-group and out-group dynamics, where veteran players target newcomers, especially those perceived as feminine, causing some to quit gaming while others accept and continue the cycle. Common coping mechanisms include blocking offenders or quitting the game, with women often hiding their gender.

### 5.1.4. Studied populations

The systematic reviews on cyberbullying cover a wide range of age groups, with some examining its impact on the general population (e.g., Huang et al., 2024; D. Zhang et al., 2025) but most concentrating on specific segments. As noted in the umbrella review conducted by Kasturiratna et al. (2025), children, adolescents, and adults may encounter and perceive cyberbullying in fundamentally distinct ways due to differences in their cognitive and social development. For instance, younger children may not possess the emotional maturity required to accurately recognise incidents of cyberbullying. In contrast, adolescents, as they become more socially integrated, may both experience cyberbullying more frequently and be better equipped to identify it. Adults, however, might interpret such interactions differently because of their life experiences and maturity, which can affect how they respond to potential cyberbullying situations.

Overall, within the reviews on the implications of cyberbullying for the general population, only a small fraction of reviewed studies looked specifically at middle- and old-age populations (Huang et al., 2024). Conversely, the literature has paid considerable attention to cyberbullying among students across different educational levels, including compulsory (Chicote-Beato et al., 2024; Evangelio et al., 2022; Rusillo-Magdaleno et al., 2024) and post-compulsory education (Bussu et al., 2025; Shaikh et al., 2020).

In particular, reviews often focus on participants aged 10 to 18 (e.g., Buelga et al., 2022; Henares-Montiel et al., 2022; Lozano-Blasco et al., 2020; Mubashir et al., 2022; Ng et al., 2022). In contrast, only in exceptional cases did some reviews include studies with younger children. For example, out of the 57 studies reviewed by Lin et al. (2024) on the connection between childhood maltreatment and cyberbullying, only two included participants coded as children, with a mean age range of 5 to

12 years. Similarly, in the 32 studies reviewed by Real Fernández (2022) on executive functions in children and adolescents, only two included participants under 10. Only one systematic review, conducted by Chicote-Beato et al. (2024), focused specifically on programs aimed at tackling and preventing cyberbullying in primary education for children aged 6 to 12.

Besides those reviews looking at cyberbullying in Higher Education, which by definition are specifically concerned with young adults, others with a wider scope also examined studies with samples including young adults of up to 20 (Biagioni et al., 2023; Estévez et al., 2020), 24 (Doty et al., 2022; Fulantelli et al., 2022) or even 29 (Morales-Arjona et al., 2024).

Few reviews focused on studies dedicated to more specific populations within educational contexts, namely to cyberbullying among gifted students (Martínez-Monteagudo et al., 2023) and minors with intellectual and developmental disabilities (Martínez-Cao et al., 2021). No systematic reviews focused specifically on other particularly vulnerable populations based on other characteristics such as gender, sexual orientation, race, ethnicity or religion.

Studies addressing cyberbullying behaviour outside education have examined cyberbullying experiences in the workplace, customer cyberbullying or cyberbullying in online labour markets (Huang et al., 2024; Tang et al., 2023).

### 5.1.5. Roles: types of involvement

Whereas most reviews covered research on cyberbullying in relation to different kinds of actors simultaneously, some of the systematic reviews were specifically dedicated to examining studies on distinct forms of individuals' involvement in cyberbullying, namely as perpetrators, victims or bystanders.

Basal et al. (2023) conducted a qualitative systematic review and bibliometric analysis to gain insight into the perspectives of cyberbullying perpetrators, highlighting the association between this behaviour and important societal challenges such as mental health issues and moral disagreement. The review by Zheng et. al (2025) focused more specifically on the associations between family variables (e.g., parenting style, family conflict, parent-child attachment) and engagement in cyberbullying perpetration.

Likewise, some reviews have analysed the exchange between victim and perpetrator roles. Estevez et al. (2020) reported heterogenous findings, but noted consensus on the continuity or overlap in the roles involved in both traditional bullying and cyberbullying. Some of the studies they reviewed noted patterns of role-switching where victims choose to confront their aggressors online, thus becoming cyber-aggressors themselves. After conducting a meta-analysis, Lozano-Blasco (2020) noted that longitudinal studies have revealed a connection between initially reporting being a cybervictim and later becoming a cyberbully in subsequent survey waves.

Few reviews were specifically devoted to other types of actors involved, whether directly or indirectly, in cyberbullying. Lo Cricchio et al. (2021) examined research on the role of moral disengagement in both cyberbullying perpetration and passive bystanders, while Rudnicki et al. (2023) looked at studies on the role of bystander in online hate and cyberbullying incidents among adults. Zheng et al. (2025) looked at research exploring the connection between family factors and adolescent cyberbullying perpetration. Out of 48 reviewed studies, family variables were categorised into contextual and practical types, based on their influence on adolescent cyberbullying and aiming to provide a comprehensive framework for understanding family effects on adolescent cyberbullying.

## 5.2. Key findings

The systematic reviews of literature on cyberbullying provide valuable insights into its effects and identify diverse factors that may either increase or decrease the likelihood of this harmful behaviour. A subset of these reviews specifically focuses on evaluating programs and interventions designed to combat or prevent cyberbullying. The findings from these systematic reviews are essential for informing future actions, and many of them offer policy recommendations that can be drawn upon to guide effective strategies.

### 5.2.1. Key elements from definitions

All the systematic reviews included in our analysis are based on some form of definition of cyberbullying and while there is no universally accepted definition of the concept there are certain elements that recur frequently. A handful of authors are often cited across the systematic literature reviews on cyberbullying when defining the concept, most notably Smith (Slonje et al., 2008; Smith et al., 2008), Hinduja and Patchin (2008), Tokunaga (2010) and Kowalski (2014, 2007).

Based on the definitions utilised in systematic literature reviews, the following key elements can be consistently identified:

1. **Aggression**: the aggressive or hostile nature of the behaviour
2. **Technology**: the behaviour is mediated by electronic digital media and enabled by affordances that differentiate cyberbullying from traditional bullying:
   a) Interactions may be perceived as anonymous
   b) Larger networks of people might be affected by the phenomenon
   c) Exposure to harm can happen anytime and anywhere
3. **Repetition**: harm is experienced by victims repeatedly and over long periods
4. **Intentionality**: harm results from the actions of perpetrators driven by the intention to cause suffering in targeted victims
5. **Power Imbalance**: aggressors rely on the inability of victims to defend themselves due to individual attributes and social factors that may differ from those typical of traditional bullying (e.g., physical strengths).

Several systematic reviews focus specifically on analysing how cyberbullying is defined and measured. An analysis by Chun et al. (2020)of 64 international studies on cyberbullying found that nearly 72% of them offered their own definitions, with many indeed acknowledging the lack of a common definition as a significant limitation to research on this topic. However, many studies included in that review addressed cyberbullying as “a repeated and intentional act to threaten/harass/embarrass others through electronic means or devices.” (Chun et al., 2020, p. 3)

After reviewing 25 studies that made use of cyberbullying measurement scales in relation to children and adolescents, Zhang et al. defined cyberbullying as:

> *“behaviors expressed by an individual or group through Information and Communication Technologies (ICT), such as social media and e-mail, that repeatedly convey hostile or offensive information with the intention of causing harm or discomfort to others” (2022, p. 2).*

Similarly, a review of 71 studies by Ray et al. (2024) revealed 22 different definitions of cyberbullying, highlighting the inconsistencies and the need for a standardised conceptual framework, which led them to propose their own definition:

> *"The use of technology to manipulate and exploit targeted vulnerable victims using online aggression or harassment and repeated threats, to embarrass or humiliate by posting harmful content, with the purpose or intent to cause psychological or emotional harm, in some cases, leading to physical harm." (Ray et al., 2024, p. 6)*

### 5.2.2. Effects of cyberbullying

Cyberbullying victimisation has been consistently associated with maladaptive coping behaviours and increased internalising symptoms, including negative psychological outcomes such as depression and anxiety (Anichitoae et al., 2025; Kasturiratna et al., 2025; Morales-Arjona et al., 2024). Some studies have suggested that victims are more likely to experience decreased self-esteem and confidence (Agustiningsih et al., 2024).

The consequences of cyberbullying can be severe and long-lasting, with some individuals even engaging in self-injury (Predescu et al., 2024) and suicidal ideation (Buelga et al., 2022; Dorol-Beauroy-Eustache et al., 2021; Morales-Arjona et al., 2024). There seems to be a two-way connection between cyberbullying and depression, where cyberbullying can lead to increased depression and, conversely, depression can increase the likelihood of being involved in cyberbullying (D. Zhang et al., 2025).

The effects of cyberbullying can also have a negative impact on academic performance, student wellbeing and the school environment (Chicote-Beato et al., 2024; Dorol-Beauroy-Eustache et al., 2021; Martínez-Monteagudo et al., 2023). This can have long-term consequences for students' educational and career trajectories, as well as their overall wellbeing and life satisfaction.

In addition to the individual-level effects, cyberbullying can also have broader societal implications. The prevalence of cyberbullying can contribute to a culture of fear and intimidation, where individuals feel reluctant to express themselves online or participate in online communities. Moreover, cyberbullying can perpetuate existing social inequalities, with certain groups, such as minorities and individuals with disabilities or health conditions, being disproportionately targeted and affected (Martínez-Monteagudo et al., 2023; Zhu et al., 2021).

### 5.2.3. Risk Factors and Protective Factors

Systematic literature reviews have identified a wide array of factors that may serve as predictors of cyberbullying, encompassing demographic, psychological, behavioural, cultural, socio-technical and contextual or environmental aspects.

#### *5.2.3.1. Age*

Age is an important predictor of both cyberbullying victimisation and perpetration. In this regard, the umbrella review conducted by Kasturiratna et al. (2025) revealed that school-aged populations are more likely to be cyberbullied. They also pinpointed a nonlinear relationship between age and cyberbullying victimisation. Victimisation rates tend to increase as children and adolescents grow older, due to their heightened use of computers, engagement with social media, and greater exposure to digital devices. However, these rates level off in adulthood. This flattening could be attributed to a general decline in aggressive behaviours with age. These findings indicate that while younger individuals are more vulnerable to cyberbullying, older adults may be less affected, highlighting the need for a nuanced interpretation of age-related trends in cyberbullying.

Zhu et al. (2021) point out that senior students tend to be more impulsive and less empathetic, with those over 15 years old at a higher risk of becoming cyberbullying perpetrators. According to the review by Real Fernández et al. (2022), deficits in executive functions, such as inhibition and self-control, are associated with involvement in cyberbullying. Adolescents engage in more complex social interactions than children, thus increasing their risk as either victims or aggressors. On the other hand, Camerini et al. (2020) reported inconsistent findings regarding age, with some studies indicating that older students are at significantly higher risk of non-public cyberbullying perpetration and cyberbullying victimisation, while others concluded that younger students are at higher risk of cyberbullying victimisation.

#### *5.2.3.2. Gender and sex*

Systematic reviews often identify gender or sex as an important factor for cyberbullying. However, further research is needed to address some inconsistencies in findings. The meta-analyses by Kasturiratna et al. (2025) consistently show that females are at a slightly higher risk of experiencing cyberbullying victimisation compared to males. The increased risk is partly due to their greater involvement in indirect forms of aggression and more frequent use of social networking sites. Additionally, based on the reviewed literature, they noted that females tend to share more personal information online, which may heighten their vulnerability to cyberbullying, and that they also tend to interpret online comments as hurtful more quickly than males, which could also explain higher reported levels of victimisation. The review by Camerini et al. (2020) indicated that males and females are at equal risk of cyberbullying victimisation, with males more likely than females to become cyberbullies.

In their review of longitudinal studies on cyberbullying and suicidal behaviour, self-harm, and non-suicidal self-injury, Morales-Arjona et al. (2024) reported on five studies exploring the impact of gender on the connection between cyberbullying and suicidal ideation, with two showing significant gender-related findings. One of them revealed that female cyberbullying victims faced a higher risk of depression, which subsequently elevated their likelihood of experiencing suicidal ideation, while the other one found that the rate of suicidal ideation was three times higher in females compared to males. Additionally, Díaz-Esterri et al. (2025) found articles revealing a higher prevalence of ‘cybergossip’ among adolescent girls, as compared to boys, and higher likelihood of developing pathologies such as depression or anxiety.

In the context of education, regardless of gender, children generally report similar effects from cyberbullying victimisation, such as depression symptoms, anger, and frustration. However, the emotional and academic impacts are more significant in girls, who tend to experience poorer academic performance, higher levels of school absenteeism, and lower rates of class participation (Martínez-Monteagudo et al., 2023).

Biagoni et al. (2023) reviewed several studies indicating that gender operates as a moderator factor of the associations between cyber-victimisation and the use of legal and illegal psychoactive substances. Those studies found significant links, among female students only, between being a victim of cyberbullying and consumption of alcohol, cigarettes, non-medical drugs, as well as binge drinking. When discussing possible explanations for this, based on the literature, they noted that girls who experience cyber-victimisations may face greater relational and reputational victimisation compared to boys, which may lead to long-term distress and substance consumption. Additionally, they noted that being female and engaging in maladaptive behaviours, like using psychoactive substances, could predict cyber-victimisation. However, not all studies reviewed by Biagoni et al. found gender interactions, leaving the relationship between substance use and cyberbullying uncertain, as there are other important factors at play, like parent-child relationships or peer influence.

In online gaming environments, Hu et al. (2025) found that men are more likely to be both victims and perpetrators of cyberbullying, while women face disproportionate levels of sexual harassment. Women often cope by concealing their gender and blocking perpetrators, indicating gender-specific experiences and responses in gaming contexts.

#### *5.2.3.3. Minority groups*

Five meta-analyses included in the umbrella review by Kasturiratna et al. (2025) assessed the impact of minority status on cyberbullying, with four of them indicating that individuals who belong to racial, ethnic or sexual minorities faced a higher likelihood of becoming cyberbullying victims compared to majority groups, such as Caucasians and heterosexuals. Sexual orientation and gender identity are important predictors of cyberbullying victimisation and exposure to online hate material (Fulantelli et al., 2022). Moreover, the studies reviewed by Dorol-Beauroy-Eustache et al. (2021) indicate that adolescents who are cyber-harassed on the basis of sexuality, racial or ethnic background are more likely to both report suicidal ideation and attempt suicide than those harassed for other reasons.

#### *5.2.3.4. Psychological aspects*

Psychological and behavioural risk factors play a prominent role in cyberbullying dynamics. Reviews by Anichitoae et al. (2025) and Morales-Arjona et al. (2024) emphasise the role of low self-esteem, impulsiveness, and prior victimisation experiences in cyberbullying victimisation. As already noted, internalising symptoms, including depression and anxiety, are identified as mediators in the relationship between cyberbullying involvement and adverse outcomes, such as non-suicidal self-injury and suicidal ideation (Morales-Arjona et al., 2024; Predescu et al., 2024).

According to the review by Agustiningsih et al. (2024), low self-esteem and victimisation mutually reinforce each other. They noted that peers may avoid adolescents with low self-esteem, leading to bullying, while low self-esteem is often accompanied by anxiety, depression, and suicidal thoughts, making it difficult for individuals to find a comfortable social group and increasing the risk of being bullied. Since bullying involves an imbalance of power, low self-worth can be a precondition for its occurrence. Additionally, lack of peer approval can contribute to feelings of worthlessness. Poor self-esteem, unlike average or high self-esteem, might also contribute to the development of bullying perpetration.

On the other hand, the review by Quintana-Orts et al. (2021) revealed that forgiveness and bullying behaviours — including cyberbullying — have an inverse relationship, as adolescents who exhibit greater levels of forgiveness are less likely to engage in bullying. Likewise, forgiveness is inversely related to victimisation, as those with higher forgiveness tend to experience less victimisation. Conversely, a lack of forgiveness is positively associated with both traditional and online bullying.

Other personal traits, such as empathy and emotional intelligence, have been highlighted as protective factors due to their role in enhancing social interactions and conflict management, which in turn can contribute to reducing involvement in cyberbullying (Zhu et al., 2021).

#### *5.2.3.5. Other individual characteristics*

Dorol-Beauroy-Eustache (2021) identified other characteristics that may increase the likelihood of being targeted by cyberbullies, including Autism Spectrum Disorder, Intellectual and Developmental Disorders, obesity or asthma. Very few systematic reviews have specifically addressed subgroups of individuals who might be particularly vulnerable due to special characteristics.

Martínez-Cao (2021) conducted a review of 37 studies on bullying and cyberbullying among young people under 18 with intellectual and developmental disabilities (IDD), aiming to identify risk and protective factors, the impact on victims, and effective responses to these incidents. The review concluded that promoting safer, more inclusive environments and strengthening support networks through evidence-based prevention and intervention protocols can significantly reduce the prevalence and impact of bullying and cyberbullying in this vulnerable population.

Martínez-Monteagudo (2023) examined 15 studies on school bullying and cyberbullying among academically gifted students. The review highlighted a high prevalence of these issues within samples consisting exclusively of gifted students. Although there is insufficient evidence to definitively confirm a greater vulnerability to bullying among academically gifted students, the review emphasises the need for the educational community to implement preventive measures and specific interventions for this group.

#### *5.2.3.6. Relational dynamics*

Perceived social support is an important protective factor against the negative effects of cyberbullying victimisation. The presence of strong support networks, including family, peers, and school connections, reduces the likelihood of victimisation and buffers against negative psychological outcomes.

According to the systematic review on perceived social support and cyberbullying in adolescents conducted by Castaño-Pulgarín et al. (2022), studies have focused primarily on the role of family and friends or peers. Likewise, they note that cyberbullying is more difficult to detect and that opportunities for victims to access social support is often more limited than in traditional bullying, as a result of perpetrators being able to operate both anonymously and beyond school boundaries.

Reviews by Bussu et al. (2025) and Dorol-Beauroy-Eustache and Mishara (2021) reported that active parental engagement, including supervision of online activities and fostering open communication, can help adolescents navigate digital environments more safely, reducing the risk of both perpetration and victimisation.

Kasturiratna et al. (2025) highlighted that parental support is consistently recognised in the literature as a protective factor against cyberbullying victimisation, though its impact is generally small. Nine meta-analyses revealed a modest positive correlation between strong family ties and a decreased likelihood of cyberbullying victimisation. Children and adolescents with engaged parents who monitor their internet use and stay informed about their online activities are less prone to victimisation. Nonetheless, the protective effect is limited, as children’s online activities frequently occur beyond parental oversight, particularly in environments like schools.

Beyond supervision of technology use, other family dynamics may help mitigate cyberbullying risks. For example, the review by Dorol-Beauroy-Eustache et al. (2021) found evidence in the literature that family dinners are associated with less risk of suicidal and self-harm behaviours resulting from cyberbullying victimisation, while Díaz-Esterri (2025) highlighted that engaging in shared leisure activities with family members can be an effective way to decrease the risk of young people being victimised.

The meta-analysis by Lozano-Blasco et al. (2020) concluded that girls with unstable family environments were more likely to be victims of cyberbullying. Problematic Internet use in this population, which increases the risk of becoming victims of cyberbullying, was reinforced by parenting styles characterised by either a permissive approach or total lack of clear rules (i.e., laissez-faire), as well as poor communication within families. Based on a meta-regression analysis, they also found that, at a macrosystem level, differences across cultures — in terms of norms, social responses, and protection issues — play a role in promoting or inhibiting cyberbullying perpetration. In particular, their findings indicate that developing a dual role as cybervictim and cyberbully is more likely to affect adolescents within Central European culture, Mediterranean culture, Asian culture, North American culture and South America Culture.

One of the systematic reviews was specifically devoted to exploring the connection between family variables and adolescent cyberbullying perpetration (Zheng et al., 2025). It categorised family factors into contextual (e.g., parenting style, family conflict) and practical (e.g., parental mediation, family communication) variables, emphasising the importance of family dynamics in shaping adolescents' behaviour. According to this review, the prevalence of cyberbullying tends to be higher when parents, typically using a controlling style, reduce their control or are inconsistent in mediating internet use. Long-term exposure to family conflict increases negative emotional arousal and feelings of insecurity in children, leading to weaker attachment to their parents. As a result, adolescents may choose coping strategies that do not align with their moral values, such as cyberbullying, highlighting the significant role of moral disinhibition.

Based on three meta-analyses, the umbrella review by Kasturiratna et al. (2025) also suggests that non-supportive romantic relationships may increase — though only to a small extent — the risk of cyberbullying victimisation. Additionally, having a younger partner may also be linked to a higher risk of cyberbullying victimisation, possibly because younger couples are more active online.

#### *5.2.3.7. Behavioural aspects*

Certain behaviours and activities have been associated with cyberbullying victimisation and perpetration, whether increasing or minimising risks.

Based on the results of seven meta-analyses, Kasturiratna et al. (2025) identified a small but significant link between increased digital media and Internet use and higher cyberbullying victimisation. In particular, frequent internet users are more likely to become victims of cyberbullying if they engage in risky online behaviours, such as sharing personal details or photos, and visiting unverified websites.

The review by Díaz Esterri et al. (2025) suggested a connection between digital leisure activities and cyberbullying, although with low levels of certainty due to the observational nature of reviewed studies. It pointed to a dual nature of leisure activities and spaces regarding bullying and cyberbullying, where the same activity can be either a risk factor or a protective factor, depending on the context. The majority of studies included in this review found a link between digital leisure activities, cyberbullying, and being a victim of cyberbullying, with this connection being more evident when digital devices were misused.

Looking at research on the interplay between physical activity and bullying as well as cyberbullying among children and adolescents, Rusillo-Magdaleno et al. (2024) concluded that cooperative activities at various times of the day (i.e., before, during and after school) can reduce victimisation, improve aggressive and disruptive behaviours, and alleviate associated psychological issues. However, factors such as the type of sport, the context, the roles assigned to students, the pedagogical approach, and the school climate can significantly influence aggressive behaviours.

The review by Biagioni et al. (2023) delved into the relationship between psychoactive substance use — both legal and illegal — and cyberbullying. Various factors, including the type and frequency of cyberbullying, the specific substance used, gender, peer pressure, and parental relationships, all play a role in shaping this relationship. However, since most studies on this topic have used a cross-sectional approach, it is challenging to pinpoint a direct cause-and-effect link between substance use and cyberbullying. As a result, the review concludes that it's currently unclear whether there's a causal relationship between the two behaviours, and it's possible that they may be linked to shared underlying factors.

#### *5.2.3.8. Cyberbullying victimisation as a precursor of perpetration*

As concluded by Kasturiratna et al. (2025), research has consistently shown that being a victim of cyberbullying can increase the likelihood of later becoming a cyberbully oneself. Unlike traditional bullying, which often relies on physical power imbalances, cyberbullying takes place online, where victims can easily turn into perpetrators due to the lack of physical constraints and the anonymity of the internet. This anonymity can lead to a blurring of lines between victims and bullies, allowing victims to seek revenge by adopting the role of bullies, thereby perpetuating a cycle of online aggression and escalating its harmful effects.

Lozano-Blasco (2020) noted that having been a victim of cyberbullying in the past is the most important risk factor for cyberbullying perpetration. Individuals who experience both cyberbullying and cybervictimisation, often referred to as cybervictims-bullies, tend to report more severe negative consequences, such as suicidal ideation, compared to those who are solely cyberbullies or cybervictims. Additionally, they found in the literature that cybervictims-bullies often exhibit lower empathy levels than pure cyberbullies.

In their review, Estévez et al. (2020) indicate that victims of traditional school bullying who are also being cyberbullied could see the online environment as an extension of the school setting that makes it possible for them to experience the harassment 24 h a day, but also as a space where they can assert dominance over others as compensation for being harassed at school. Additionally, for cyberbullies, the online environment can be a platform where they exhibit a more aggressive personality. Therefore, the authors call for further research on the co-occurrence of traditional bullying and cyberbullying, as well as on the exchange of roles and contexts between the two.

#### *5.2.3.9. Educational institutions*

Based on the results of ten meta-analyses, Kasturiratna et al. (2025) highlight that unfavourable school climates — characterised by inadequate teacher-student interactions — are consistently linked to slight increases in cyberbullying victimisation. This risk is further increased by the lack of supervision and unrestricted access to digital media and school devices, which can also facilitate traditional bullying. All those meta-analyses also suggest that engagement in traditional bullying, as victim or aggressor, is an important predictor of cyberbullying victimisation.

Several reviews point to the critical role of positive school climates in mitigating not only traditional bullying but also cyberbullying (Ng et al., 2022). Effective teacher-student engagement and supervision are emphasised as key factors in creating safe educational spaces (Dennehy et al., 2020). Furthermore, Castaño-Pulgarín et al. (2022) highlighted that fostering a culture of openness and support within schools can empower students to report incidents of cyberbullying and seek help, while noting that researchers should pay more attention to the role of schools as providers of social support against cyberbullying.

### 5.2.4. Stakeholders' perspectives

A short number of systematic reviews tackle the topic of perceptions of cyberbullying by different groups. In particular, Dennehy at al. (2020) reviewed 13 studies that conceptualise cyberbullying by young people aged 10 to 19, giving a voice to this group in the efforts to fight cyberbullying. Among the five key concepts identified by the review — intent to harm, repetition, accessibility, anonymity and barriers to disclosure—, some nuances are worth highlighting. To adolescents' view, intent is closely related to the victim's perception of the acts, as there is a dose of ambiguity on how online no malicious messages can be interpreted by the recipient and affected by internal and external factors (e.g., nature of relationship, lack of face-to-face interaction), and therefore the notion of intent also links with the impact on the victim. Repetition is considered as a sufficient but not necessary condition for cyberbullying, as "one-time actions may have repetitive effects", and sometimes perpetrators are unaware of their lasting consequences. Also, in the online environment virality can be as harmful as repetitiveness. Accessibility is linked to the ubiquitous nature of digital technologies, potentially affecting anybody, anytime, anywhere ("non-stop bullying"), and it is reported to be more experienced while at home (sometimes as a form of continuation of traditional school bullying), due to technology access and insufficient parental monitoring. Anonymity contributes to increased fear, distress and feeling of impotence, and is recognised as "a large part of the power and impact of cyber bullying". It is also perceived as equalling factor, as everybody can be bullied or become a bully. Interestingly, anonymity is also linked to barriers of disclosure, as it increases the chances that perpetrators avoid responsibility of their acts. Some factors that hinder cyberbullying reporting are related to adults: the adolescents' perception of adults' inability to deal with the cyber world; the concern that disproportionate adult intervention may intensify the perpetrator's actions and even lead to physical violence; the fear of social disconnection if access to digital devices or internet is restricted or discontinued. In conclusion, the review highlights the complex nature of cyberbullying, and how features such as anonymity, ambiguity, accessibility and public exposure play a two-way role that disempower victims and empower perpetrators.

Adolescents' perceived helplessness when it comes to adults' intervention is endorsed by Pardo-González et al. (2022) in their review of 12 qualitative studies on parents' and caregivers' opinions, where parents request guidance to help them become effective in prevention and response to cyberbullying. The review identified parents' low digital competence as the main barrier to cyberbullying prevention, and links with parents' perception of a generational gap in what concerns computer literacy. The most common parental strategy for prevention is monitoring, supervision and restriction of ICT use and content (especially for highly vulnerable groups such as persons with disabilities), combined with communication to build trust. Parent's preferred intervention measures are of protective nature (for cybervictims), sanctioning (for perpetrators) and supportive with the victim but not confronting the aggressor (for cyberwitnesses). Parents also expressed the need to better understand how their children interact in social networks for an effective parental intervention.

Parents of victims often feel disappointed about how the cases are dealt with by authorities, what fuels the desire to act in isolation. As in Denehy et al (2020), anonymity, use of technology, and avoidance of retaliation are mentioned by parents as drivers for cyber aggressors. Other risk factors for cyberbullying perpetration include normalisation of violence through internet, being a girl or an adolescent, and previous cyber victimisation. Similarly, former perpetrators are also perceived as having higher probability of becoming victims. Parents recognise the importance of cyberbullying reporting and help-seeking for both victims and witnesses, and identify as main barriers the fear of repercussions, normalisation of cyberbullying, and the thought that parental intervention is not needed.

Tang and Omar (2023) conducted a review of cyberbullying studies that have adopted a phenomenological approach, identifying eight salient topics from students' perceptions of cyberbullying, grouped into four main areas: the origin of cyberbullying, experiences of cyberbullying, its influence, and coping strategies. In what respects motives for cyberbullying: it is generally rooted in damaged or broken (romantic) relationships, spread of rumours, revenge, group affiliation, and intolerance. The review identifies specific contexts or environments in which cyberbullying is prevalent, most notably the educational context (affecting students but also counsellors, administrators and teachers) and cyberbullying in the work environment (with a especial mention to customer cyberbullying, that is, the one perpetrated by customers towards service jobs employees). A number of impacts on victims' psychological scope (feelings of anxiety, embarrassment, frustration, low self-esteem, suicidal thoughts…) and physiological scope (substance and alcohol abuse, insomnia, eating disorders, physical health problems) are reported by the review.

### 5.2.5. Reviews on interventions

Based on our rapid scoping umbrella review, 12 publications have reviewed in detail the literature on interventions for the prevention of cyberbullying. These studies can be classified into two groups of a) nine reviews focusing on educational or skill-development programs and b) three reviews focusing on technological interventions (e.g., applications for the automatic detection of cyberbullying.

In the first group of articles, three systematic reviews without meta-analyses of intervention effects are included (Chicote-Beato et al., 2024; Henares-Montiel et al., 2023; Tozzo et al., 2022); five systematic reviews with meta-analyses (Doty et al., 2022; Lang et al., 2022; Ng et al., 2022; Polanin et al., 2022; Wang & Jiang, 2023), which add the value of providing quantitative estimates of such effects; and one umbrella review of meta-analyses (Kasturiratna et al., 2025), which provides a pooled estimate of multiple meta-analyses, offering strong value as an evidence synthesis.

The second group of articles includes a review of various technology-based interventions against cyberbullying (Nee et al., 2023), and two reviews specifically focused on automatic cyberbullying detection tools (Mishra et al., 2024; Salawu et al., 2020).

#### *5.2.5.1. Educational or Skill-Development Intervention Programmes*

Existing programmes for the prevention of cyberbullying take many forms and include highly diverse components. Some examples of past programmes (covered in the articles reviewed by Ng et al., 2022) are: Media Heroes Medienhelden, Cyber Friendly Schools, Viennese Social Competence (ViSC) programme, PREDEMA, and Tabby Improved Prevention and Intervention Program.

These programmes can be classified in groups according to diverse criteria. Henares-Montiel et al. (2023) identify three categories of programmes based on the strategies followed:

1. Educational/Informational: "information or educational materials are offered in order to broaden and deepen theoretical knowledge of CB (involved agents, impact on health, etc.)."

2. Cognitive/Behavioural: “strives to impact on the way in which students perceive the phenomenon of cyberbullying and their behaviors in relation to it, generally through activities that promote empathy.”
3. Skill development: “works on developing practical skills which students can put into practice in order to generate safe settings which are free from violence.”

In turn, Lan et al. (2022) analyse the pedagogical components of several types of anti-cyberbullying interventions with adolescents and identify five programme typologies, as defined by their focus on:

1. “student peer tutoring and knowledge mobilization”;
2. “students’ knowledge mobilization and teacher adaptation”;
3. “teacher adaptation”;
4. “instruction-centered information support”;
5. “student peer tutoring and community-oriented events”.

Finally, Polanin et al. (2022) provide a classification of programme components into seven non-exclusive categories, including:

1. ‘Skill Building’, focusing on response strategies, empathy and perspective-taking, effective communication, role playing, or goal setting.
2. ‘Curricula and Prepared Materials’, such as handouts, posters, homework, or worksheets.
3. ‘Psychoeducational approached’, raising awareness of cyberbullying, cyber-safety and coping strategies.
4. ‘Media Materials’, such as interactive games or courses, video courses, online courses, and digital citizenship resources.
5. ‘Training’, including teachers and parents training, or peer training.
6. ‘School Climate or School Policy’, including reporting and disciplinary policies, conferences, screening, class-management, bonding, etc.
7. ‘Group or Individual-Targeted Responses’, such as group sessions, at-risk targeting, or individual sessions.

The numerous existing programmes vary in their combinations of these different elements, as well as across several dimensions, such as their target audience (mostly children and adolescents, but in some cases also parents or other stakeholders), their duration, and their mode of delivery (in-school or at home, in-person or blended with online formats), among others.

#### *5.2.5.2. Effectiveness of Intervention Programmes*

The reviews analysed conclude that existing intervention programmes are generally effective (Chicote-Beato et al., 2024; Henares-Montiel et al., 2023; Tozzo et al., 2022). However, it is important to note that the effect sizes reported in the reviewed meta-analyses, although statistically significant, are mostly small, both for reductions in perpetration and in victimisation. This is the case in the review by Polanin et al. (2022), which covers children and adolescents in K-12 settings (typically from ages 5–6 up to 17–18). Other meta-analyses with a more specific focus on adolescents provide similar results (Ng et al., 2022, which includes samples aged 10–18; Lan et al., 2022, which also includes studies in the same age range).

The only exception is the meta-analysis by Doty et al. (2022), which includes studies with participants up to 24 years old. While it also reports a small effect size for reductions in cybervictimisations, it finds a moderate effect size for reductions in cyberbullying perpetration. Similarly, the umbrella review of meta-analyses by Kasturiratna et al. (2025) also points to a small reduction in cybervictimisations as a result of interventions against cyberbullying (pooled effect size across 11 meta-analyses). Therefore, the small size of these effects should be taken into account when evaluating the cost-effectiveness of such interventions.

#### *5.2.5.3. Long-Term Effectiveness*

Another key aspect to consider is the long-term effectiveness of interventions. Many of the studies included in the examined reviews did not assess this dimension. For example, the meta-analysis by Lang et al. (2022) reports that, due to the small number of studies providing data on long-term effectiveness, its findings were inconclusive in this respect.

In contrast, the meta-analysis by Ng et al. (2022) suggests that cyberbullying interventions had a significant but “negligible” effect on reducing cybervictimisation (and no effect on perpetration). The meta-analysis by Wang et al. (2023), which includes some follow-up studies (from 10 months to 2 years after the intervention), also indicates a reduction in victimisation frequency, but no effect on perpetration. Finally, the umbrella review of meta-analyses by Kasturiratna et al. (2025) emphasizes the need for more studies with long-term follow-ups to adequately assess these aspects.

#### *5.2.5.4. Factors related to programme effectiveness*

While interventions can generally be considered effective, not all are equally so (Tozzo et al., 2022), and their effectiveness seems to depend largely on the specific characteristics of each intervention. In this regard, some of the findings from the reviewed literature highlight factors that may contribute to intervention effectiveness, as detailed in Table 8.

**Table 8.** Factors associated to intervention programme effectiveness

| Factors | Considerations |
|---|---|
| Target Population | It is important to consider who the intervention is directed at, since different approaches may vary in effectiveness for different populations. Among the reviews analysed, the only one focused exclusively on primary school students is the article by Chicote-Beato et al. (2024). These authors conclude that effective anti-cyberbullying programmes at this age range are those that address students’ emotional competence and self-regulation skills, a positive school climate, and online safety issues. The remaining reviews analyses include both children and adolescents, adolescents only, or adolescents and young adults, and point to various factors related to effectiveness in those cases, discussed further below. In what regards adults; however, the number of studies that include adult populations is limited and likely insufficient to draw conclusions based on evidence synthesis (Kasturiratna et al., 2025). |
| Pedagogical Components | First, as highlighted by Polanin et al. (2022), programmes specifically designed to reduce cyberbullying are more effective in reducing it than programmes that target violent behaviours in a more generic way, without focusing specifically on cyberbullying. |

| Factors | Considerations |
|---|---|
| | More specifically, the review conducted by Henares-Montiel et al. (2023) describes three types of components in anti-cyberbullying interventions (as mentioned above): "educational/informational," "skill development," and "cognitive/behavioural." Their analysis concludes that most effective interventions include the first two components, while the cognitive/behavioural component seems to have less influence on effectiveness. Furthermore, programmes that combine more than one of these components appear to be more effective than those focusing on only one. It should be noted, however, that this review does not include a meta-analysis, so it is not possible to quantitatively estimate the weight of these components in effectiveness.<br>In turn, the meta-analysis by Lan et al. (2022) shows that programmes that foster collaborative agency (among students and/or teachers) are significantly more effective than those merely providing information and knowledge about the phenomenon. This highlights the relevance of engaging students and teachers (and possibly other stakeholders, such as parents) in agentic peer interactions, beyond simply improving their knowledge of cyberbullying. |
| Mode of Delivery | Some of the reviews analysed examine how the mode of delivery (face-to-face at school, at home, online) influences effectiveness. In their meta-analysis, Doty et al. (2022) conclude that school-based interventions have demonstrated effectiveness, while findings are inconclusive for home-based interventions. However, the umbrella review conducted by Kasturiratna et al. (2025) suggests that interventions reduce cybervictimisations "regardless of whether the programme was school-based, targeting children and adolescents, or home-based, aimed at increasing parental awareness."<br>With respect to online delivery (as a complement to face-to-face interventions), Doty et al. (2022) found no significant differences in effect sizes between hybrid programmes (including an online component) and those delivered only face-to-face. Moreover, only two studies included in their analysis involved online-only interventions, making it difficult to draw conclusions. Relatedly, Ng et al. (2022) found that the effectiveness of cyberbullying programmes was higher when delivered by technology-savvy experts compared to teachers, possibly because in some cases teachers may lack sufficient technological expertise. |
| Duration of the Intervention | Ng et al. (2022) found no significant differences in programme effectiveness across interventions lasting less than 3 months, 3–6 months, or more than 6 months. By contrast, the review and meta-analysis conducted by Wang and Jiang (2023), which only includes studies with a parental involvement component, indicates that interventions lasting less than six months are more effective in reducing cybervictimisations than longer ones, suggesting that programme effects may fade over time.<br>The meta-analysis by Doty et al. (2022) did not find significant differences in effect sizes between interventions lasting 8 hours or less and those of longer duration. The authors therefore interpret that shorter interventions may be just as effective as longer ones, which should be taken into account when evaluating programme cost-effectiveness. |
| Parental Involvement | The studies reviewed provide inconclusive evidence regarding the role of parental involvement in intervention effectiveness. The review with meta-analysis by Ng et al. (2022) did not find significant differences in programme effectiveness related to parent involvement. One possible interpretation of this absence of effects, according to the authors, is that since many studies reviewed focus on adolescents, peer influence may outweigh parental influence in cyberbullying behaviours. Alternatively—and in light of previous studies suggesting a positive role of parent involvement—it may be that many |

| Factors | Considerations |
|---|---|
| | programmes included in this analysis involved parents only passively (e.g., receiving information). Thus, it is possible that only more active parental participation contributes to intervention effectiveness. Relatedly, Wang and Jiang's (2023) meta-analysis points to very small effect sizes in interventions including a parental component and also highlights the need to better understand how parental participation can enhance intervention outcomes. |

*Source: synthesis by JRC researchers.*

#### *5.2.5.5. Technology-Based Interventions*

Our review includes three review articles focusing on technology-based interventions against cyberbullying (Nee et al., 2023; Mishra et al., 2024; Salawu et al., 2020).

The article by Nee et al. (2023) provides a systematic review of technology-based approaches to addressing cyberbullying. The authors distinguish five types of technology-based interventions:

- 'Filtering and blocking software', which detects and/or removes content or messages that may be part of cyberbullying acts.
- 'Monitoring and reporting tools', which allow parents or educators to monitor children's internet use and/or generate alerts when problematic content is detected.
- 'Anonymous reporting tools', enabling (primarily students) to report instances of cyberbullying anonymously.
- 'Education and awareness programmes', such as workshops, seminars, or online resources on how to recognises and respond to cyberbullying.
- 'Peer mentoring programmes', including strategies to promote prosocial online behaviour and identify and report cyberbullying.

The authors conclude that these interventions have potential to support cyberbullying prevention. However, the article does not provide a detailed analysis of their effectiveness.

The review by Salawu et al. (2020) focuses on technological approaches to cyberbullying detection and identifies four typologies: a) supervised learning, b) lexicon-based, c) rule-based, and d) mixed-initiative approaches. The results suggest that the lack of labelled datasets and the non-holistic consideration of cyberbullying (e.g., whether online aggression is repeated, or other factors characterising the phenomenon) are the main barriers to developing effective applications for automatic detection of cyberbullying. Finally, the review by Mishra et al. (2024) addresses several approaches to detecting cyberbullying in online messages and texts, and agrees with Salawu et al. (2020) in highlighting the need for high-quality datasets—including contextual information—for better application performance in this area.

It is important to note, however, that the emergence of modern Large Language Models (LLMs) has provided revolutionary capacities in automated text processing, unthinkable just a few years ago, with strong potential for some of the approaches described for cyberbullying detection. Considering that the popularization of these models has only occurred in recent years, and given the time required for the publication of studies and reviews, it is unlikely that the existing reviews have yet captured possible LLM-based applications for cyberbullying detection. Therefore, the advent of these technologies may already have rendered some of the findings in these reviews outdated.

# 6. Definitions of cyberbullying by the scientific community

Researchers have consistently highlighted the absence of a universally accepted definition of cyberbullying (Bauman, Cross et al., 2013; Thomas et al., 2015; W. Zhang et al., 2022), despite major efforts in the scientific community to propose a construct around this phenomenon. For example, in September 2010, an International Cyberbullying Think Tank funded by the US National Science Foundation (NSA) was convened in Arizona to address that challenge. The group of 20 experts, which brought together researchers from three continents, eight countries and a range of academic disciplines — including psychology, public health, social work, counselling, communications and education —, could not come up with a precise definition that would move the field forward (Bauman, Cross et al., 2013). Indeed, the challenges for this endeavour are manifold:

> *Defining a construct is a challenging endeavor, particularly when, as in this case, the term is also used in colloquial and popular media—nonscientific contexts. Researchers' thinking may be influenced by these informal uses, which can lead to definitions that are not exact enough to allow reliable measurement. An additional dilemma is the tendency to assume that since the construct is labeled as a variant of "bullying," the characteristics should be parallel to those used to define traditional bullying. (Bauman, Card et al., 2013, p. 73)*

Nevertheless, there seems to be at least some level of consensus on several core elements that characterise the phenomenon. This consensus — as previously outlined in our analysis of commonly cited definitions among systematic literature reviews — includes repetition, intentionality and the use of electronic means, while power imbalance is also considered by many researchers a key characteristic that differentiates cyberbullying from other types of aggression involving the use of digital technologies.

It is worth noting that research on cyberbullying has been largely influenced by the seminal work of Olweus, who defined bullying or victimisation as a situation where "[a] person is being [...] exposed, repeatedly and over time, to negative actions on the part of one or more other persons" (1994, p. 98). As revealed by our bibliometric analysis and the review of systematic literature reviews, a few attempts to define cyberbullying have been rather influential, in particular the foundational definitions by:

- Patchin and Hinduja (2006, p. 152): "willful and repeated harm inflicted through the medium of electronic text."
- Kowalski and Limber (2007 S24): "bullying through e-mail, instant messaging, in a chat room, on a website, or through a text message sent to a cell phone."
- Smith et al. (2008, p. 376): "[a]n aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself."
- Tokunaga (2010, p. 278): "any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others."

Nonetheless, the goal of establishing a definition that can be adopted as the standard by all relevant stakeholders — including researchers, policymakers, and practitioners in key sectors such as education and health — remains largely unfulfilled. An important challenge is that the lived experiences of those involved in, or affected by, cyberbullying often go well beyond the boundaries of conventional definitions. As noted by Kofoed and Staksrud (2019): "The messiness in cases of cyberbullying is omitted from much of the conceptual work and a substantial part of children's experiences with a vast range of exclusionary practices is thereby left out of the dominant research paradigm and, as a result, from operational and preventive work."

The scientific community remains committed to the ambition of developing a definition that is comprehensive, accurate, and does not lose currency despite rapid socio-technical changes. Below are some examples of recent attempts to define cyberbullying by:

- Chun et al. (2020, p. 3): "a repeated and intentional act to threaten/harass/embarrass others through electronic means or devices."
- Zhang et al. (2022, p. 2): "behaviors expressed by an individual or group through Information and Communication Technologies (ICT), such as social media and e-mail, that repeatedly convey hostile or offensive information with the intention of causing harm or discomfort to others."
- Ray et al. (2024, p. 6): "The use of technology to manipulate and exploit targeted vulnerable victims using online aggression or harassment and repeated threats, to embarrass or humiliate by posting harmful content, with the purpose or intent to cause psychological or emotional harm, in some cases, leading to physical harm."
- O'Higgins Norman (2024, p. 4) "a damaging social process that is characterized by an imbalance of power driven by social (societal) and institutional norms. It is often repeated and manifests as unwanted interpersonal behaviour among students or school personnel that causes physical, social, and emotional harm to the targeted individuals or groups, and the wider school community."

Rather than establishing an overarching definition, in their *Teens and Cyberbullying 2022* study, the Pew Research Centre (2022) considered as cyberbullying victims those adolescents who had reported personally experiencing any of six distinct behaviours online or while using their phones: a) offensive name-calling, b) the spreading of false rumours about them, c) receiving explicit images they did not ask for, d) receiving physical threats, e) constantly being asked where they are, what they were doing, or who they were with by someone other than a parent, f) or having explicit images of them shared without their consent.

A key point of contention when trying to define cyberbullying is whether it should be regarded as an extension of traditional bullying or a distinct phenomenon on its own. In this regard, Olweus and Limber (2018) concluded, though tentatively, that empirical facts and deliberations in the literature "are consistent with the view of cyberbullying as a form of bullying, in line with other forms such as verbal, physical, and indirect/relational bullying" (Olweus et al., 2018, p. 141). On the contrary, after reviewing several meta-analyses to examine the correlations between cyberbullying and other variables, Barlett et al. (2024) found that the majority of meta-analytic effect sizes remained significant even after controlling for traditional bullying, indicating that cyberbullying accounts for unique variance. This suggests that cyberbullying has unique relationships with outcome variables, such as risk and protective factors, and that traditional bullying victimisation and perpetration do not fully explain cyberbullying. The findings support the idea that cyberbullying is a distinct phenomenon that requires special consideration, despite its frequent co-occurrence with traditional bullying.

## 6.1. Cyberbullying as a type of technology-mediated violence

Over the past decades, ICTs — such as computers, the World Wide Web, smartphones and social media — have gradually permeated all aspects of daily life, playing an increasingly central role in social dynamics while reconfiguring processes and practices across virtually every domain of society. Along with numerous benefits and opportunities, digital technologies are also associated with important societal challenges such as the facilitation of new forms of aggression. In this regard, the use of digital technology for abusive purposes requires rethinking some of the key elements that have traditionally underpinned the notion of bullying.

The definitions above refer to these technologies as “the medium of electronic text” (Patchin et al., 2006), “electronic forms of contact” (Smith et al., 2008), “electronic or digital media” (Tokunaga, 2010), “electronic means or devices” (Chun et al., 2020), “Information and Communication Technologies” (W. Zhang et al., 2022) or simply “technology” (Ray et al., 2024). A few definitions also mention more specific examples of technologies, including e-mail, instant messaging, chat rooms, websites, cell phones, social media, (Kowalski et al., 2007; W. Zhang et al., 2022).

It is worth noting that the definition by O’Higgins Norman do not mention technology explicitly, as it was formulated to cover school bullying and cyberbullying at the same time. However, by widening the spectrum of harms (i.e., physical, social, and emotional) and harmed parties (i.e., targeted individuals and the wider school community), this definition aims to “leaves more room for new and unexpected forms, such as those that digital technology may enable.” (O'Higgins Norman et al., 2025, p. 198).

Digital technologies have significantly altered the traditional boundaries of bullying, both in terms of time and space. In this regard, bullying is no longer confined to the physical walls of a school or a school bus, as digital platforms have enabled it to transcend physical boundaries, allowing it to occur anywhere and at any time, and shifting the behaviour from traditional face-to-face interactions to online environments. By reconfiguring the temporal and spatial boundaries of social interactions, along with the way we access, produce, and share content, digital technologies have made it possible for victims of cyberbullying to encounter harmful experiences anytime and anywhere.

The possibility to interact and share content anonymously is also one of those affordances of digital technologies that have been consistently discussed in the literature since the early days of research on this phenomenon (Hinduja et al., 2008; Kowalski et al., 2007; Ray et al., 2024).

Over the years, new online environments have emerged as modern-day playgrounds, where many young people spend a significant amount of time interacting with their peers (boyd, 2014). Unfortunately, new contexts of interaction like social media and online multiplayer gaming platforms have often become breeding grounds for new forms of cyberbullying (Ademiluyi et al., 2022; Giumetti et al., 2022; Hu et al., 2025; Teng et al., 2024). More recent developments include the capacity to generate hyper-realistic media (i.e., deepfakes) by means of generative artificial intelligence (Alexander, 2025; Negreiro, 2025).

Online interactions may also contribute to a moral disengagement, decreased empathy and disinhibition or inadequate awareness of the consequences of one’s actions, facilitating cyberbullying (Ray et al., 2024; L. Wang et al., 2024; Zammit, 2025).

‘Aggressive’, ‘hostile’ or ‘harmful’ are the terms most frequently employed in the definitions to characterise those behaviours that constitute cyberbullying. For example, perpetrators may cause harm by using digital technologies for impersonation, insulting or threatening someone, spreading rumours, or sharing compromising content. However, just like not all types of aggression or harassment can be regarded as bullying, not all violent or harmful acts that involve the use of digital technologies should be treated as cases of cyberbullying.

Repetition, intentionality and power imbalance are the three primary criteria used in the literature to distinguish both bullying and cyberbullying from other forms of violence. Since the early days of cyberbullying research, scholars have sought to unpack the implications of digital technologies for these aspects.

## 6.2. Repetition

The recurrent nature of harm in bullying and cyberbullying is one of the main pillars that have traditionally differentiated these phenomena from other types of aggression in the scientific literature. For example, in his seminal definition of bullying, Olweus used the expression "repeatedly and over time" (1994, p. 98), which was echoed literally in the definition of cyberbullying proposed by Smith et. (2008). All the subsequent definitions discussed above mention either the word "repeated" or "repeatedly."

It is worth noting that O'Higgins Norman (2024) placed the word "often" before "repeated", implying that repetition — at least on the part of the same aggressor — might not always be needed for an event to be classed as a case of cyberbullying. Repetition in cyberbullying is not simply about how many times an abusive behaviour occurs, but also the lingering impact on victims who fear that a single incident could be replayed or redistributed online. In this regard, Slonje and Smith chose the case of bullying based on the distribution of photos or videos to illustrate this point:

> *"The behavior of taking the picture or clip may have occurred merely once; yet if the bullying child sends that picture to more than one other person, or if the person receiving the image forwards it to anyone else, it could be argued that this falls under the category of repetition. If the picture or clip is uploaded onto a webpage, every hit on that specific page could count as a repetition." (Slonje et al., 2008, p. 154)*

As noted by O'Higgins Norman, sharing "a single harmful message/image/video online which is highly likely to be reposted or shared with others can however be seen as bullying behaviour " (2024, p. 6). In this sense, cyberbullies might exploit virality within networked communities to repeatedly harm their victims through the actions of others (i.e., those reposting), even if they act only once. According to this interpretation, while repeated actions are a clear hallmark of cyberbullying, they are not strictly required considering that an isolated episode can generate ongoing, repetitive harm.

## 6.3. Intentionality

The idea of harm being intentional is also core to traditional definitions of bullying and has therefore been included in most attempts to define cyberbullying too. Smith at el. (2013) argue that aggression is limited to purposeful acts intended to harm somebody who does not want to be harmed,[15] leaving out harm that is caused accidentally. Moreover, they point to three complementary criteria that can help in determining the intentional nature of harm: "the victim did

[15] Excluding thus self-harm behaviour.

experience harm; [...] the perpetrator intended not only the behavior but the harm; [... and] whether a reasonable person would judge that the action could be foreseen as likely to cause harm to the intended recipient" (Smith et al., 2013, pp. 58–59).

Intentionality is embedded in most of the definitions introduced at the start of this section. For example, the behaviour is described as "willful" harm (Patchin et al., 2006, p. 152), an "intentional act" (Chun et al., 2020, p. 3; Smith et al., 2008, p. 376), "intended to inflict harm or discomfort" (Tokunaga, 2010, p. 278), or "with the purpose or intent to cause" (Ray et al., 2024, p. 6).

However, some researchers have suggested that the idea of intentionality might be somehow diluted in some instances of cyberbullying where causing harms is not the main motivation behind the harming behaviour. Research conducted by Kowalski and Limber almost two decades ago already suggested that:

> *"a relatively large percentage of "friends" (and, to a lesser extent, siblings) were perpetrators of cyberbullying, it will be important to explore further the extent to which these behaviors are indeed indicators of intentional aggression via electronic sources or something less intentional and potentially less serious." (Kowalski et al., 2007, p. S29)*

Certain characteristics (e.g., absence of verbal and visual cues) of some forms of online interaction may make it more difficult to decipher intent in cyberbullying (Cassidy et al., 2013; Dennehy et al., 2020). As noted by O'Higgins Norman et al:

> *"Actors in these spaces are lacking information about who exactly they are communicating with, who else is present, who else will see what they have intimated, or in what ways any of these people are reacting. If they had that information, not only might they temper their words or behaviors, but they also might stop what they are doing right away." (O'Higgins Norman et al., 2025, p. 193)*

## 6.4. Power imbalance

The unequal balance of power — whether real or perceived — between perpetrators and victims is one of the main aspects that differentiates bullying from other forms of violence or aggression:

> *"It must be stressed that the terms bullying or victimization are not (or should not be) used when two persons of approximately the same strength (physical or psychological) are fighting or quarrelling. In order to use the term bullying, there should be an imbalance in strength (an asymmetric power relationship): The person who is exposed to the negative actions has difficulty in defending him or herself and is somewhat helpless against the harasser or harassers." (Olweus, 1994, p. 2)*

The imbalance of power in bullying can manifest in different ways, including:

1. "being physically weaker (for example, for physical attacks);
2. being verbally less fluent (for example, when teased);
3. lacking confidence or self-esteem;
4. being outnumbered;
5. lacking friends or social support;
6. having a low status or rejected position in the peer group." (Smith et al., 2013, p. 4)

Digital technologies add an extra layer of complexity to the power dynamics that underpin this form of abusive behaviour. The definition by Smith et al. highlights that aggressions in cyberbullying are directed at “a victim who cannot easily defend him or herself” (2008, p. 376), while O'Higgins Norman indicates that it is “a damaging social process that is characterized by an imbalance of power” (2024, p. 4). However, the rest of the definitions above do not feature this a core element.

Whereas power imbalance in bullying is mainly determined by physical strength and social capital, other important factors come to the fore when technology is at play, such the digital competence or access to technology of aggressors and victims.

> *“Although power in traditional bullying might be physical (stature) or social (competency or popularity), online power may simply stem from proficiency. That is, youth who are able to navigate the electronic world and utilize technology in a way that allows them to harass others are in a position of power relative to a victim.” (Patchin et al., 2006, p. 152)*

Likewise, the ability of aggressors to remain anonymous online may make it difficult for the victim to confront them or defend themselves (Barlett et al., 2022; Peter et al., 2018; Wegge et al., 2016). Furthermore, the ability to attack anonymously may provide a sense of protection to individuals who might otherwise be reluctant to engage in bullying behaviour (Barlett et al., 2016; Polanin et al., 2022; Vandebosch et al., 2008). All these considerations mean that children and young people “who have ‘power’ in offline spaces might not be the same who have power in virtual spaces” (Gottschalk, 2022).

It is also worth noting that cyberbullying can occur between people of diverse ages. In this regard, power imbalances may manifest in different ways, depending on whether this form of violence takes place between children (e.g., pupil to pupil), between children and adults (e.g., teacher to student or student to teacher) or between adults (e.g. employer to employee).

## 6.5. Cyberbullying as a socially situated phenomenon

Cyberbullying not only involves perpetrators and victims, but also a wider range of actors who may participate as bystanders or be indirectly affected by this behaviour, including peers (e.g., other students or colleagues), figures of authority within organisations (e.g., teachers, managers), and other social groups or communities to which the main affected parties belong (e.g., their families, friends).

Kowalski et al. (2014) hypothesised that the social dimension of abuse in terms of motivation might also differ between traditional bullying and cyberbullying, suggesting that the reasons underpinning the former could be more *interpersonal* and, in the case of the latter, more *intrapersonal*:

> *“the rewards for engaging in cyberbullying may be tied more to performing the action than to witnessing the consequences of that action or to having other ‘bystanders’ witness the effects of one’s aggressive behaviors on another individual.” (Kowalski et al., 2014, p. 1107)*

However, certain forms of cyberbullying can be largely driven by some expected reactions on the part of the wider community, as it is the case of trolling when defined as “a form of entertaining activity for both trolls and (some) bystanders at the behest of the victims” (Scriven, 2025, pp. 284–285).

Some of the definitions above specify that harm in cyberbullying can be inflicted by individuals either operating on their own or collectively (Smith et al., 2008; Tokunaga, 2010; W. Zhang et al., 2022). Whether victims and perpetrators need to be socially connected as part of a shared community for technology-mediated aggression to be regarded as a case of cyberbullying remains a contentious issue in the literature.

Olweus and Limber argue that it is important to differentiate cyberbullying from other forms of cyber-aggression or cyber-harassment “where the perpetrator(s) and the targeted youth do not belong to the same classroom, school, or other common social unit, and the youth exposed may have no idea of who the perpetrator is.” (Olweus et al., 2018, p. 142). However, according to Anichitoae et al. “In contract [sic] with traditional school bullying that involves a perpetrator who is often someone the victim knows, in cyberbullying, the perpetrator may be someone the victim has never met in person” (Anichitoae et al., 2025, p. 1).

Identifying clear social links connecting victims and aggressors within the boundaries of social communities can be more challenging in the case of cyberbullying, as compared to traditional bullying, since it can often occur in the context of informal communities (e.g., playing in an online game platform, as opposed to the schoolyard).

Most often, bullying has been studied in relation to specific organisational contexts, especially in school settings (Olweus, 1994) and, to a lesser extent, in the workplace (Eurofound, 2024). Indeed, most of the definitions above were proposed in scientific articles specifically devoted to the study of this phenomenon in educational contexts (Kowalski et al., 2007; O’Higgins Norman, 2024; Patchin et al., 2006; Smith et al., 2008; Tokunaga, 2010). Overall, research on cyberbullying has been primarily concerned with children and it can be argued that the term is closely associated with younger populations, while other terms like online harassment or cyber-aggression seem to be applied more generally to the wider population. However, it is worth noting that research institutions like the Pew Research Centre (2022) use “cyberbullying” and “online harassment” as synonyms.

The power dynamics already discussed are largely dependent on the organisational cultures, institutional dynamics and broader social fabric in which bullying and cyberbullying take place. In this regard, belonging to a marginalised group will likely confer less power to a potential victim:

> *“Here, although at an individual level he or she may be strong or confident, the group to which they identify or to which they are perceived to belong is in a weaker position or is discriminated against. This, of course, varies with societal context but can be defined contextually by ethnicity, race, religion/faith, sex, sexual orientation, or disability. […] It is not necessarily any deficit characteristic in the victim that puts him/her in a vulnerable or disadvantaged position. Perhaps it is neutral (being new in a classroom) or a quality that when viewed from a third-party perspective is seen as positive (e.g., being more articulate, having a particular talent) that makes him/her the target of the peer attacks. Imbalance of power very often can be summarized as being different from the majority in the group and thus having less power in the social hierarchy.” (Smith et al., 2013, p. 4)*

It is worth noting that only one of the definitions discussed above highlights the social dimension of this type of behaviour as core element. The definition by O'Higgins Norman, which refers specifically to school bullying (including cyberbullying), approaches it as “a social process that is characterized by an imbalance of power driven by social (societal) and institutional norms” (2024, p. 4). This definition emphasises:

1. the relational nature of both bullying and cyberbullying (i.e., happening within a network of people),

2. the enabling or inhibiting role of social and institutional contexts, and

3. the fact that some aggressors might be driven by group dynamics, instead of the intention to harm the victim (e.g., in sharing a photo based on peer pressure, as opposed to the intent to harm the victim). (O'Higgins Norman et al., 2025).

It is worth noting that while conventional definitions of bullying have been mainly proposed from a developmental psychology perspective, this effort to formulate a more inclusive definition is based on a diverse range of scholarly disciplines — including education, sociology, technology studies, criminology — that approach human behaviour as a situated phenomenon that takes place in overlapping social contexts.

# 7. Insights from policy and legislation

This chapter presents an overview of how cyberbullying is defined by several international organisations (section 7.1). It also investigates how EU Member States, and other countries within the European Economic Area (EEA), incorporate cyberbullying into their national legal frameworks. Building on previous studies (Council of Europe, 2018; Murphy, 2024; O'Neill et al., 2025), we conducted our own analysis of national legislation and definitions included in legal texts (section 7.2).

## 7.1. Cyberbullying through the lens of international organisations

There is no universally accepted definition of bullying or cyberbullying in the realm of policymaking. However, several international organisations (e.g., UN, EU, CoE, UNESCO, WHO) have offered definitions of cyberbullying formulated in the context of efforts aimed at tackling this phenomenon, especially in relation to the safeguarding of children from the emerging risks associated with digital technology use. In this regard, cyberbullying is often approached as a form of 'online violence' and, more specifically, a type of 'cyber-aggression.' In this regard, referring to online violence against children in particular, the World Health Organization (WHO) notes that:

> *"Online violence encompasses a wide range of activities which can be perpetrated by adults or peers who can be family members, acquaintances or strangers. Adults can try, and sometimes succeed, to engage children and adolescents in sexual activities online. They can coerce children to abuse other children. Peers can bully or sexually harass schoolmates, extort images and spread false rumors, or digitally record sexual activity that occurs offline. A type of abuse that has been particularly exacerbated by technology is the making and distribution of images or videos depicting child sexual abuse or exploitation." (WHO, 2022a)*

Within the realm of online violence, WHO (2022b) identifies two domains: 1) online sexual exploitation and abuse and 2)·cyber-aggression and cyber-harassment. WHO places cyberbullying under the latter domain, while recognising that the two domains may overlap, for instance in cases of nonconsensual sexting and sexual extortion.

The UN General Assembly (2024, 2023, 2019) has adopted several resolutions that focus on protecting children from bullying and cyberbullying, urging States to implement measures such as establishing specialised bodies to prevent and address cyberbullying, and integrating online protection into national policies to combat exploitation, violence, and abuse, with a particular emphasis on safeguarding the rights of persons with disabilities.

In the EU context, as early as 2009, the European Commission (EC) defined cyberbullying as part of the Safer Internet campaign, recognising that digital technologies can facilitate new forms of harassment through interactive services. Since then, a diversity of working definitions has been used by international organisations. Table 9 offers several definitions of cyberbullying, in some instances in relation to other related terms and expressions. It is worth noting that in many of these efforts a definition of bullying is outlined first, to then specify that the term cyberbullying applies when digital technologies play a role in that behaviour.

**Table 9.** Definitions of cyberbullying and associated terms in documents by international organisations

| Initiatives / Organisations | Terms | Definitions |
|---|---|---|
| United Nations: Resolution adopted by the Human Rights Council on 9 October Countering cyberbullying | Cyberbullying | "cyberbullying may be understood as an intentional act carried out by an individual or a group using electronic forms of contact against victims, which is typically carried out repeatedly and over time and is often characterized by a power differential," (UN General Assembly, 2024, p. 2) |
| European Commission: Safer Internet Day 2009 | Cyberbullying | "repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, 'happy slapping', disagreeable comments or slander. Interactive online services (e-mail, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims." (European Commission, 2009) |
| European Commission: *Wellbeing and mental health at school Guidelines for education policymakers* | Cyberbullying | "use of technology to bully (harass, threaten, embarrass, or target) another person. It usually takes 4 mains forms: (1) written/verbal through phone-calls, text messages, emails, chats, blogs, posts on social media; (2) visual, through posting compromising or humiliating photos or videos; (3) exclusion by intentionally excluding a person from a group; (4) impersonation by using another person's account details to cause harm. Although the three core elements of bullying—power imbalance, intent to harm, and repetition—are recognised in cyberbullying, there is continuing debate over how these are expressed online, mainly because cyberbullying operates 24/7, resulting in potential multiplication of the effect on victims, with a consequent heightened risk to their mental health." (EC: DG EAC, 2024a, pp. 32–33) |
| Council of Europe | Bullying | Bullying is unwanted, aggressive behaviour among school aged children that involves a real or perceived power imbalance. The behaviour is repeated, or has the potential to be repeated, over time. Both kids who are bullied and who bully others may have serious, lasting problems. Bullying may include physical violence, sexual violence, threats, teasing, social exclusion or other psychological violence. The presence of bullying is often a sign of aggressive or violent behaviour elsewhere in children's lives and young children may be acting out at schools or elsewhere what they have observed and learned at home. (Council of Europe, n.d.) |
| Council of Europe | Cyberbullying | Cyber bullying, or using electronic technologies in order to bully another person through the Internet is becoming more common among children and youth today. The challenge with cyber bullying is the fact that it takes on so many different forms. Examples of cyber bullying include mean text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos or websites. (Council of Europe, n.d.) |

| Initiatives / Organisations | Terms | Definitions |
|---|---|---|
| UNICEF (with the participation of UNODC and The World Bank among other organisations):<br>INSPIRE - Ending Violence Against Children | Bullying | "Unwanted, aggressive behaviour by another child or a group of children who are neither siblings nor in a romantic relationship with the victim. Bullying involves a repeated pattern of physical, psychological or social aggression likely to cause harm, and often takes place in schools and other settings where children gather, as well as online. It may occur in person or online (cyber bullying).<br>In-person bullying may include: physical acts, such as pushing and hitting, and verbal acts, such as making fun of people for their race, religion or appearance, or sexual comments or jokes. Bullying may also include repeatedly leaving people out or ignoring them." (UNICEF, 2018, p. vi) |
| UNICEF (with the participation of UNODC and The World Bank among other organisations):<br>INSPIRE - Ending Violence Against Children | Cyber (digital) bullying | "may include: sending hurtful messages or posting them online where others can see; threatening someone online; creating a website that makes fun of someone; and sharing or posting hurtful images or pictures without permission through texting, emails, social media or other online channels." (UNICEF, 2018, p. vi) |
| World Health Organization: *Violence Against Children Online. What health systems and health care providers can do* | Cyberbullying | "Repetitive aggression, hostility and other attempts to cause harm in online communications such as threats, distributing defamatory information, hate speech, including homophobic and sexist content mostly perpetrated by peers." (WHO, 2022a) |
| World Health Organization: *What works to prevent online violence against children?* | Cyberbullying | "The term cyberbullying references verbal aggression, threats, hostility, and other attempts to cause harm in online communications. It encompasses terms such as flaming, outing, hate speech, online drama, and online harassment. It can include the posting of false profiles, distributing defamatory information, and sometimes includes cyberstalking. Apart from physical threats and threats to home, family, and friendships, cyberbullying (like face-to-face bullying) often includes sexual content, such as sexual harassment, sexual shaming, and homophobic and sexist insults. Hate communication, racial, ethnic and gender attacks are also common. Online bullying, harassment and aggression also often occur in the context of adolescent dating relationships, among school peers, as well as in relationships started online and through dating apps. These topics are sometimes referred to separately as online dating or relationship abuse, but they fit within the definition of cyberbullying." (WHO, 2022b, p. 7) |
| World Health Organization: | Cyberstalking | "Cyberstalking refers to persistent unwanted contact via technology that directly or indirectly communicates a threat or creates fear in the victim, and it can involve frequent unwanted requests for communication or favours. Even when they have |

| Initiatives / Organisations | Terms | Definitions |
|---|---|---|
| *What works to prevent online violence against children?* | | been blocked, cyberstalkers, continue to contact victims through other platforms or under changed identities. Sometimes cyberstalkers threaten to appear in person or retaliate in social networks. Cyberstalking can be a mix of online and offline harassment and can have a sexual component in the form of persistent requests for sexual images or face-to-face sexual activities. The most common perpetrators of cyberstalking against both males and females are acquaintances or current and former intimate partners), as well as internet contacts who want to establish or continue a relationship that is no longer wanted." (WHO, 2022b, p. 7) |
| UNESCO:<br>Safe to learn and thrive: Ending violence in and through education | Bullying | "Bullying is characterized by an imbalance of power or strengths driven by societal and institutional norms. Newer analysis of evidence suggests that bullying is often repeated and manifests as unwanted interpersonal behaviour among students or school personnel that causes physical, social and emotional harm to the targeted individuals or groups, and the wider school community. Bullying can be physical, which includes repeated aggression such as being hit, hurt, kicked, pushed, shoved around or locked indoors, having things stolen, having personal belongings taken away or destroyed, or being forced to do things; psychological, which includes verbal abuse, emotional abuse and social exclusion and refers to being called mean names, being teased in an unpleasant way, being left out of activities on purpose, excluded or completely ignored, and being the subject of lies or nasty rumours; and sexual, which refers to being made fun of with sexual jokes, comments or gestures." (UNESCO, 2024, p. 16) |
| UNESCO:<br>Safe to learn and thrive: Ending violence in and through education | Technology-facilitated violence / Cyberbullying | "Technology-facilitated violence refers to diverse forms of violence that take place via information and communication technologies or digital platforms such as by SMS, messaging applications or online. Cyberbullying includes being bullied by online messages, for example sharing mean instant messages, posts or emails; by images, for example posting unflattering or inappropriate pictures of someone online without their permission; or via the phone, for example sending hurtful texts or making hurtful calls. Technology-facilitated gender-based violence includes acts or threads of acts of violence committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media and based on gender. This can encompass behaviours like cyberbullying, online harassment, and online grooming, where perpetrators exploit digital platforms to manipulate and coerce victims, often with a focus on vulnerable groups. These forms of violence can occur in, around and through schools and education." (UNESCO, 2024, pp. 16–17) |

*Source: Definitions compiled by JRC from the indicated sources.*

As a form of violence and aggression, bullying and cyberbullying are always characterised as hostile behaviour intended at causing **harm**. All the definitions in Table 9 recognise the harmful and negative impact these phenomena can have on individuals, particularly children and adolescents. Such policy definition highlights the various ways in which bullying can manifest, including physical, psychological, and sexual forms. They also emphasise the importance of recognising the overlap between cyberbullying and other forms of online harassment.

The role of **technology** in facilitating bullying is also a common theme across policy definitions, with mentions to the role of digital platforms in giving perpetrators new opportunities to abuse their victims. Some of them highlight the various forms that cyberbullying can take, including written, visual, and exclusionary behaviours. More specifically, some definitions mention "phone-calls, text messages, emails, chats, blogs, posts on social media" (EC: DG EAC, 2024a, pp. 32–33) or "sharing or posting hurtful images or pictures without permission through texting, emails, social media or other online channels." (UNICEF, 2018, p. vi).

The definitions differ in their level of detail and scope, with some providing a broad overview of bullying and others focusing specifically on cyberbullying. In line with the definitions from the scientific literature previously discussed, these policy documents also identify **repetition** as a key characteristic of cyberbullying, as implied by phrases like "the behaviour is repeated, or has the potential to be repeated, over time" (Council of Europe, n.d.) or "involves a repeated pattern of physical, psychological or social aggression" (UNICEF, 2018).

However, the **intentional** nature of the behaviour is largely absent from these definitions, except for the one included in the *Wellbeing and mental health at school Guidelines for education policymakers*, which highlights that:

> *Although the three core elements of bullying—power imbalance, intent to harm, and repetition—are recognised in cyberbullying, there is continuing debate over how these are expressed online, mainly because cyberbullying operates 24/7, resulting in potential multiplication of the effect on victims. (EC: DG EAC, 2024a, p. 33).*

Apart from this definition, only a few others explicitly refer to the role of **power imbalance** as a defining aspect of bullying (and thus cyberbullying), with the Council of Europe (n.d.) indicating that bullying "involves a real or perceived power imbalance" and UNESCO (2024, p. 16) specifying that it is "characterized by an imbalance of power or strength."

Following the G7 commitments made in 2019, UNESCO and the French Ministry of Education, Youth and Sports established a Scientific Committee to develop recommendations for preventing and addressing school bullying and cyberbullying. One of the key tasks of this committee was to re-examine the conventional definition of school bullying, taking into account the impact of digital technologies on the evolution of this behaviour.

> *"Previous definitions considered bullying as concerned largely with repeated aggressive behaviour that occurs between two individuals or a group against an individual who are unable to make it stop. However, today there is recognition that bullying of students occurs within a system of relationships and structures that exist both within the school and outside the school." (UNESCO, 2020)*

In 2021, UNESCO and the World Anti-Bullying Forum (WABF) created a working group to propose a revised definition of school bullying (including cyberbullying), that was finalised in 2023:

> *"School bullying is a damaging social process that is characterized by an imbalance of power driven by social (societal) and institutional norms. It is often repeated and manifests as unwanted interpersonal behaviour among students or school personnel that causes physical, social, and emotional harm to the targeted individuals or groups, and the wider school community." (O'Higgins Norman, 2024)*

This definition was used in the report *Safe to learn and thrive: Ending violence in and through education* (UNESCO, 2024), which is the only one in Table 9 that explicitly recognises that bullying and cyberbullying result from power imbalances grounded upon social dynamics.

Considering the definition is the result of work by a scientific committee of experts (O'Higgins Norman et al., 2025), we have discussed it before along with the definitions formulated in the context of the academic literature.

As a form of violence and aggression, bullying and cyberbullying are always characterised as hostile behaviour intended at causing **harm**. All the definitions in Table 9 recognise the harmful and negative impact these phenomena can have on individuals, particularly children and adolescents. Such policy definition highlights the various ways in which bullying can manifest, including physical, psychological, and sexual forms. They also emphasise the importance of recognising the overlap between cyberbullying and other forms of online harassment.

The role of **technology** in facilitating bullying is also a common theme across policy definitions, with mentions to the role of digital platforms in giving perpetrators new opportunities to abuse their victims. Some of them highlight the various forms that cyberbullying can take, including written, visual, and exclusionary behaviours. More specifically, some definitions mention "phone-calls, text messages, emails, chats, blogs, posts on social media" (EC: DG EAC, 2024a, pp. 32–33) or "sharing or posting hurtful images or pictures without permission through texting, emails, social media or other online channels." (UNICEF, 2018, p. vi).

The definitions differ in their level of detail and scope, with some providing a broad overview of bullying and others focusing specifically on cyberbullying. In line with the definitions from the scientific literature previously discussed, these policy documents also identify **repetition** as a key characteristic of cyberbullying, as implied by phrases like "the behaviour is repeated, or has the potential to be repeated, over time" (Council of Europe, n.d.) or "involves a repeated pattern of physical, psychological or social aggression" (UNICEF, 2018).

However, the **intentional** nature of the behaviour is largely absent from these definitions, except for the one included in the *Wellbeing and mental health at school Guidelines for education policymakers*, which highlights that:

> *Although the three core elements of bullying—power imbalance, intent to harm, and repetition—are recognised in cyberbullying, there is continuing debate over how these are expressed online, mainly because cyberbullying operates 24/7, resulting in potential multiplication of the effect on victims. (EC: DG EAC, 2024a, p. 33).*

Apart from this definition, only a few others explicitly refer to the role of **power imbalance** as a defining aspect of bullying (and thus cyberbullying), with the Council of Europe (n.d.) indicating that bullying "involves a real or perceived power imbalance" and UNESCO (2024, p. 16) specifying that it is "characterized by an imbalance of power or strength."

Following the G7 commitments made in 2019, UNESCO and the French Ministry of Education, Youth and Sports established a Scientific Committee to develop recommendations for preventing and addressing school bullying and cyberbullying. One of the key tasks of this committee was to re-examine the conventional definition of school bullying, taking into account the impact of digital technologies on the evolution of this behaviour.

> *"Previous definitions considered bullying as concerned largely with repeated aggressive behaviour that occurs between two individuals or a group against an individual who are unable to make it stop. However, today there is recognition that bullying of students occurs within a system of relationships and structures that exist both within the school and outside the school." (UNESCO, 2020)*

In 2021, UNESCO and the World Anti-Bullying Forum (WABF) created a working group to propose a revised definition of school bullying (including cyberbullying), that was finalised in 2023:

> *"School bullying is a damaging social process that is characterized by an imbalance of power driven by social (societal) and institutional norms. It is often repeated and manifests as unwanted interpersonal behaviour among students or school personnel that causes physical, social, and emotional harm to the targeted individuals or groups, and the wider school community." (O'Higgins Norman, 2024)*

This definition was used in the report *Safe to learn and thrive: Ending violence in and through education* (UNESCO, 2024), which is the only one in Table 9 that explicitly recognises that bullying and cyberbullying result from power imbalances grounded upon social dynamics.

Considering the definition is the result of work by a scientific committee of experts (O'Higgins Norman et al., 2025), we have discussed it before along with the definitions formulated in the context of the academic literature.

## 7.2. Legislation and policies in the European Economic Area

This section aims to understand how cyberbullying is addressed in national legislation, offering an overview of the diversity of approaches across all EU Member States and other countries in the EEA. This section focuses on how EU Member States, and other countries within the EEA, incorporate cyberbullying into their national legal frameworks. Building on previous studies (Council of Europe, 2018; Murphy, 2024; O'Neill et al., 2025), we conducted our own analysis of national legislation and definitions included in legal texts.

Legislation, definitions, and terms were reviewed in English when translations from the original source were available; otherwise, machine translations from the national language were used. Consequently, there may be discrepancies between the translated texts (definitions and terms) and those in the original national language. For instance, a term corresponding to 'cyberbullying' in the original language might be translated as 'online harassment,' and vice versa. These translations may not fully capture the underlying concepts, and some relevant definitions may have been inadvertently omitted. Examples of terms from the original sources in languages other than English include '*Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems*' (Austria), '*obtěžováním*' (Czechia), '*harcèlement scolaire*' (France), '*cyberbullismo*' (Italy), or '*acoso*' (Spain), among others.

Considering this, we adopted a flexible approach when examining the legislation. Apart from texts that explicitly tackle cyberbullying, we addressed specific aggressive behaviours that, under certain circumstances, can be related to or regarded as instances of cyberbullying. In this sense, the analysis included in section 7.2 covers illegal acts of aggression that may be considered as cases of cyberbullying when committed through electronic means and leading to repetitive harm over time, irrespective the term used.

### 7.2.1. Legislation

With cyberbullying prevalence rising among young people, institutional bodies across the European Economic Area (EEA) countries[16] are pursuing legislation and policies to prevent its spread and ensure safe online environments. Since cyberbullying can be reflected in a broader spectrum of abusive or aggressive behaviours, it may be covered by existing legislation targeting other forms of violence. At the same time, not all forms or instances of cyberviolence are equally severe and not all of them necessarily require a criminal law solution but may be addressed by a graded approach and a combination of preventive, educational, protective and other measures (Council of Europe, 2018).

Existing legislation at European level, such as the EU's General Data Protection Regulation (GDPR), the European Media Freedom Act (EMFA), the revised Audiovisual Media Services Directive (AVMSD), the Regulation on preventing and combatting the sexual abuse and sexual exploitation of children, ePrivacy Regulation, the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act and the Artificial Intelligence Act, also guided countries implement related laws and regulations in their national legislative system that can also cover cyberbullying aspects.

To map how the phenomenon is addressed by national legislations, we have broadened the scope to cover, besides cyberbullying, other types of aggression that may be related to or constitute cyberbullying when committed by means of technologies. The definitions presented in section 7.2.2 come from this corpus of criminal and civil legislation currently in place, and therefore do not consider legislation that is still in draft form and pending formal adoption. This section neither covers definitions emanating from non-legislative documents, official websites, nor other initiatives used by EEA countries to address cyberbullying. Examples of these are protocols and strategies to prevent cyberbullying at schools, awareness campaigns, official websites focused on combating cyberbullying and offering services to stakeholders.

Our analysis shows that in all EEA countries bullying or cyberbullying aspects can be covered to a certain extent under their criminal justice — cyberbullying may be a specific case of crimes related to, for example, harassment, violence, threat, defamation, hate speech, sexual abuse, when these are committed through electronic means. Most of the EEA countries (23) make explicit references to the use of electronic means in the description of the offenses, addressing cyberbullying — or other related acts such as online harassment, stalking and violence — in ad-hoc legislation or specific Criminal code articles.

A detailed look at ad hoc legislation confirms a wide range of approaches taken by countries: some regulations focus on concrete social and institutional contexts (e.g. educational settings, workplace, domestic violence) or population groups (children, minors), while other legislation covers cyberbullying as part of wider areas (e.g., discrimination, communications).

For instance, the following cases relate to the prevention and reporting of cyberbullying in **education**: Denmark, ‘Educational Environment Act’ (art. 1b); Finland, the ‘Pupil and Student

[16] The 27 EU Member States plus three of the four EFTA states: Iceland, Liechtenstein and Norway.

Welfare Act' rules on student welfare in sectorial acts; France: 'Law No. 2022-299 aimed at combating school bullying' (art. 2 amends article L421-8 of the Education Code); Greece: 'Law 5029/2023 on Arrangements to prevent and address violence and bullying in schools and other classrooms' (arts. 3 to 15); the Netherlands, 'School Safety Act' (art.1 amends the Primary Education Act introducing art. 4c on duty of care for safety at school); Portugal, 'Law No 51/2012 on Student Statute and School Ethics' combats school violence; Romania: 'National education law 1/2011' (art. 7 and 56); Spain, 'Organic Law 2/2006, of May 3, on Education explicitly addresses school bullying and cyberbullying; Sweden: 'School Act 2010:800'(chapter 6); and Norway: 'The Norwegian Education Act' (chapter 12).

Legislation focused on protection of **minors or youth** includes: Germany, 'Youth Protection Act'; Italy, 'Law 71 of 29 May 2017 on Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying'; Latvia, 'Law on the protection of children's rights'; Lithuania, 'Law on Fundamentals of Protection of the Rights of the Child'; and Spain, 'Organic Law 8/2021, of 4 June, on the comprehensive protection of children and adolescents against violence'.

National legislation that tackles cyberbullying in the **workplace** includes: Denmark, 'Working Environment Authority executive order' and Iceland 'Regulation on measures against victimisation, sexual harassment, gender-based harassment and violence in workplaces'.

Two countries protect against cyberbullying through legislation on **discrimination**: Czechia, 'Anti-Discrimination Act' and Sweden, 'Discrimination Act'. Another two focus on **domestic violence**: Poland, 'Law of 29 July 2005 on combating domestic violence' and Romania, 'Law no 217/2003 on preventing and combating domestic violence'. Additionally, Cyprus legislates on **harassment**, 'Law 2021 (L.114(I)/2021) on Protection from Harassment and Stalking'; Ireland on **harassment and communications**, 'Harassment, Harmful Communications and Related Offences Act 2020', and Belgium on **electronic communications**: Belgium, 'Law on Electronic Communications'; and Hungary, on internet aggression, 'The Act LXXVIII of 2024 on the Suppression of Internet Aggression'. Finally, Portugal has the comprehensive 'Charter on Human Rights in the Digital Age'.

The enormous heterogeneity in the approaches adopted by EEA countries to address cyberbullying in legislation, especially when done through isolated articles within the criminal justice system, suggests that, in general, cyberbullying is not addressed in an integrated manner within the legal framework. The adoption of legislation specifically focusing on bullying or cyberbullying could be a way to effectively and comprehensively introduce the various elements of early detection, prevention, awareness-raising, and protection that this problem requires.

Table 10 presents the list of legislative texts identified as addressing cyberbullying or related acts of aggression, with the detail of the articles more directly legislating on the phenomenon.  1 presents country fiches with details about the legislation, the text of the referred articles considered as definitions in this analysis, and examples of initiatives put in place by each country to prevent and fight cyberbullying.

Moreover, EEA countries have introduced specific legislation on child sexual harassment, in compliance with the Regulation on preventing and combating the sexual abuse and exploitation of children (Directive 2011/93/EU, 2011). Although sometimes related to cases of cyberbullying, these instances are not strictly considered as such, and this type of legislation is excluded from the scope of our analysis.

In all EEA countries, we found national or regional actions that promote the digital competence of individuals, as well as actions to promote media literacy in the curriculum and school-based policies and actions to combat cyberbullying.

As noted by Gottschalk (2022), the lack of a consistent international definition of cyberbullying leads jurisdictions to address it differently, sometimes using extreme measures like criminal justice responses. This can be controversial when dealing with children, as it risks criminalising those unaware of their actions' seriousness. In the same line of reasoning, Livingstone et al. point that:

> *"in cases of violence or abuse by children, for instance in cases of cyberbullying, frameworks might need to be revised in order to pursue suitable and adequate preventive and restorative approaches, while preventing the criminalisation of children. In many countries cyberbullying may engage the criminal law in the context of offences against the person although it is likely to be the case that involving law enforcement, or the courts will only be appropriate in the rarest of cases." (Livingstone et al., 2020, p. 58)*

**Table 10**. Cyberbullying-related legislation in EEA countries

| Countries | How cyberbullying is addressed in legislation |
|---|---|
| **Belgium** | Article 442bis of the Criminal Code defines harassment in a broad sense. Articles 443, 444 and 448 of the Criminal Code may also apply to cyberbullying (crimes of threats, defamation, slander or offenses involving text or images).<br>Also, Article 145 §3b of the Law on Electronic Communications, refers to the use of electronic communication means to cause damage and nuisance. |
| **Bulgaria** | The Criminal Code criminalises discrimination, violence or hatred by electronic information systems, when committed on the basis of race, nationality or ethnic origin (Chapter Three Section I - Crimes Against the Equality of All Citizens, Art. 162). |
| **Czechia** | The Anti-Discrimination Act (Act 198/2009 Coll.) rules on harassment, sexual harassment and stalking (Art. 4).<br>Several articles in the Criminal Code are applicable to cyberbullying (when committed by electronic means, although not mentioned) (e.g., Arts. 353-354 on dangerous threats and dangerous stalking, Arts. 180, 181, 182 and 184, under section on offences against rights to the protection of personality, privacy and correspondence), as well as in the Act no. 251/2016 Coll. on Certain Offences (e.g. Art. 7(1)(a) and Art. 7(1)(c)4). |
| **Denmark** | The Criminal Code contains a number of provisions that may be applicable to cyberbullying, although not mentioned (e.g., under chapter 26 on crimes against personal freedom, and chapter 27 on peace and defamation).<br>In addition, the Educational Environment Act Executive order, Art. 1b refers to the obligation of educational institutions to have an antibullying strategy (LBK nr 316 of 05/04/2017).<br>The Working Environment Authority executive order 1406 of 26 September 2020 on Psychosocial Working Environment refers to bullying, sexual harassment and offensive behaviour in the working context. |
| **Germany** | Articles in the Criminal Code may apply to cyberbullying when committed with electronic means. such as section 238 (stalking) and section 176 (child abuse), which expressly covers conduct by means of telecommunications. |

| Countries | How cyberbullying is addressed in legislation |
|---|---|
| | In addition, sections on the Youth Protection Act (JuSchG): Section 3-Protection of minors in the media, Section 4-Federal Centre for the Protection of Children and Young People in the Media and Section 15-Media harmful to minors. |
| **Estonia** | Articles in the Penal Code can be applied to cyberbullying when committed online, although not mentioned, and more specifically, 157$^3$ – Harassing stalking. |
| **Ireland** | The Non-Fatal Offences Against the Person Act, 1997 legislates on harassment.<br>The Irish Harassment, Harmful Communications and Related Offences Act 2020 and the Incitement to Violence or Hatred and Hate Offences Act 2022 include references that may be used in relation to cyberbullying when the offenses are committed through electronic means. |
| **Greece** | The Law No. 5029 introduces as of March 2023 actions and regulations to prevent, identify and address violence and bullying in schools, including electronic or online violence.<br>Also, the Greek Penal Code contains specific provisions that may refer to cyberbullying. Indicatively, art. 333(2) imposes stricter punishments for perpetrators of cyberstalking against minors. |
| **Spain** | Law 1/2015 of 30 March amending the Criminal Code (Art. 172 ter) introduced an offence related to harassment (also by any communication means), updated in 2022 and 2023. Other Criminal Code provisions protect against unauthorised sharing of images or recordings (art. 197.7) and hate crimes on social media (art. 510).<br>In addition, there is a series of legal instruments addressing offences related to cyberbullying, including Organic Law 8/2021, which provides comprehensive protection against violence for children and adolescents.<br>Also, schools are responsible for preventing and investigating all forms of harassment or offensive behaviour, explicitly including cyberbullying (Organic Law 2/2006, of May 3, on Education).<br>An Organic Law for the Protection of Children in Digital Environments has been approved for processing in September 2025. |
| **France** | Law No. 2022-299 of March 2, 2022 aimed at combating school bullying amended Criminal Code's article 222-33-2 on harassment, aggravated when committed through an online public communication service or a digital or electronic medium. Other articles that may be applied to cyberbullying when committed by electronic means, although not stated, include: art. 223-13 and 223-14 on inducing suicide, art. 226-1 on invasion of private life, ar. 226-2 on unauthorised sharing of documents or recordings, including of sexual nature. |
| **Croatia** | The Criminal Code addresses several offenses that may apply to cyberbullying, some of which are aggravated when committed by electronic means: unauthorised audio recording, eavesdropping or sharing of images (arts. 143-144), insult, libel, aggravated when using computer systems or network (art. 147, 149), sexual harassment (art. 156). |
| **Italy** | Law 71 of 29 May 2017 entitled "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying".<br>In addition, besides the general offences concerning violence or threat, the Italian Criminal Code includes the specific offences of stalking (art. 612-bis), illicit dissemination of sexually explicit images or videos (art. 612-ter), and illegal dissemination of content generated or altered with artificial intelligence systems (art. 612-quarter). |

| Countries | How cyberbullying is addressed in legislation |
|---|---|
| **Cyprus** | Law 2021 (L.114(I)/2021) on 'Protection from Harassment and Stalking' introduces both criminal and civil offenses of harassment and stalking. They may apply to cyberbullying when committed by electronic means, although not mentioned. |
| **Latvia** | Articles in the Criminal Law may be applied to cyberbullying when committed through electronic means, and more specifically, section 157-Defamation (aggravated if in mass media), section 132$^1$ Persecution, section 150-Incitement to Social Hatred and Enmity.<br>The Law on Protection of the Children's Rights sets out the rights and freedoms of a child and defines physical and emotional violence in this context (section 81). |
| **Lithuania** | The Law on Fundamentals of Protection of the Rights of the Child (I-1234 of 14 March 1996), in its article 3, identifies bullying as a form of violence against children, among other forms of violence.<br>Also, the Criminal code's article 152-Sexual harassment and article 152$^1$-Grooming of a person under the age of sixteen years may constitute cyberbullying if committed through electronic means. |
| **Luxembourg** | Criminal Code includes in Chapter IV.2 the offense of obsessive harassment (introduced by L.5 June 2009). This offense may be applied to cyberbullying when committed through electronic means, although not mentioned. |
| **Hungary** | The Act LXXVIII of 2024 on the Suppression of Internet Aggression entered into force on the 1st of January 2025 and amended existing legislation in a number of areas, introducing new obligations and procedural rules. The provision was added to Act C of 2012 on the Criminal Code to criminalise aggression on the Internet. |
| **Malta** | Criminal Code (Chapter 9) deals with harassment and stalking and, since 2025, cyberstalking and cyberbullying. |
| **Netherlands** | Many forms of cyberbullying of persons, regardless of age, are prosecutable in the Netherlands under the Dutch Criminal Law. Examples include harassment, threat, stalking or doxing (dissemination of personal data for intimidation).<br>Also, the Netherlands introduced in 2015 the School Safety Act, under which schools have the duty to ensure a safe school environment, including anti-bullying measures. |
| **Austria** | Under 'Federal law consolidated: Criminal Code', several articles apply to cyberbullying, e.g. Article 107c - Persistent harassment by means of telecommunication or a computer system, or Article 107a - Persistent persecution/stalking |
| **Poland** | In 2011, Poland incorporated in the Criminal Code the offense of stalking or persistent harassment (art. 190a). Cyberbullying can also be covered by other offenses of the Criminal Code (e.g. offenses of threat, causing impairment to health, insult).<br>Also, Law of 9 March 2023 on amending the act on combating domestic violence and some other acts covers actions undertaken through electronic communication means. |
| **Portugal** | Even though there is no specific legislation on cyberbullying, it can be considered as a crime or combination of crimes under the Portuguese Penal Code (e.g. stalking, disseminating intimate images, publishing unauthorised information, private data or images, defamation, threat, coercion, etc.)<br>Also, the Portuguese Charter on Human Rights in the Digital Age approved by law 27/2021 of 17 May addresses the topic of security in the use of Internet, especially for children and young people. Law No 51/2012 on Student Statute and School Ethics combats school violence. |

| Countries | How cyberbullying is addressed in legislation |
|---|---|
| **Romania** | Several provisions of the Criminal Code may apply to cyberbullying (when committed by electronic means), such as on threats, blackmail and harassment (Articles 206 to 208). The Article on stalking includes the use of 'means of remote communication'. In addition, it can refer to the context of domestic violence (Law no 106/2020 amending and complementing Law no 217/2003).<br>Also, in the Law no 1/2011 on National Education (Legea educației naționale nr. 1/2011), in its consolidated version of August 2018, cyberbullying is addressed in a school context (article 7). |
| **Slovenia** | There is no specific criminal provision for cyberbullying, however, article 134.a of the Slovenian Criminal Code deals with stalking (via electronic means of communication) and Article 143 covers misuse of personal data. |
| **Slovakia** | Cyberbullying is referred under article 360b Dangerous electronic harassment of the Criminal Code (amendment of 2021, effective as of 31.12.2021). |
| **Finland** | Articles in the Penal Code can be applied to cyberbullying when committed online, although not mentioned (e.g. assault, harassing communications, defamation, stalking and coertion).<br>The Pupil and Student Welfare Act rules on the right to student welfare referred to in sectorial acts (basic, upper secondary and vocational education and training). |
| **Sweden** | There are provisions in the Penal Code that criminalise offensive acts when they take place on the internet (e.g. stalking, slander or aggravated defamation, molestation, offensive photography).<br>The Discrimination Act 2008:567 tackles harassment as a form of discrimination.<br>In addition, the School Act (2010:800), Chapter 6-Measures against abusive treatment considers schools and all of their staff responsible for preventing and also investigating all forms of harassment or offensive behaviour. |
| **Iceland** | Provisions under General Criminal Law on violations of personal freedom and personal privacy (Ch. XXII, XXIV and XXV) may be applied to cyberbullying.<br>There are also specific references in the Act on Working Environment, Health and Safety in Workplaces, No. 46/1980 and related Regulation 1009/2015. |
| **Liechtenstein** | Cyberbullying is not defined in its own specific law in Liechtenstein, but it is addressed through various existing laws, similar to how bullying is treated in general, and provisions are applied in its Criminal Code. More particularly, articles 107a-Persistent stalking and 107c-Continuous harassment by way of electronic communication or a computer system were inserted. |
| **Norway** | Cyberbullying can be covered by provisions in the Penal Code, such as harassing conduct (section 266) or violation of privacy (section 267).<br>In addition, The Norwegian Education Act (chapter 12) states the school must have a zero tolerance for violations such as bullying (including cyberbullying), violence, discrimination and harassment. |

*Source: JRC own elaboration based on legislation compiled from national sources.*

### 7.2.2. Cyberbullying behaviours as defined in national legislation

This section presents and analyses articles of national legislation that cover behaviours that, under certain circumstances, can constitute cyberbullying. Here by 'definition' we refer to the text of the articles that either define the phenomenon in general — whether using the term cyberbullying or not — or describe the penalties of specific offenses. In the first case, an explicit definition is provided by the legislation, in the second, the articles describe the actions, impact, aggravating circumstances and penalty without defining the wider phenomenon. For the sake of simplicity, in this section we use the term ‘definition’ in both cases.

Definitions and terms used across EEA countries related to cyberbullying are varied and include, among others, terms like persistent harassment by means of a telecommunication or a computer system, stalking, online violence, obsessive harassment, cyberbullying, cyberviolence, dangerous electronic harassment, harassment stalking. In some cases, there is a differentiation between very specific terms (e.g., between harassment and harassing surveillance/tracking in the case of Cyprus; between school violence and bullying in Greece; between cyberbullying and cyberstalking in Malta; or between psychological violence-bullying and cyber psychological violence-cyberbullying in Romania), while in some other cases a broad term covers actions that may constitute cyberbullying (e.g., work-related violence in Denmark, stalking in Portugal, harassment in Czechia).

As in most cases we have used machine-translated versions of the legal texts, the nuances provided in the original language may be lost in translation and not fully capturing the underlying concepts. We study the definitions not based on the term used (e.g. cyberbullying or persistent harassment) but based on the aspects of cyberbullying present in the definition. Therefore, for the analysis, we map each definition to the key elements underpinning the notion of cyberbullying as consistently identified in our investigation (sections 5.2.1 and 6): harm or aggression, use of technologies, recurrence or repetition, intention, power imbalance, and social context.

In 2016, 14 EU Member States had an official definition of bullying online (Dalla Pozza et al., 2016). From our investigation, we found that currently all the EEA countries include definitions of behaviours related to cyberbullying (e.g., online harassment, stalking, e-violence, defamation) in their legislation, with a majority of them explicitly including the electronic means element. We identified 61 cases extracted from the national legislation which refer to acts that directly or indirectly apply to cyberbullying, and which define the behaviours in legal terms. Out of the 61 definitions, 10 definitions from nine countries use the specific term of cyberbullying or bullying: Denmark, France, Greece, Italy, Lithuania, Malta, Romania, Spain and Iceland. But the observation of the elements present in each definition gives a more nuanced and detailed idea of how cyberbullying is treated in legislation.

Table 12 presents the main characteristics of the 61 identified definitions: term defined (in English language and original language), the language of the source text analysed (some legal texts are offered translated into English by the official national website, or by other sources), the legislative source, and the mapping to the six elements of cyberbullying. The text of the definition, and its source, can be found in the country profiles in  1.

A summary of the analysis is shown in Table 11, which provides the number of countries and definitions that consider each of the six elements of cyberbullying.

**Table 11**. Overview of national legislation definitions in the EEA relevant to cyberbullying in relation to key elements underpinning the notion of cyberbullying

| | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|
| Countries | 30 | 23 | 23 | 19 | 21 | 10 | 11 |
| Definitions | 61 | 37 | 33 | 27 | 32 | 12 | 19 |

*Source: JRC own elaboration.*

**Harm or aggression**: all identified definitions refer to the aggressive nature of the act or its effect on the victim. Examples include references to actions of impairment of a person's lifestyle, impairment of physical or mental health, nuisance, damage, discrimination, ridicule, humiliation, violence, hatred, damage of honour or reputation, bodily or other harm, defamation, threat, privacy violation and violation of rights that can cause fear or terror, intimidation, diminish of dignity and self-respect, anxiety and distress, and self-harm.

**Technology-mediated**: in the majority of the cases (37 cases in 23 countries), technology is mentioned with terms such as 'electronic means', 'computer systems and networks', 'internet', or 'social media'. In our analysis we also considered as a valid reference to technology cases like 'mass media' or 'any method of communication', as we understand it also includes digital means. The absence of explicit references to technology in legislation does not imply that behaviours involving technology are exempt from the law. In fact, in highly digitalised countries, it is reasonable to assume that ICTs are so ingrained in society and everyday life that their use for this purpose is implicitly understood.

**Recurrence** or **repetition** is another key element found in many of the cases (33 cases in 23 countries) with references such as repeated occurrence, persistent, continuous, systematic, lasting, for several times, for a long or prolonged period of time. In one case ('persistent harassment by means of telecommunication or a computer system', Austria) the notion of duration perceptibility is mentioned, and used as an aggravating circumstance to increase the sentence.

**Intention** is mentioned in 27 definitions (in 19 countries) with terms such as intentional, deliberate, having as object, with the aim of, have the purpose, intention or wish, pursuing, in such a way as to cause. In a few additional cases (5), intentionality is implicitly mentioned as a reference to when a person 'continuously impose himself' or 'while knowing or should have known that such conduct causes harassment' or by 'intrusive efforts.' Considering these implicit references as an intention from the perpetrator, this element would be covered by 32 definitions and 21 countries.

**Power imbalance** is rarely explicitly mentioned as such in legislation, although we have identified some cases where real or perceived imbalance of power is mentioned (Greece, Romania). Power imbalance can be inferred by references to specific groups, such as minors or children, pregnant women, persons with disability or minorities and groups with special characteristics (e.g. race, ethnicity, religion, sexual orientation). In addition, imbalance can be implicitly inferred if the offence is committed by two or more persons (examples of such reference include Czechia, France and Malta). Cases where power imbalance is explicitly addressed include references to persons with vulnerability or weakness (France, Malta, Slovenia and Spain), age difference between the offender and the victim (Germany), persons unable to defend themselves (Greece), exploitation of a physical, mental or economic advantage (Poland). In cases of power imbalance, offence is usually aggravated, as for example if against a minor or vulnerable person; cases include legislation in Czechia, France, Germany, Greece, Italy, Malta, Romania, Slovenia and Spain.

**Social dimension**: in our analysis we found some cases (19 cases in 11 countries) where the offense is described in a social context - e.g. school, work, public gathering, family or cohabitation– aligned with some definitions from the literature review which refer to cyberbullying as a socially-embedded phenomenon. One definition ('cyber psychological violence or cyberbullying', Romania) refers the online world as the context in which the act happens: 'exclusion/marginalization of a child in the online space'.

Based on our analysis, one third of the definitions (20) mention at least four out of the six elements we identified as core to cyberbullying, while five definitions only include the element of harm or aggression, not even mentioning the use of technology. However, those legal provisions can be used to fight cyberbullying from legislation. Out of the 60 definitions, three fulfil all six key elements: these are the definition of '[electronic/online] school violence and bullying' (Greece), 'domestic violence [by means of electronic communication]' (Poland), and 'psychological violence - bullying' (Romania).

Other aspects stemming from the analysis include the fact that almost two thirds of definitions come from criminal or penal codes, and one third come from specific legislation (on protection from harassment, anti-discrimination, work-related, prevention of bullying in schools, protection of children's rights, etc.). Also, we observe that the severity of potential consequences for perpetrators often increase when the impact on the victim is more serious, e.g. damage to the victim's health, permanent damage, total incapacity to work, attempt of suicide, suicide or death; examples include cases in Austria, France, Germany, Poland, and Liechtenstein. Finally, some definitions refer to the fact that the act of aggression may be perceived by a large audience (Austria, Croatia, Germany, Portugal), highlighting the amplifying ability of technology to spread aggressive behaviours and their impact.

**Table 12**. Mapping of cyberbullying elements in relevant national legislation (EEA countries)

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Belgium | [online harassment] | term not coined | nl | Law on Electronic Communications | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Bulgaria | [discrimination, violence or hatred by electronic information systems] | [дискриминация, насилие или омраза чрез електронни информационни системи] | en | Criminal Code | ✓ | ✓ |  |  |  |  |  |
| Czechia | harassment | obtěžováním | cs | Anti-Discrimination Act | ✓ |  |  | ✓ | ✓ |  |  |
| Czechia | dangerous stalking | Nebezpečné pronásledování | cs | Criminal Code Act No 40/2009 | ✓ | ✓ | ✓ |  |  | ✓ |  |
| Czechia | defamation | Pomluva | cs | Criminal Code Act No 40/2010 | ✓ | ✓ |  |  |  |  |  |
| Denmark | [defamation] | [ærekrænkelse] | en | Criminal Code | ✓ |  |  |  |  |  |  |
| Denmark | [defamation through mass media] | [Ærekrænkning udbredt gennem indholdet af et massemedie] | en | Criminal Code | ✓ | ✓ |  |  |  |  |  |
| Denmark | offensive behaviour actions [including bullying and sexual harassment] | Krænkende handlinger [herunder mobning og seksuel chikane] | en | Working Environment Authority executive order | ✓ |  | ✓ |  |  |  | ✓ |
| Denmark | work-related violence | Arbejdsrelateret vold | en | Working Environment Authority executive order | ✓ |  |  |  |  |  | ✓ |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Germany | stalking [by means of telecommunications] | Nachstellung | en | Criminal Code | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |  |
| Estonia | harassment stalking | ahistav jälitamine | en | Penal code | ✓ |  | ✓ |  |  |  |  |
| Ireland | Harassment | Harassment | en | Non-Fatal Offences Against the Person Act, 1997 | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Ireland | distributing, publishing or threatening to distribute or publish intimate image | distributing, publishing or threatening to distribute or publish intimate image | en | Harassment, Harmful Communications and Related Offences Act 2020 | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Ireland | distributing, publishing or sending threatening or grossly offensive communication | distributing, publishing or sending threatening or grossly offensive communication | en | Harassment, Harmful Communications and Related Offences Act 2020 | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Greece | [electronic/online] school violence and bullying | [ηλεκτρονική] ενδοσχολική βία και εκφοβισμός | el | Law No. 5029 of 10 March 2023 on Arrangements to prevent and address violence and bullying in schools and other classrooms | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Greece | threat [via telecommunication or electronic mean] | Απειλή | el | Penal code | ✓ | ✓ | ✓ |  |  | ✓ | ✓ |
| Spain | [harassment, incl. through any method of communication] | [acoso, incl. a través de cualquier medio de comunicación] | es | Penal Code | ✓ | ✓ | ✓ |  |  | ✓ | ✓ |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Spain | violence [incl. through any method of communication, cyberbullying] | violencia [incl. la realizada a través de las tecnologías de la información y la comunicación, ciberacoso] | es | Organic Law 8/2021, of 4 June, on the comprehensive protection of children and adolescents against violence | ✓ | ✓ | | | | | |
| France | harassment [in the workplace] | harcèlement [au travail] | fr | Criminal Code | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| France | harassment [through a digital or electronic medium] | harcèlement [par le biais d'un support numérique ou électronique] | fr | Criminal Code | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| France | school harassment/school bullying | harcèlement scolaire | fr | Criminal Code | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Croatia | insult [through computer system or network] | uvreda | hr | Criminal Code | ✓ | ✓ | | | | | ✓ |
| Croatia | libel [through computer system or network] | Kleveta [putem računalnog sustava ili mreže] | hr | Criminal Code | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Italy | cyberbullying | cyberbullismo | it | Law 71 of 29 May 2017 on “Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying” | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Italy | stalking acts | Atti persecutori | it | Penal Code | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cyprus | harassment | Παρενόχληση | el | Law 2021 (L.114(I)/2021) on 'Protection from Harassment and Stalking' | ✓ | | | | ✓ | | |
| Cyprus | harassing surveillance/tracking | Παρενοχλητική παρακολούθηση | el | Law 2021 (L.114(I)/2021) on 'Protection from Harassment and Stalking' | ✓ | ✓ | | | ✓ | | |
| Cyprus | civil offense of harassment and stalking | Παρενοχλητική Παρακολούθηση | el | Law 2021 (L.114(I)/2021) on 'Protection from Harassment and Stalking' | ✓ | ✓ | | | ✓ | | |
| Latvia | persecution | vajāšana | lv | Criminal Code | ✓ | | ✓ | | | I | ✓ |
| Latvia | defamation [in mass media] | neslavas celšana [masu saziņas līdzeklī] | lv | Criminal Code | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Latvia | emotional abuse | emocionāla vardarbība | lv | Law on the protection of children's rights | ✓ | | | | | | |
| Lithuania | psychological violence [incl. bullying] | psichologinis smurtas | lt | Law on Fundamentals of Protection of the Rights of the Child | ✓ | | ✓ | ✓ | ✓ | | |
| Luxembourg | obsessive harassment | harcèlement obsessionnel | fr | Criminal Code | ✓ | | ✓ | ✓ | ✓ | | |
| Hungary | internet aggression | Internetes agresszió | hu | Criminal Code | ✓ | ✓ | | ✓ | ✓ | | |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Malta | cyberbullying | bullying fuq l-internet | en | Criminal Code | ✓ | ✓ |  | ✓ | ✓ | ✓ |  |
| Malta | cyberstalking | segwiment ċibernetiku | en | Criminal Code | ✓ | ✓ |  | ✓ | ✓ | ✓ |  |
| Netherlands | [stalking] | term not coined | nl | Criminal Code | ✓ |  | ✓ |  | ✓ |  |  |
| Netherlands | [harassment] | [belaging] | nl | Criminal Code | ✓ |  | ✓ | ✓ | ✓ |  |  |
| Austria | persistent harassment by means of telecommunication or a computer system | Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems | de | Criminal Code | ✓ | ✓ | ✓ |  |  |  |  |
| Austria | persistent persecution/stalking [by means of telecommunications] | Beharrliche Verfolgung [Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels] | de | Criminal Code | ✓ | ✓ | ✓ |  |  |  |  |
| Poland | domestic violence [by means of electronic communication] | przemocy domowej [za pomocą środków komunikacji elektronicznej] | pl | Law of 29 July 2005 on combating domestic violence | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Poland | persistent harassment. identity theft / stalking | uporczywe nękanie. Kradzież tożsamości | pl, en | Penal Code | ✓ |  | ✓ |  |  |  |  |
| Portugal | stalking | Perseguição | pt | Penal Code | ✓ |  | ✓ |  |  |  | ✓ |
| Portugal | disseminating, through social media, the internet, or other means of broad public dissemination | Devassa através de meio de comunicação social, da Internet ou de outros meios de difusão pública generalizada | pt | Penal Code | ✓ | ✓ |  |  |  |  |  |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Romania | cyberviolence | violența cibernetică | ro | Law no 217/2003 on preventing and combating domestic violence | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Romania | psychological violence - bullying | violență psihologică - bullying | ro | Norms of application of provisions of art. 7 of Law no 1/2011 on National Education | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Romania | cyber psychological violence or cyberbullying | violență psihologică cibernetică sau cyberbullyingul | ro | Norms of application of provisions of art. 7 of Law no 1/2011 on National Education | ✓ | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Romania | harassment | hărțuirea | ro | Criminal code | ✓ | ✓ | ✓ |  |  |  |  |
| Slovenia | stalking [via electronic means of communication] | Zalezovanje [preko elektronskih komunikacijskih] | sl | Criminal Code | ✓ | ✓ | ✓ |  | ✓ | ✓ |  |
| Slovakia | dangerous electronic harassment | nebezpečné elektronické obťažovanie | sk | Criminal Code | ✓ | ✓ | ✓ | ✓ | ✓ |  |  |
| Finland | [harassing communications] Breach of the peace of communication | Viestintärauhan rikkominen | en | Criminal code | ✓ | ✓ | ✓ | ✓ | ✓ |  |  |
| Finland | stalking | Vainoaminen | en | Criminal code | ✓ |  | ✓ |  |  |  |  |
| Sweden | unlawful persecution | olaga förföljelse | sv | Penal Code | ✓ |  | ✓ |  |  |  |  |
| Sweden | harassment | trakasserier | en | Discrimination Act | ✓ |  |  |  |  |  |  |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Iceland | victimisation / [bullying] | Einelti | en | Regulation on measures against victimisation, sexual harassment, gender-based harassment and violence in workplaces | ✓ |  | ✓ |  | ✓ |  | ✓ |
| Iceland | gender-based harassment | Kynbundin áreitni | en | Regulation on measures against victimisation, sexual harassment, gender-based harassment and violence in workplaces | ✓ |  |  | ✓ | ✓ |  | ✓ |
| Iceland | violence | Ofbeldi | en | Regulation on measures against victimisation, sexual harassment, gender-based harassment and violence in workplaces | ✓ |  |  |  |  |  | ✓ |
| Liechtenstein | persistent stalking [by means of electronic communication or by use of other means of communication] | Beharrliche Verfolgung [im Wege einer elektronischen Kommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels] | en | Criminal Code | ✓ | ✓ | ✓ |  |  |  |  |
| Liechtenstein | continuous harassment by way of electronic communication or a computer system | Fortgesetzte Belästigung im Wege einer elektronischen Kommunikation oder eines Computersystems | en | Criminal Code | ✓ | ✓ | ✓ |  |  |  |  |

| Country | Term defined (en)[1] | Term defined (original language)[1] | Source language[2] | Legislative source | Harm / Aggression | Technology-mediated | Recurrence / Repetition | Intention (explicit) | Intention (incl. implicit) | Power imbalance | Social dimension |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Norway | reckless behaviour | Hensynsløs atferd | nb | Criminal Code | ✓ | | | | | | |
| Norway | serious personal persecution | Alvorlig personforfølgelse | nb | Criminal Code | ✓ | | ✓ | | | | |

[1] Note 1: Terms in square brackets are extracted from the article content, but are not used as such in the title of the article.

[2] Note 2: ISO 639-2 code

*Source: JRC own elaboration.*

.

### 7.2.3. Examples of other initiatives

All EEA countries offer awareness and support activities on how to combat cyberbullying. Collaboration between different stakeholders — government bodies, NGOs, academia, private sectors and other stakeholders — is common practice, which is further facilitated by the EU Better Internet for Kids strategy (BIK+) at different levels. All EU Member States are part of the EU Safer Internet initiative supporting the BIK+ strategy and provide services through the Safer Internet Centres (SICs) network. Among other initiatives, the centres provide awareness activities and campaigns such as the Safer Internet Day (SID). In addition, they usually host the Helplines providing a channel for support through the InSafe network and the Hotlines providing a channel to report illegal online activities through the InHope network. In addition to the EU MSs, from the three EFTA countries Iceland has a SIC, Helpline and Hotline, and Norway a SIC and Helpline. All three EFTA countries promote the BIK+ strategy and participate in the SID campaign.

According to the BIK+ latest policy monitor report, in 22 of the 29 reporting countries,[17] safeguarding children's mental health and wellbeing online is an emerging priority (O'Neill et al., 2025). According to our findings, EEA countries promote the development of digital competence as one of the ways to promote a safe and responsible use of digital technologies. There are already education policies and practices to combat cyberbullying at school, at regional and national level, including building of digital competence for both students and teachers, as well as procedures to deal with and report cyberbullying incidents. In most cases, activities against cyberbullying lie under a broader umbrella of digital competence, media literacy and online safety.

According to our analysis, most countries still do not collect data on cyberbullying in a systematic way. However, almost all of them participate in international studies where the topic of cyberbullying is also addressed, such as the EU Kids Online study supported by the European Commission and the Health Behaviour in School-aged Children (HBSC) study supported by the WHO (Cosma et al., 2024). More specifically, we found that 23 EEA countries participated in the EU Kids Online 2010[18] (Sonia Livingstone et al., 2011), 16 in the EU Kids Online 2020[19] (Smahel et al., 2020), and 29 in the most recent HBSC[20] (Cosma et al., 2024).

Half of the countries also conduct national surveys, as for example: Belgium, on media use and media literacy as well as digital practices of children and adolescents; Czechia, on children online behaviour or perceptions of cybercrime; Denmark, on young consumers and social media; Estonia, on bullying on children and adolescents; Greece, on the attitudes and behaviours of children on the internet; Ireland, on online safety; Latvia, on bullying and violence in schools; Lithuania, on problematic usage of internet; Luxemburg, on negative experiences online; the Netherlands, on harmful behaviour online; Portugal, on combatting bullying in schools; Spain, on children and adolescents in digital environments; Sweden, on media usage among children and young people;

[17] All EU Member States plus Norway and Iceland.

[18] EU Kids Online 2010: A survey in 25 EU countries on the internet use, risk experiences and safety mediation of children aged 9-16. Data collected between 2009-2011.

[19] EU Kids Online 2020: A survey in 19 EU countries on the internet use, risk experiences and safety mediation of children aged 9-16. Data collected between 2017-2019.

[20] BSC study: A study conducted every four years among 11-, 13- and 15-year-olds on health behaviours, social determinants and developmental trends in adolescence. The most recent study collected data in 44 countries and regions between 2020-2021.

Iceland, on the welfare and attitudes of children and young people; and Norway, on digital bullying. The 'Media and Information Literacy Index across the Nordic countries' also addresses cyberbullying. (Schofield et al., 2021). Data are usually collected as part of broader surveys, using different methodologies and relying on a variety of definitions, which hinders cross-country comparability.

Examples of national and regional policies and actions in relation to cyberbullying are presented in the country profiles in  1. Overall, EEA countries acknowledge the need to have legislation related to cyberbullying. All of them have policies or initiatives in place to combat cyberbullying, in many cases through digital competence development programmes at schools, and beyond, or by introducing policies and interventions at national, regional or school level.

# 8. Discussion and conclusions

## 8.1. Scientific evidence on cyberbullying

The body of scientific literature on cyberbullying has grown exponentially over the past two decades, with the US, Spain, and China being the most prolific contributors to the production of journal articles on this topic. Researchers affiliated with institutions in all EU Member States have contributed to the authorship of articles addressing cyberbullying. However, the number of articles on cyberbullying varies significantly across EU MSs, with researchers in four countries contributing to the publication of over 100 articles each.

Our review of systematic literature reviews shows that scientific research has focused predominantly on children and young adults, particularly in the context of educational settings, including secondary schools and higher education institutions. Research suggests that certain individuals may be at a greater risk of becoming perpetrators and/or victims of cyberbullying due to various factors, including individual characteristics (e.g., age, gender, personality), social factors (e.g., perceived social support, family dynamics, cultural context), and risky behaviours (e.g., the oversharing of sensitive data). Findings of these studies have been largely indicative, and more research is needed to establish stronger relations between these factors and between them and cyberbullying prevalence and impacts.

The scientific literature indicates that age is a significant predictor of cyberbullying. School-aged individuals are more likely to experience cyberbullying, with victimisation rates increasing with age in parallel to increased technology use and social media engagement (Kasturiratna et al., 2025). However, the relationship between age and cyberbullying is complex, with inconsistent findings reported in the literature (Camerini et al., 2020; Real Fernández et al., 2022), which highlights the need for further research across different age group to fully understand the underlying factors.

There is also evidence on the role of gender as a risk factor for cyberbullying, indicating that females tend to be affected by this phenomenon more often than males (Kasturiratna et al., 2025; Pew Research Center, 2022). Females also seem to experience more severe consequences, including depression, suicidal ideation, and substance use (Biagioni et al., 2023; Díaz-Esterri et al., 2025; Morales-Arjona et al., 2024). In educational settings, girls often experience poorer academic performance and higher levels of school absenteeism due to cyberbullying (Martínez-Monteagudo et al., 2023). Additionally, online gaming environments reveal gender-specific experiences, with men more likely to be victims and perpetrators, and women facing disproportionate levels of sexual harassment (Hu et al., 2025).

Individuals who belong to minority groups — such as racial, ethnic, or sexual minorities — are more likely to experience cyberbullying, with four out of five meta-analyses indicating a higher likelihood of victimisation. Additionally, sexual orientation and gender identity are important predictors of cyberbullying victimization and exposure to online hate material (Fulantelli et al., 2022). Psychological and behavioural risk factors, such as low self-esteem, impulsiveness, and prior victimisation experiences, play a significant role in cyberbullying dynamics (Anichitoae et al., 2025; Morales-Arjona et al., 2024). In addition, traits like forgiveness, empathy, and emotional intelligence can serve as protective factors, reducing the likelihood of involvement in cyberbullying (Quintana-Orts et al., 2021; Zhu et al., 2021).

Furthermore, individual characteristics — such as those in people with intellectual and developmental disorders, obesity, asthma or academically gifted students — may increase the victimisation risk of certain populations (Dorol-Beauroy-Eustache et al., 2021; Martínez-Cao et al., 2021; Martínez-Monteagudo et al., 2023), therefore requiring specific attention and support.

Perceived social support is a crucial protective factor against the negative effects of cyberbullying victimisation, with strong support networks, including family, peers, and school connections, reducing the likelihood of victimisation and buffering against negative psychological outcomes (Castaño-Pulgarín et al., 2022; Kasturiratna et al., 2025). Active parental engagement, including supervision of online activities and fostering open communication, can also help adolescents navigate digital environments more safely, reducing the risk of both perpetration and victimisation (Bussu et al., 2025; Dorol-Beauroy-Eustache and Mishara, 2021).

Certain behaviours and activities (e.g., revealing private information online) can increase the risk of cyberbullying victimisation, while others, like cooperative physical activities, can reduce victimisation and improve aggressive and disruptive behaviours (Kasturiratna et al., 2025; Rusillo-Magdaleno et al., 2024). Being a victim of cyberbullying increases the likelihood of becoming a cyberbully oneself, highlighting the need for further research specifically devoted to this overlap and exchange of roles (Estévez et al., 2020; Lozano-Blasco et al., 2020).

Cyberbullying is frequently linked to traditional bullying, with the two forms of aggression often occurring together (Gefen et al., 2025; Tural Hesapcioglu et al., 2017; WHO, 2022b). In this regard, educational institutions can play a critical role in mitigating cyberbullying, with positive school climates, effective teacher-student engagement, effective school protocols and supervision being key factors in creating safe educational spaces (Kasturiratna et al., 2025; Ng et al., 2022). It is important that educational institutions have mechanisms in place to quickly intervene as soon as signs of cyberbullying are detected, even if the behaviours happen outside their premises and digital ecosystems. While traditional bullying and cyberbullying tend to be deeply intertwined, there is evidence supporting the idea that cyberbullying is a distinct phenomenon that requires separate consideration from traditional bullying, as it has unique relationships with outcome variables such as risk and protective factors (Barlett et al., 2024).

## 8.2. Fighting cyberbullying

In response to the increasing prevalence of cyberbullying, governments, organisations, and stakeholders at international, national, regional, and local levels have introduced numerous initiatives aimed at preventing and mitigating its effects. Beyond Europe, through several resolutions, the UN has called upon States to adopt a multi-faceted approach in the protection of children and persons with disabilities from cyberbullying (UN General Assembly, 2019, 2023, 2024).

While cyberbullying continues to increase, all countries in the EU provide awareness and support activities to combat cyberbullying, often through collaboration between governments, NGOs, academia, and private sectors. The EU's Better BIK+ strategy and Safer Internet initiative facilitate these efforts, with all EU MSs participating and providing services through the Safer Internet Centres network, which offers awareness campaigns, helplines for support, and hotlines for reporting illegal online activities.

European legislation — including the GDPR, DSA, AVMSD, AI Act, and other regulations — covers aspects relevant to the fight against cyberbullying, while institutional bodies across the European Economic Area (EEA) countries (the 27 EU MSs plus three EFTA states — Norway, Iceland and Liechtenstein) are pursuing legislation and policies to prevent its spread and ensure safe online environments. In all EEA countries, bullying or cyberbullying aspects can be covered to a certain extent under their criminal justice, and half of them cover cyberbullying through laws on specific contexts, population groups or topics (education, workplace, minors, domestic violence, discrimination, etc.).

Systematic reviews of scientific literature on the effectiveness of interventions aimed at tackling cyberbullying suggest that different kinds of initiatives can be effective, even though the reported effect sizes tend to be moderate at best. Effective interventions address the specificities of cyberbullying and consider the concrete needs of different populations, such as primary school students (Chicote-Beato et al., 2024) or adolescents (Ng et al., 2022; Polanin et al., 2022). Programmes that include educational/informational and skills development components are more effective than those that focus exclusively on cognitive/behavioural components (Henares-Montiel et al., 2023; Lan et al., 2022). In general, school-based interventions tend to be effective, while findings are inconclusive for home-based interventions (Doty et al., 2022; Kasturiratna et al., 2025).

Active parental participation may contribute to better outcomes, while longer duration of an intervention does not necessarily lead to higher effectiveness: in some cases, shorter interventions can be equally (or even more) effective than longer ones (Doty et al., 2022; Ng et al., 2022; L. Wang et al., 2023). This should be taken into account when assessing the cost-effectiveness of the intervention.

## 8.3. Key elements underpinning the notion of cyberbullying

The lack of a universally accepted definition of cyberbullying is an important barrier to both research and policymaking, hindering the development of accurate measures of cyberbullying and the design of effective interventions (Bauman, Cross et al., 2013; Chun et al., 2020; Ray et al., 2024; W. Zhang et al., 2022). However, there are several key elements underpinning the characterisation of this phenomenon as described in the scientific literature, policy documents, and legislation. A standard definition should be concise, comprehensive and integrate those elements.

Cyberbullying, like traditional bullying, is a type of hostile or aggressive behaviour that exposes victims to harmful experiences repeatedly and over time. Another specificity is that the perpetrator takes advantage of some form of power imbalance, whether real or perceived. At the same time, it is characterised by some specificities that set it apart from traditional bullying, even though both phenomena tend to be interlinked and often simultaneously affect individuals. Indeed, there is scientific evidence pointing to unique relationships with outcome variables, such as risk and protective factors, and that traditional bullying victimisation and perpetration do not fully explain cyberbullying (Barlett et al., 2024).

Likewise, cyberbullying can be conceptualised as a form of aggressive or hostile behaviour that is distinct from other types of violence that are also mediated by digital technology. In other words, not all forms of violence involving the use of information and communication technologies can be regarded as instances of cyberbullying. In this regard, WHO (2022b) identifies 'sexual exploitation and abuse' (e.g., 'online grooming') and 'cyber-aggression and cyber-harassment'[21] (e.g., 'cyberbullying') as two separate domains, even though they may intersect in some cases. For example, cyberbullying may involve nonconsensual sexting and sexual extortion, while hate speech

[21] Online harassment is also used in other publications (Pew Research Center, 2022) as a synonym of cyberbullying.

disseminated through digital means would only constitute cyberbullying when targeted at specific individuals and meeting other criteria, as determined by the elements we have identified.

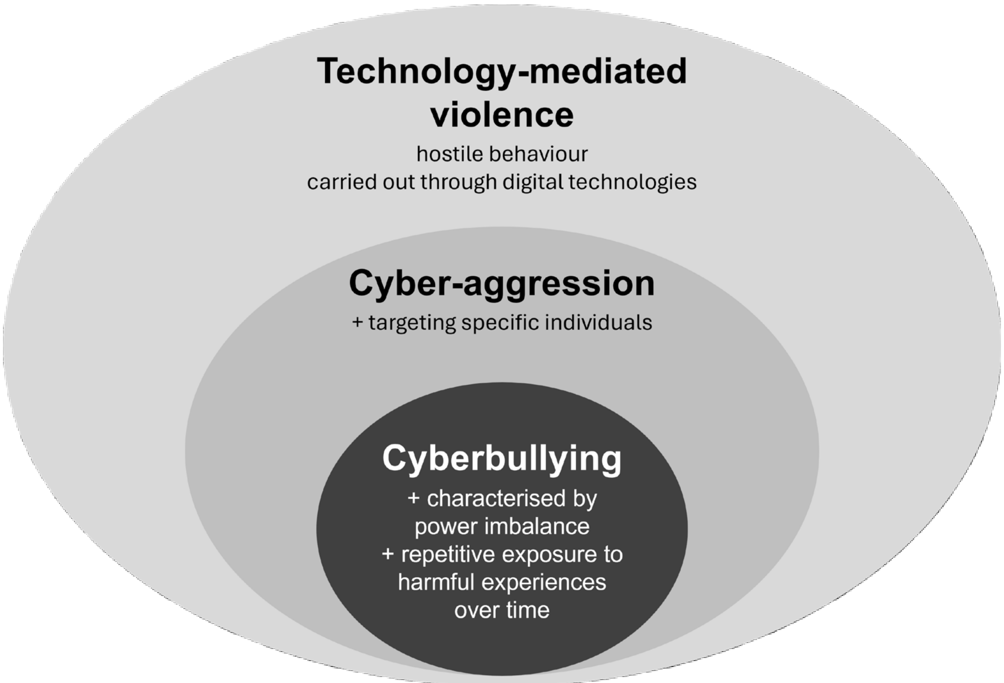
Cyberbullying can be regarded as a specific type of cyber-aggression, a wider phenomenon that has been defined as “intentional behavior aimed at harming another person or persons through computers, cell phones, and other electronic devices, and perceived as aversive by the victim” (Schoffstall et al., 2011, p. 588). Whereas cyberbullying is associated with harmful experiences triggered by the actions of an individual or group of aggressors who often intend to cause suffering in the victims, the intentional nature of harm in cyberbullying has been contested, as in some cases it might be primarily driven by other motivations.

Cyberbullying can take many different forms of behaviour, from direct threats and aggressions to more subtle practices aiming to harm victims in other ways. These include various forms of actions and interactions, some of which might be illegal under certain jurisdictions.

Some definitions have also emphasised that cyberbullying, like bullying in general, is a socially-situated phenomenon (O’Higgins Norman et al., 2025). This means that it is enabled, or otherwise constrained, by social, cultural and institutional factors at play. Moreover, it tends to happen within the boundaries of well-defined communities or social units, whether formal (e.g., educational institutions) or informal (e.g., online games)

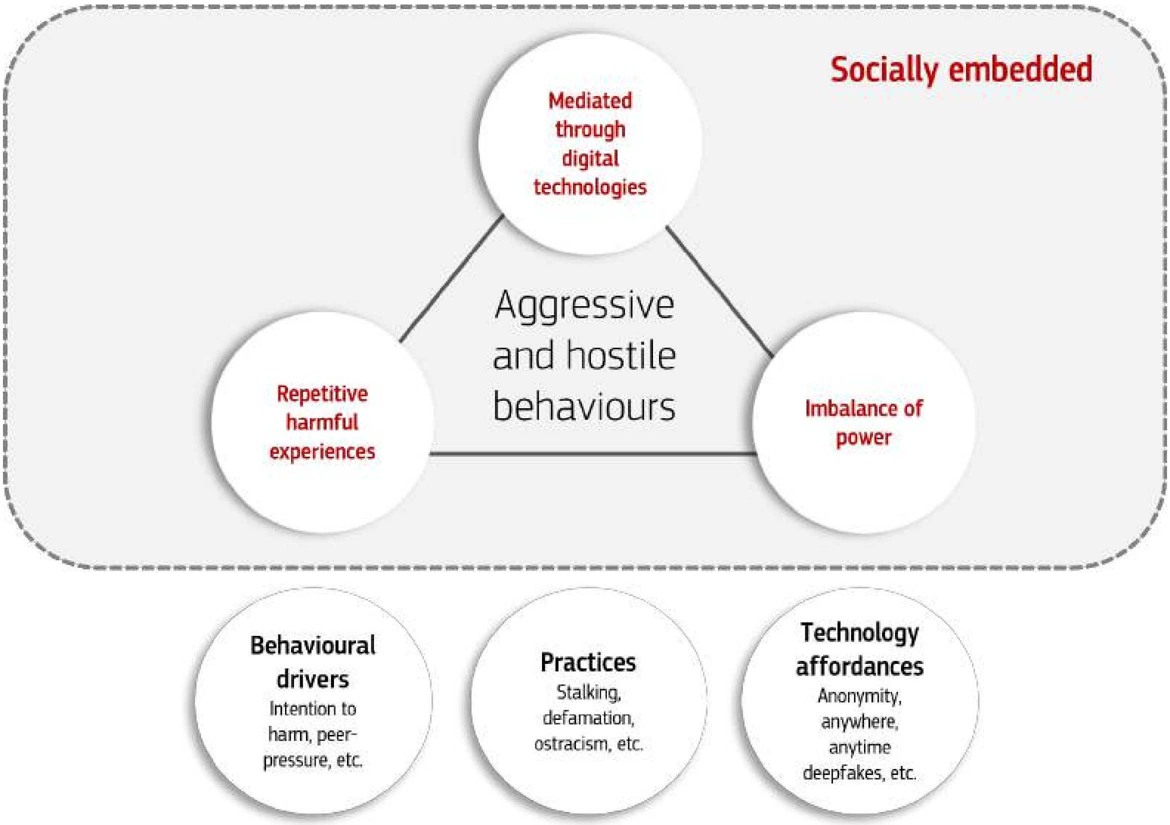
Figure 15 identifies the specificities of cyberbullying, as compared to the wider domain of cyber-aggression and the overall realm of violence involving digital technology. Figure 16 offers a more detailed view of the core elements that should be considered while formulating a specific and comprehensive definition of cyberbullying. Our research identifies the following key aspects: aggressive or hostile behaviour mediated through (digital) technologies, targeted at specific individuals, socially embedded into formal or informal communities, characterised by a form of power imbalance, and involving repetitive exposure to harmful experiences.

**Figure 15.** Specificities of cyberbullying as a form of cyber-aggression and technology-mediated violence


Technology-mediated violence
hostile behaviour
carried out through digital technologies
Cyber-aggression
+ targeting specific individuals
Cyberbullying
+ characterised by power imbalance
+ repetitive exposure to harmful experiences over time

*Source: JRC own elaboration.*

**Figure 16.** Key elements of cyberbullying


Socially embedded
Mediated through digital technologies
Aggressive and hostile behaviours
Repetitive harmful experiences
Imbalance of power
Behavioural drivers
Intention to harm, peer-pressure, etc.
Practices
Stalking, defamation, ostracism, etc.
Technology affordances
Anonymity, anywhere, anytime deepfakes, etc.

*Source: JRC own elaboration.*

Table 13 illustrates how the elements underpinning the notion of cyberbullying have been incorporated into definitions formulated in the context of scientific research, policymaking and legislation.

**Table 13**. Key elements underpinning the notion of cyberbullying: examples from scientific publications, policy documents and national legislation

| Elements | Scientific documents | Policy documents | National legislation |
|---|---|---|---|
| **Aggressive and hostile nature of the behaviour** | "*harm* inflicted" (Patchin et al., 2006, p. 152)<br>"*hostile* or *aggressive* messages intended to inflict *harm* or *discomfort* on others" Tokunaga (Tokunaga, 2010, p. 278)<br>"online *aggression* or *harassment* and repeated *threats*" (Ray et al., 2024, p. 6):<br>"physical, social, and emotional *harm*" | "to bully (*harass*, *threaten*, *embarrass*, or target) another person (EC: DG EAC, 2024a, pp. 32–33)<br>"*Unwanted*, *aggressive* behaviour" (UNICEF, 2018, p. vi)<br>"verbal *aggression*, *threats*, *hostility*, and other attempts to cause *harm*" (WHO, 2022b, p. 7) | "to cause *nuisance* to their correspondent or to cause *damage*" (Belgium, Criminal Code Art. 145.3bis)<br>"propagates or incites *discrimination*, *violence* or *hatred*" (Bulgaria, Criminal Code Art. 162)<br>"Any form of physical, verbal, psychological, emotional, social, racist, sexual, electronic, online or other *violence* and |

| Elements | Scientific documents | Policy documents | National legislation |
|---|---|---|---|
| | (O'Higgins Norman, 2024, p. 4) | | delinquent behaviour" (Greece, Law 5029 Art. 4)<br>"Whoever intentionally, through an electronic communication service, computer system or computer network, significantly *impairs* the quality of life of another person" (Slovakia, Criminal Code, Art. 360b |
| **Digital/electronic technologies** | "the medium of *electronic text*" (Patchin et al., 2006), "*electronic* forms of contact" (Smith et al., 2008)<br>"*electronic* or *digital media*" (Tokunaga, 2010)<br>"*electronic means* or devices" (Chun et al., 2020)<br>"*Information* and *Communication Technologies*" (W. Zhang et al., 2022)<br>"*technology*" (Ray et al., 2024). | "use of *technology* to bully" (EC: DG EAC, 2024a, pp. 32–33)<br>"*electronic technologies* in order to bully another person through the *Internet*" (Council of Europe, n.d.)<br>"*online communications*" (WHO, 2022b, p. 7)<br>"*texting*, *emails*, *social media* or other *online channels*." (UNICEF, 2018, p. vi) | "Persistent harassment by means of *telecommunication* or a *computer system*" (Austria, Criminal Code Art. 107c)<br>"[use of] an *electronic communications network* or service or other *electronic communications* means..." (Belgium Criminal Code Art. 145.3bis)<br>"via an *electronic communications network*" (Hungary, Criminal Code, Art. 332A<br>"actions that are carried out through the *internet*, *computer*, *tablet*, *mobile phone* ... any *technology-mediated* behaviour, identified in the space of *social media*, *websites*, *messaging*." (Romania, Law 106/2020, Art. 4.1h) |
| **Recurrence** | "repeated harm" (Patchin and Hinduja, 2006, p. 152)<br>"repeatedly and over time" (Smith et al., 2008, p. 376)<br>"repeatedly communicates hostile or aggressive messages" (Tokunaga, 2010, p. 278) | "the behaviour is *repeated*, or has the *potential to be repeated*, *over time*" (Council of Europe, n.d.)<br>"involves a *repeated pattern* of physical, psychological or social aggression" (UNICEF, 2018) | "for a *prolonged* period of time" (Austria, Criminal Code Art. 107c)<br>"through *repeated* comments or behaviours" (France, Criminal Code Art. 222-33-2)<br>"the systematic or intentional or *repeated* threat and insult to the personality, physical integrity or mental |

| Elements | Scientific documents | Policy documents | National legislation |
|---|---|---|---|
| | | | balance of students" (Greece, Law 5029 Art. 4)<br>"*repeatedly* observing, pursuing or intrusive efforts to establish direct contact or contact via electronic means of communication and thereby causes fear or danger in that person or a close relative" (Slovenia, Criminal Code, Art. 134a) |
| **Intentionality** | "*intentional* act" (Smith et al., 2008, p. 376)<br>"*intended* to inflict harm or discomfort on others" (Tokunaga, 2010, p. 278)<br>"*intentional* aggression" (Kowalski et al., 2014);<br>"*willful* and repeated harm" (Hinduja and Patchin, 2006, p. 152) | "the three core elements of bullying—power imbalance, *intent* to harm, and repetition—are recognised in cyberbullying" (European Commission. Directorate General for Education, Youth, Sport and Culture, 2024, p. 33). | "*intended* or resulting in a deterioration of their living conditions" (France, Criminal Code Art. 222-33-2)<br>"the systematic or *intentional* or repeated threat and insult to the personality, physical integrity or mental balance of students" (Greece, Law 5029 Art. 4)<br>"whose *intentional* and predominant purpose is to isolate a minor or a group of minors by committing serious abuse, a harmful attack, or ridicule them." (Italy, Law 71/2017, Art. 1.2)<br>"with *intention* to cause physical or mental harm to another person" (Malta, Criminal Code, Art. 251BC) |
| **Power imbalance** | "cyberbullies have some perceived or actual *power* over their victims" (Patchin and Hinduja, 2006, p. 152)<br>"victim who *cannot* easily *defend* him or herself" (Smith et al., 2008, p. 376)<br>"an *imbalance* of *power*" (Kowalski et al., 2014) | "involves a real or perceived *power imbalance*" (Council of Europe, n.d.)<br>"characterized by an *imbalance* of *power* or *strength*." (UNESCO, 2024, p. 16) | "unwanted, aggressive behaviour that occurs between school-age children and the corresponding behaviour of teachers that includes a real or perceived *imbalance of power* (Greece, Law 5029 Art. 4)<br>"in a social context that is difficult to avoid, committed intentionally, which involve an |

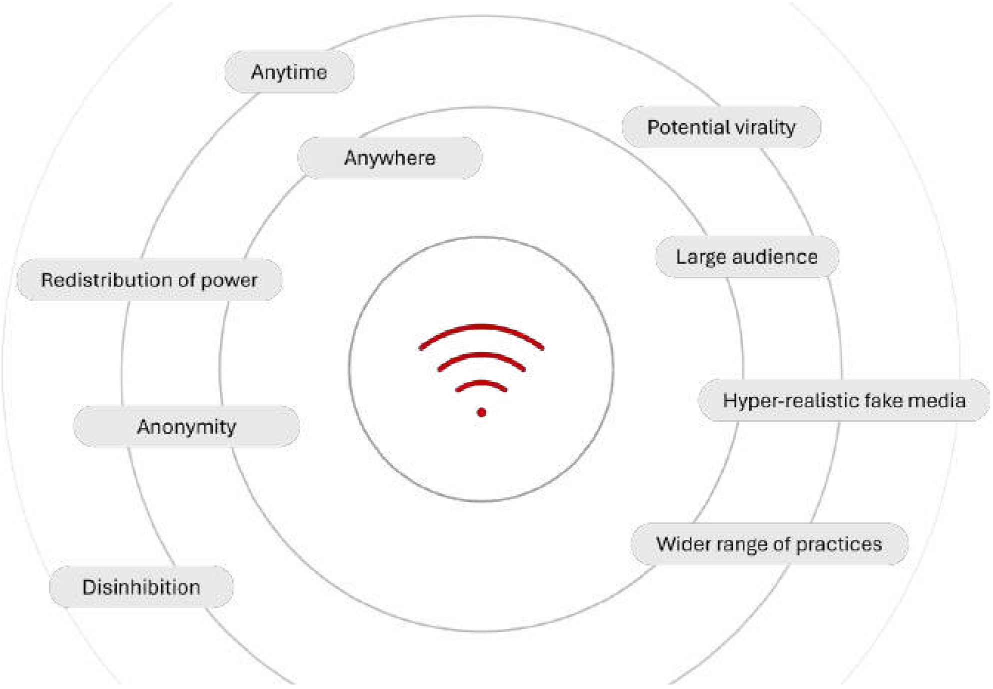
| Elements | Scientific documents | Policy documents | National legislation |
|---|---|---|---|
| | | | *imbalance of power...*" (Romania, Law 1/2011) |
| **Social dimension** | "carried out by a group or individual" Smith et al. (2008, p. 376)<br>"a *social process* that is characterized by an imbalance of power driven by social (*societal*) and *institutional* norms" (O'Higgins Norman, 2024, p. 4). | "exclusion by intentionally *excluding* a person from a group" (EC: DG EAC, 2024a, pp. 32–33)<br>"Bullying is characterized by an imbalance of power or strengths driven by *societal* and *institutional norms*" (UNESCO, 2024, p. 16) | "violent exclusion of students either from the educational process or from their participation in daily school life, as well as the social exclusion, threats and psychological violence in students' contacts with their classmates" (Greece, Law 5029 Art. 4)<br>"offensive behaviour is defined as a situation where one or more persons grossly or several times expose one or more other persons in the company to bullying, sexual harassment or other degrading behaviour in the workplace" (Denmark, The Working Environment Authority Executive Order, sect. 23)<br>"prohibition of any action that could endanger the physical or psychological health and wellbeing of children in schools" (Romania, Law 1/2011) |

*Source: JRC own elaboration.*

The growing popularity of digital platforms and tools that enable new forms of communication and networked interactions (e.g., social media, messaging apps, online multiplayer video games) has also facilitated new forms of technology-mediated aggression and harassment, contributing to a higher prevalence of cyberbullying victimisation and perpetration (Giumetti et al., 2022). Conceptualisations of cyberbullying encompass many aspects that were already present in traditional bullying, but the incorporation of digital technologies introduces additional complexity to the behaviours and social interactions that characterise this type of abusive behaviour, as summarised in Figure 17.

The ability to create and disseminate **user-generated content** and the possibility to respond in real-time to attacks not only facilitates the perpetrators' actions but also allows cyberbullying victims to retaliate and become perpetrators themselves. At the same time, bystanders or witnesses may inadvertently pass along cyberbullying messages or respond in ways that are harmful to a victim (Kowalski et al., 2012). Moreover, emerging technologies such as GenAI introduce new forms of harm, for instance through the creation of hyper realistic synthetic media content (i.e., deepfakes) that can damage reputations and may lead to psychological trauma (Alexander, 2025; Vaccari et al., 2020).

**Figure 17.** Key technology affordances differentiating cyberbullying from traditional bullying



*Source: JRC own elaboration.*

Digital technologies have significantly redefined the **spatial and temporal boundaries** that traditionally separated different realms of life, such as work vs. personal life, public vs. private spaces, and online vs. offline environments. The implication of these changes for bullying is that harm can be experienced from anywhere and anytime (Anichitoae et al., 2025; EC: DG EAC, 2024a; Hinduja et al., 2009; Li et al., 2024). Moreover, while an act of aggression in a physical space is limited in time and place, in the context of cyberbullying offensive messages may remain online for extended periods as they are difficult to delete once distributed, potentially reaching large audiences and, in some cases, even going viral and being reposted by others indefinitely (Slonje et al., 2008).

Consequently, while **repetitive acts** of aggression are a common characteristic of cyberbullying, they are not a strict requirement, given that a single action (e.g., posting content online) might be deliberately planned to exploit the potential for mass distribution of social networks, causing harm to the victim through an exposure to harmful events over time. Therefore, a comprehensive definition of cyberbullying should focus on the frequency with which a victim experiences harmful behaviour, rather than solely on the number of repetitive actions taken by the perpetrator.

Online aggression can occur at any time of day, regardless of the victim’s location and does not require co-presence of victim and perpetrator. Cyberbullies may also reach larger communities with their actions and, by doing so, amplify the effects on victims and bystanders (Lo Cricchio et al., 2021; Zheng et al., 2025). In the BIK study, during consultations with numerous stakeholder groups, including children, participants mentioned bullying and trolling as significant problems with harassment often starting in class and continuing online (Verdoodt et al., 2025).

**Anonymity** is a significant affordance of online technologies that may enable aggressive behaviours associated with cyberbullying. The potential for anonymous interactions in digital environments can embolden individuals to engage in behaviours they might not exhibit in face-to-face interactions, including engaging in aggressive or abusive behaviour, contributing to the phenomenon of 'online disinhibition' (Barlett et al., 2016; Kim et al., 2023; L. Wang et al., 2024). Furthermore, online interactions can contribute to moral disengagement, decreased empathy, and inadequate awareness of the consequences of one's actions, facilitating cyberbullying (Ray et al., 2024; L. Wang et al., 2024; Zammit, 2025).

Anonymity can also make it difficult for victims to identify their perpetrators, to confront their aggressors or defend themselves (Barlett et al., 2022; Peter et al., 2018; Wegge et al., 2016), exacerbating the emotional distress and sense of vulnerability associated with cyberbullying.

Additionally, the ability to attack victims anonymously can provide a sense of protection to perpetrators who might otherwise be reluctant to engage in bullying behaviour (Barlett et al., 2016; Polanin et al., 2022; Vandebosch et al., 2008). Moreover, the possibility to use fake profiles or online personas may facilitate the manipulation and deception of victims, as well as the spreading of false information, rumours and sensitive content (L. Wang et al., 2024).

Some researchers suggest that digital technologies also reshape the notion of **intentionality**, as the main motivation behind the aggressive behaviour may not be to cause harm, but other socially related drivers, such as peer pressure. For example, research by Kowalski and Limber (2007) found that a significant percentage of cyberbullying perpetrators were friends or siblings, which raises questions about the extent to which the harm is intentional or not, as well as on whether they should be classified as cyberbullying or another type of violence. Additionally, the characteristics of online interactions, such as the lack of verbal and visual cues, can make it difficult to determine the intent behind cyberbullying behaviours (Cassidy et al., 2013; Dennehy et al., 2020; O'Higgins Norman et al., 2025).

The use of technology redefines the **distribution of power** across those involved in cyberbullying behaviour. While in traditional bullying the concept of power imbalance may be determined by physical attributes (e.g., size, strength) or social influence (e.g., 'popularity', number of friends), in cyberbullying it can also depend on unequal levels of digital competence or access to technology and content (e.g., photos or videos). In other words, "who have 'power' in offline spaces might not be the same who have power in virtual spaces" (Gottschalk, 2022, p. 10). It is also worth highlighting that cyberbullying can occur between children (e.g., pupil to pupil), children and adults (e.g., teacher to student or student to teacher) or adults and adults (e.g. employer to employee).

There is a wide and growing **range of aggressive or hostile behaviours** that can be characterised as cyberbullying. Some of these behaviours involve harassment, stalking, defamation, denigration, extorsion, impersonation, hate speech or social exclusion, just to mention a few of the hostile practices reported in the literature (Myers et al., 2019; Teng et al., 2024). Emerging examples of cyberbullying include, for example, multiplayer online video games where players can be more disinhibited to verbally bully one another or may use their character to denigrate their opponents (O'Higgins Norman et al., 2025). While our research has identified some of these behaviours, integration and consultation with young people will ensure that new emerging online practices are identified and hence, researched and addressed when combating cyberbullying.

In some cases, it can be challenging, especially for young people, to realise that certain behaviours are not only harmful, but also illegal (e.g., posting certain content online). Indeed, what starts as behaviour perceived by aggressors as less severe could escalate, for instance driven by peer-pressure, and result in **unlawful actions**. In this regard, considering the prevalence of cyberbullying among young populations, some authors have warned about the risk of criminalising children (Gottschalk, 2022; Livingstone et al., 2020). Moreover, what constitutes illegal cyberbullying can vary by jurisdiction.

The term cyberbullying refers to a wide and rapidly evolving spectrum of hostile technology-mediated practices and behaviours, which makes it extremely challenging to propose a definition that is comprehensive, accurate and stable over time. However, establishing a standardised definition is essential for the comparison of studies, evaluation of interventions, and accumulation of evidence. Such a definition should mention:

- The hostile and aggressive nature of this behaviour, so that it can cover a wide spectrum of practices.
- Power imbalance, as it is a crucial factor that differentiates cyberbullying from other forms of violence.
- Specific individuals targeted as victims, to differentiate it from other forms of violence directed towards collectives.
- Digital information and communication technology as a general concept, to ensure it remains current in the face of emerging technologies and rapidly evolving behaviours.
- Intentional harm, but also harm as a result of actions that are not primarily driven by the desire to cause suffering, so that it covers a diverse range of motivations.
- Exposure of victims to harmful experiences repeatedly and over time, to differentiate it from other forms of aggression.
- The social and cultural dimension of the phenomenon, as it takes place within the boundaries of institutions or informal communities with norms and values that can facilitate or hinder this phenomenon.

# 9. Recommendations

This report informs policy stakeholders on the research and policy work that has been conducted to date in the context of cyberbullying. This work is conducted in the context of the upcoming Action Plan on cyberbullying.

Based on our scientific analysis, we propose the following recommendations with the aim of supporting policy efforts and research to tackle this growing issue effectively.

1. Outline a comprehensive definition of cyberbullying that distinguishes this behaviour from other practices taking into account:

   (a) the role of digital technology while avoiding references to specific types of technologies (i.e., systems, applications or devices) and behaviours, to mitigate the risk of becoming quickly outdated;

   (b) cyberbullying behaviour as a form of aggression or hostility directed towards specific individuals;

   (c) power imbalance as a defining element that — whether perceived or real — enables the behaviour of perpetrators;

   (d) that cyberbullying might be driven by different motivations in addition to the intention to harm the victims (e.g., peer-pressure, dark leisure).

   (e) a wider interpretation of the 'repetitive' nature of the behaviour, including the of exposure to harmful experiences repeatedly and over time, as opposed to just limited to the frequency of attacks.

   (f) That cyberbullying is a socially embedded phenomenon that may be enabled or limited by community factors.

   To make such a definition operational, it would be advisable to complement it with an interpretation of the different components, including examples of specific behaviours and actions that can typically constitute cyberbullying. This could enable the design of standardised research instruments that can support the monitoring of this phenomenon.

   Additionally, the definition should be subjected to validation by scientific experts and stakeholders from different domains (including education, healthcare, psychology, social sciences, technology, policymaking, legal, etc.). This will ensure that the definition is applicable across domains, to achieve effectiveness for measurement, monitoring, interventions and evaluation of actions aimed at tackling cyberbullying.

2. Support initiatives aimed at reducing the prevalence and negative effects of cyberbullying. Their design and implementation should be informed by the following considerations:

   (a) To draw on insights from scientific research for the design of programmes.

   (b) To include actions addressing the specificities of cyberbullying to improve the effectiveness of interventions, while also taking into account the overlap that often exists between bullying and cyberbullying.

   (c) To combine strategies that are designed on protective factors (e.g. awareness raising, provision of training, etc) aimed at both preventing people from becoming cyberbullying perpetrators and protecting victims and bystanders.

(d) To choose programme typologies in line with contextual factors and needs.

(e) To adopt a multi-stakeholder approach involving victims, aggressors, families, educational institutions, health systems, local authorities, charities and the police, among others relevant actors;

d) (f) To consult and listen to the views and experiences of young people and vulnerable population groups, given the rapid change of practices and technologies.

(f) To monitor and evaluate the impact and effectiveness of interventions with the help of standardised and validated research instruments based on the operationalisation of the commonly agreed definition of cyberbullying.

(g) To foster coordinated strategies to maximise the benefits of research and policy efforts across the EU.

(h) To carefully consider the duration of interventions in the light of existing evidence, since in some cases shorter interventions can be more cost-effective while being equally effective.

3. Nurture responsible technology design that limits opportunities for cyberbullying, e.g. encouraging community-building features in game design, provide effective and easy to find reporting mechanisms.

4. Foster further research in support of a stronger evidence base that can help improve the effectiveness of policies and interventions against cyberbullying that include:

(a) Standardised research instruments that allow for cross-country comparability and analysis, examining the effectiveness of interventions in the long term.

(b) In-depth qualitative studies, including ethnographic approaches to better understand how cyberbullying manifests in different social contexts, its impact on individuals and communities and how it could be avoided.

(c) An EU wide systematic monitoring, preventing and reporting cyberbullying, ensuring that these instruments are inclusive and adaptable to diverse demographics.

(d) Further examination of the individual and social factors that might enhance or reduce the likelihood of being involved in cyberbullying, as perpetrators, victims and a dual role (given some current research present some conflicting results) and understanding how to use this knowledge to reduce prevalence.

(e) Cyberbullying in under-researched populations, with attention to particularly vulnerable population groups.

## References

Ademiluyi, A., Li, C. and Park, A. (2022), ‘Implications and Preventions of Cyberbullying and Social Exclusion in Social Media: Systematic Review’, *JMIR FORMATIVE RESEARCH*, Vol. 6, Issue 1, https://doi.org/10.2196/30286.

Agustiningsih, N., Yusuf, A. and Ahsan, A. (2024), ‘Relationships Among Self-Esteem, Bullying, and Cyberbullying in Adolescents A Systematic Review’, *JOURNAL OF PSYCHOSOCIAL NURSING AND MENTAL HEALTH SERVICES*, Vol. 62, Issue 5, https://doi.org/10.3928/02793695-20231013-01.

Alexander, S. (2025), ‘Deepfake Cyberbullying: The Psychological Toll on Students and Institutional Challenges of AI-Driven Harassment’, *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, Vol. 98, Issue 2, pp. 36–50, https://doi.org/10.1080/00098655.2025.2488777.

Anichitoae, F., Dobrean, A., Georgescu, R. and Roman, G. (2025), ‘Association between self-related cognitions and cyberbullying victimization in children and adolescents: A systematic review and meta-analysis’, *AGGRESSION AND VIOLENT BEHAVIOR*, Vol. 80, https://doi.org/10.1016/j.avb.2024.102021.

Aria, M. and Cuccurullo, C. (2017), ‘bibliometrix : An R-tool for comprehensive science mapping analysis’, *Journal of Informetrics*, Vol. 11, Issue 4, pp. 959–975, https://doi.org/10.1016/j.joi.2017.08.007.

Aromataris, E., Fernandez, R., Godfrey, C. M., Holly, C., Khalil, H. et al. (2015), ‘Summarizing systematic reviews: methodological development, conduct and reporting of an umbrella review approach’, *JBI Evidence Implementation*, Vol. 13, Issue 3, p. 132, https://doi.org/10.1097/XEB.0000000000000055.

Bansal, S., Garg, N. and Singh, J. (2023), ‘Perpetrators’ perspective on cyberbullying: a qualitative systematic review with bibliometric analysis’, *LIBRARY HI TECH*, https://doi.org/10.1108/LHT-06-2023-0265.

Barlett, C. P., Gentile, D. A. and Chew, C. (2016), ‘Predicting cyberbullying from anonymity.’, *Psychology of Popular Media Culture*, Vol. 5, Issue 2, Educational Publishing Foundation, p. 171, http://dx.doi.org/10.1037/ppm0000055.

Barlett, C. P., Kowalski, R. M. and Wilson, A. M. (2024), ‘Meta-analyses of the predictors and outcomes of cyberbullying perpetration and victimization while controlling for traditional bullying perpetration and victimization’, *Aggression and Violent Behavior*, Vol. 74, p. 101886, https://doi.org/10.1016/j.avb.2023.101886.

Barlett, C. P., Roth, B. R. and Rinker, A. M. (2022), ‘Muscles, popularity, social capital, and computer skills: Examining “power” in cyberbullying’, *Aggressive Behavior*, Vol. 48, Issue 6, pp. 608–615, https://doi.org/10.1002/ab.22047.

Bauman, S., Card, N. A. and Underwood, M. K. (2013), ‘Definitions: Another Perspective and a Proposal for Beginning with Cyberaggression’, in: Bauman, S., Cross, D. and Walker, J. L. (eds), *Principles of cyberbullying research: definitions, measures, and methodology*, Routledge, New York, N.Y, pp. 73–78, https://doi.org/10.4324/9780203084601.

Bauman, S., Cross, D. and Walker, J. L. (eds) (2013), *Principles of cyberbullying research: definitions, measures, and methodology*, Routledge, New York, N.Y, https://doi.org/10.4324/9780203084601.

Bertoni, E., Centeno, C. and Cachia, R. (2025), 'Social media usage and adolescents' mental health in the EU', European Commission, Ispra, https://publications.jrc.ec.europa.eu/repository/handle/JRC141047.

Biagioni, S., Baroni, M., Melis, F., Baldini, F., Menicucci, D. et al. (2023), 'Cyberbullying Roles and the Use of Psychoactive Substances: A Systematic Review', *ADOLESCENT RESEARCH REVIEW*, Vol. 8, Issue 4, pp. 423–455, https://doi.org/10.1007/s40894-023-00205-z.

Blasko, Z. and Castelli (2022), 'Social media use and loneliness.', EUR 31092 EN, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/700283.

boyd, danah (2014), *It's complicated: the social lives of networked teens*, Yale University Press, New Haven.

Buelga, S., Cava, M., Ruiz, D. and Ortega-Barón, J. (2022), 'Cyberbullying and suicidal behavior in adolescent students: A systematic review', *REVISTA DE EDUCACION*, Issue 397, pp. 43–68, https://doi.org/10.4438/1988-592X-RE-2022-397-539.

Bussu, A., Pulina, M., Ashton, S., Mangiarulo, M. and Molloy, E. (2025), 'Cyberbullying and cyberstalking victimisation among university students: A narrative systematic review', *INTERNATIONAL REVIEW OF VICTIMOLOGY*, Vol. 31, Issue 1, pp. 59–90, https://doi.org/10.1177/02697580241257217.

Cachia, R., Villar Onrubia, D., Barreda Angeles, Economou, A. and López Cobo, M. (2025), 'Cyberbullying: Considerations towards a common definition', No JRC143340, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2760/7772296.

Camerini, A., Marciano, L., Carrara, A. and Schulz, P. (2020), 'Cyberbullying perpetration and victimization among children and adolescents: A systematic review of longitudinal studies', *TELEMATICS AND INFORMATICS*, Vol. 49, https://doi.org/10.1016/j.tele.2020.101362.

Cassidy, W., Faucher, C. and Jackson, M. (2013), 'Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice', *School Psychology International*, Vol. 34, Issue 6, pp. 575–612, https://doi.org/10.1177/0143034313479697.

Castaño-Pulgarín, S., Millán, K., Echavarría, A., Mendoza, C. and Parra, M. (2022), 'Perceived Social Support and Risk of Cyberbullying in Adolescents: A Systematic Review', *QUALITATIVE REPORT*, Vol. 27, Issue 7, pp. 1290–1304, https://doi.org/10.46743/2160-3715/2022.5039.

Chen, M., Cheung, A. S. Y. and Chan, K. L. (2019), 'Doxing: What Adolescents Look for and Their Intentions', *International Journal of Environmental Research and Public Health*, Vol. 16, Issue 2, p. 218, https://doi.org/10.3390/ijerph16020218.

Chicote-Beato, M., González-Víllora, S., Bodoque-Osma, A. and Navarro, R. (2024), 'Cyberbullying intervention and prevention programmes in Primary Education (6 to 12 years): A systematic review', *AGGRESSION AND VIOLENT BEHAVIOR*, Vol. 77, https://doi.org/10.1016/j.avb.2024.101938.

Chun, J., Lee, J., Kim, J. and Lee, S. (2020), 'An international systematic review of cyberbullying measurements', *Computers in Human Behavior*, Vol. 113, p. 106485, https://doi.org/10.1016/j.chb.2020.106485.

Cosma, A., Molcho, M. and Pickett, W. (contribs) (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*, WHO Regional Office for Europe, Copenhagen.

Council of Europe (n.d.), 'Bullying', Council of Europe - Children's Rights website, accessed 5 October 2025, https://www.coe.int/en/web/children/bullying.

Council of Europe (2018), 'Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018', T-CY(2017)10, 14 July, Strasbourg, France, https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914.

Council of the European Union (2025), 'Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era (draft)', Publications Office, https://data.europa.eu/doi/10.2838/859030.

Council of the European Union (2022), 'Council conclusions on supporting well-being in digital education 2022/C 469/04', Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_469_R_0004.

Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M. et al. (2020), 'Social Media Use and Cyber-Bullying: A Cross-National Analysis of Young People in 42 Countries', *Journal of Adolescent Health*, Vol. 66, Issue 6, pp. S100–S108, https://doi.org/10.1016/j.jadohealth.2020.03.006.

Dalla Pozza, V., Di Pietro, A., More, S. and Psaila, E. (2016), 'Cyberbullying among young people', European Parliament, https://data.europa.eu/doi/10.2861/748350.

Dennehy, R., Meaney, S., Walsh, K. A., Sinnott, C., Cronin, M. et al. (2020), 'Young people's conceptualizations of the nature of cyberbullying: A systematic review and synthesis of qualitative research', *Aggression and Violent Behavior*, Vol. 51, p. 101379, https://doi.org/10.1016/j.avb.2020.101379.

Díaz-Esterri, J., Galán-Casado, D., De-Juanas, Á. and García-Castilla, F. J. (2025), 'Leisure, Bullying and Cyberbullying Prevention in Adolescents: a Systematic Review', *Electronic Journal of Research in Educational Psychology*, Issue 65, https://doi.org/10.25115/h78xgh41.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, (13 December 2011), OJ L 335, 17/12/2011, http://data.europa.eu/eli/dir/2011/93/oj.

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, (4 May 2024), OJ L, 2024/1385, http://data.europa.eu/eli/dir/2024/1385/oj.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. and Lim, W. M. (2021), 'How to conduct a bibliometric analysis: An overview and guidelines', *Journal of Business Research*, Vol. 133, pp. 285–296, https://doi.org/10.1016/j.jbusres.2021.04.070.

Dorol-Beauroy-Eustache, O. and Mishara, B. L. (2021), 'Systematic review of risk and protective factors for suicidal and self-harm behaviors among children and adolescents involved with cyberbullying', *Preventive Medicine*, Vol. 152, https://doi.org/10.1016/j.ypmed.2021.106684.

Doty, J., Girón, K., Mehari, K., Sharma, D., Smith, S. et al. (2022), 'The Dosage, Context, and Modality of Interventions to Prevent Cyberbullying Perpetration and Victimization: a Systematic Review', *PREVENTION SCIENCE*, Vol. 23, Issue 4, pp. 523–537, https://doi.org/10.1007/s11121-021-01314-8.

EC (2025a), 'Commission makes available an age-verification blueprint', 14 July, accessed 10 October 2025, https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint.

EC (2024), 'Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child', https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401238.

EC (2023), 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a comprehensive approach to mental health', https://health.ec.europa.eu/publications/comprehensive-approach-mental-health_en.

EC (2022), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A digital decade for children and youth: the new European Strategy for a better internet for kids (BIK+)', https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN.

EC (2021), 'EU strategy on the rights of the child', http://data.europa.eu/eli/C/2025/5519/oj.

EC (2025b), 'Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065', Official Journal of the European Union, http://data.europa.eu/eli/C/2025/5519/oj.

EC (2025c), 'Supervision of the designated very large online platforms and search engines under DSA', European Commission website, 23 September, accessed 2 October 2025, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

EC (2025d), 'The Union of Skills', https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52025DC0090.

EC: DG CNECT (2025a), 'Better Internet for Kids (BIK) Policy monitor', Better Internet for Kids website, https://better-internet-for-kids.europa.eu/en/knowledge-hub/policy-monitor#country-profiles.

EC: DG CNECT (2025b), 'Call for evidence: Action plan against cyberbullying', Publications Office of the EU website, Website, Publications Office of the European Union, 22 July, accessed 7 October 2025, https://op.europa.eu/en/publication-detail/-/publication/b54baf4d-66e7-11f0-bf4e-01aa75ed71a1.

EC: DG EAC (2024a), *Wellbeing and mental health at school: guidelines for education policymakers*, Publications Office, Luxembourg, https://data.europa.eu/doi/10.2766/901169.

EC: DG EAC (2024b), *Wellbeing and mental health at school: guidelines for school leaders, teachers and educators*, Publications Office of the European Union, NC-02-24-463-EN-N, https://data.europa.eu/doi/10.2766/760136.

EC: DG RTD (2025), 'Living guidelines on the responsible use of generative AI in research', April, Brussels, https://research-and-innovation.ec.europa.eu/document/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en.

EC: JRC (2025), *Generative AI outlook report: exploring the intersection of technology, society, and policy*, Kotsev, A., Navajas Cawood, E., Van Bavel, R. and Vespe, M. (eds), Publications Office, Luxembourg, https://doi.org/10.2760/0991238.

Estévez, E., Cañas, E., Estévez, J. and Povedano, A. (2020), 'Continuity and Overlap of Roles in Victims and Aggressors of Bullying and Cyberbullying in Adolescence: A Systematic Review', *INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH*, Vol. 17, Issue 20, https://doi.org/10.3390/ijerph17207452.

Eurofound (2024), 'Workplace bullying, harassment and cyberbullying – Are regulations and policies fit for purpose?', Publications Office of the European Union, Luxembourg, https://doi.org/10.2806/8853437.

European Commission (2009), 'Safer Internet Day 2009: Commission starts campaign against cyber-bullying', https://ec.europa.eu/commission/presscorner/detail/en/memo_09_58.

European Schoolnet (2024), 'Better Internet for Kids: Review of the year 2024', European Commission, https://better-internet-for-kids.europa.eu/sites/default/files/2025-02/BIK_Report2024_WEB_0.pdf.

Evangelio, C., Rodríguez-González, P., Fernández-Río, J. and Gonzalez-Villora, S. (2022), 'Cyberbullying in elementary and middle school students: A systematic review', *COMPUTERS & EDUCATION*, Vol. 176, https://doi.org/10.1016/j.compedu.2021.104356.

Fernandez Machado, R., Sofia Amaral-Garcia and Duch Brown, N. (2025), 'Workplace Adoption of In-House GenAI Tools: The Case of GPT@JRC at the European Commission', European Commission, Seville (Spain), https://publications.jrc.ec.europa.eu/repository/handle/JRC143418.

Fulantelli, G., Taibi, D., Scifo, L., Schwarze, V. and Eimler, S. (2022), 'Cyberbullying and Cyberhate as Two Interlinked Instances of Cyber-Aggression in Adolescence: A Systematic Review', *FRONTIERS IN PSYCHOLOGY*, Vol. 13, https://doi.org/10.3389/fpsyg.2022.909299.

Gámez-Guadix, M., Mateos-Pérez, E., Wachs, S., Wright, M., Martínez, J. et al. (2022), 'Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ("revenge porn") among adolescents', *Journal of Adolescence*, Vol. 94, Issue 5, pp. 789–799, https://doi.org/10.1002/jad.12064.

Garritty, C., Gartlehner, G., Nussbaumer-Streit, B., King, V. J., Hamel, C. et al. (2021), 'Cochrane Rapid Reviews Methods Group offers evidence-informed guidance to conduct rapid reviews', *Journal of clinical epidemiology*, Vol. 130, Elsevier, pp. 13–22, https://www.sciencedirect.com/science/article/pii/S089543562031146X.

Gefen, A., Gross, Z. and Heiman, T. (2025), 'Co-occurrence of Traditional and Cyberbullying Victimization Among Adolescents: Characteristics, Psychological Difficulties, and Resilience', *Violence and Victims*, Vol. 40, Issue 3, Springer Publishing Company, pp. 437–454, https://doi.org/10.1891/VV-2021-0234.

Giumetti, G. W. and Kowalski, R. M. (2022), 'Cyberbullying via social media and well-being', *Current opinion in psychology*, Vol. 45, Elsevier, p. 101314, https://www.sciencedirect.com/science/article/pii/S2352250X22000161.

Google (n.d.), 'FAQ about Google Trends data - Trends Help', FAQ about Google Trends data website, accessed 2 October 2025, https://support.google.com/trends/answer/4365533?hl=en-GB&ref_topic=6248052&sjid=10460401820760068013-EU.

Gottschalk, F. (2022), ‘Cyberbullying: An overview of research and policy in OECD countries’, OECD Education Working Papers, OECD Education Working Papers No 270, 29 March, OECD Education Working Papers, 270, https://doi.org/10.1787/f60b492b-en.

Henares-Montiel, J., Benítez-Hidalgo, V., Ruiz-Pérez, I., Pastor-Moreno, G. and Rodríguez-Barranco, M. (2022), ‘Cyberbullying and Associated Factors in Member Countries of the European Union: A Systematic Review and Meta-Analysis of Studies with Representative Population Samples’, *INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH*, Vol. 19, Issue 12, https://doi.org/10.3390/ijerph19127364.

Henares-Montiel, J., Pastor-Moreno, G., Ramirez-Saiz, A., Rodriguez-Gómez, M. and Ruiz-Pérez, I. (2023), ‘Characteristics and effectiveness of interventions to reduce cyberbullying: a systematic review’, *FRONTIERS IN PUBLIC HEALTH*, Vol. 11, https://doi.org/10.3389/fpubh.2023.1219727.

Hinduja, S. and Patchin, J. W. (2009), *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*, Corwin Press, Thousand Oaks, Calif.

Hinduja, S. and Patchin, J. W. (2010), ‘Bullying, Cyberbullying, and Suicide’, *Archives of Suicide Research*, Vol. 14, Issue 3, pp. 206–221, https://doi.org/10.1080/13811118.2010.494133.

Hinduja, S. and Patchin, J. W. (2008), ‘Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization’, *Deviant Behavior*, Vol. 29, Issue 2, pp. 129–156, https://doi.org/10.1080/01639620701457816.

Hu, Y., Evelyn, S. and Clancy, E. M. (2025), ‘Player Versus Player: A Systematic Review of Cyberbullying in Multiplayer Online Games’, *Computers in Human Behavior Reports*, Vol. 18, Issue 21, https://doi.org/10.1016/j.chbr.2025.100675.

Huang, N., Zhang, S., Mu, Y., Yu, Y., Riem, M. et al. (2024), ‘Does the COVID-19 Pandemic Increase or Decrease the Global Cyberbullying Behaviors? A Systematic Review and Meta-Analysis’, *TRAUMA VIOLENCE & ABUSE*, Vol. 25, Issue 2, pp. 1018–1035, https://doi.org/10.1177/15248380231171185.

Karpiński, Z. (2023), *The experience of being bullied at school and its effect on reading proficiency in grade 4: an analysis of PIRLS 2021 data.*, Publications Office, Luxembourg, https://data.europa.eu/doi/10.2760/149919.

Kasturiratna, K. T. A. S., Hartanto, A., Chen, C. H. Y., Tong, E. M. W. and Majeed, N. M. (2025), ‘Umbrella review of meta-analyses on the risk factors, protective factors, consequences and interventions of cyberbullying victimization’, *Nature Human Behaviour*, Vol. 9, Issue 1, pp. 101–132, https://doi.org/10.1038/s41562-024-02011-6.

Kim, M., Ellithorpe, M. and Burt, S. (2023), ‘Anonymity and its role in digital aggression: A systematic review’, *AGGRESSION AND VIOLENT BEHAVIOR*, Vol. 72, https://doi.org/10.1016/j.avb.2023.101856.

Kofoed, J. and Staksrud, E. (2019), ‘“We always torment different people, so by definition, we are no bullies”: The problem of definitions in cyberbullying research’, *New Media & Society*, Vol. 21, Issue 4, SAGE Publications, pp. 1006–1020, https://doi.org/10.1177/1461444818810026.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N. and Lattanner, M. R. (2014), ‘Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth.’, *Psychological Bulletin*, Vol. 140, Issue 4, pp. 1073–1137, https://doi.org/10.1037/a0035618.

Kowalski, R. M. and Limber, S. P. (2007), 'Electronic Bullying Among Middle School Students', *Journal of Adolescent Health*, Vol. 41, Issue 6, pp. S22–S30, https://doi.org/10.1016/j.jadohealth.2007.08.017.

Kowalski, R. M., Limber, S. P. and Agatston, P. W. (2012), *Cyberbullying: bullying in the digital age*, 2nd ed (Online-Ausg.), Wiley-Blackwell, Malden, MA.

Lan, M., Law, N. and Pan, Q. (2022), 'Effectiveness of anti-cyberbullying educational programs: A socio-ecologically grounded systematic review and meta-analysis', *COMPUTERS IN HUMAN BEHAVIOR*, Vol. 130, https://doi.org/10.1016/j.chb.2022.107200.

Li, J., Huebner, E. and Tian, L. (2024), 'Linking childhood maltreatment to cyberbullying perpetration and victimization: A systematic review and multilevel meta-analysis', *COMPUTERS IN HUMAN BEHAVIOR*, Vol. 156, https://doi.org/10.1016/j.chb.2024.108199.

Livingstone, S., Lievens, E. and Carr, J. (2020), *Handbook for policy makers on child rights in the digital environment_ENG*, Council of Europe, www.coe.int/children.

Lo Cricchio, M., García-Poole, C., te Brinke, L., Bianchi, D. and Menesini, E. (2021), 'Moral disengagement and cyberbullying involvement: A systematic review', *EUROPEAN JOURNAL OF DEVELOPMENTAL PSYCHOLOGY*, Vol. 18, Issue 2, pp. 271–311, https://doi.org/10.1080/17405629.2020.1782186.

Lozano-Blasco, R., Cortés-Pascual, A. and Latorre-Martínez, M. (2020), 'Being a cybervictim and a cyberbully - The duality of cyberbullying: A meta-analysis', *COMPUTERS IN HUMAN BEHAVIOR*, Vol. 111, https://doi.org/10.1016/j.chb.2020.106444.

Martínez-Cao, C., Gómez, L., Alcedo, M. and Monsalve, A. (2021), 'Systematic Review of Bullying and Cyberbullying in Young People with Intellectual Disability', *EDUCATION AND TRAINING IN AUTISM AND DEVELOPMENTAL DISABILITIES*, Vol. 56, Issue 1, pp. 3–17.

Martínez-Monteagudo, A., Martínez-Monteagudo, M. and Delgado, B. (2023), 'School bullying and cyberbullying in academically gifted students: A systematic review', *AGGRESSION AND VIOLENT BEHAVIOR*, Vol. 71, https://doi.org/10.1016/j.avb.2023.101842.

Mills, L., Driver, C., McLoughlin, L., Anijaerv, T., Mitchell, J. et al. (2024), 'A Systematic Review and Meta-analysis of Electrophysiological Studies of Online Social Exclusion: Evidence for the Neurobiological Impacts of Cyberbullying', *ADOLESCENT RESEARCH REVIEW*, Vol. 9, Issue 1, pp. 135–163, https://doi.org/10.1007/s40894-023-00212-0.

Morales-Arjona, I., Benítez-Hidalgo, V., Ruiz-Pérez, I., Higueras-Callejón, C. and Pastor-Moreno, G. (2024), 'Cyberbullying and Suicidal Behavior, Self-Harm, and Nonsuicidal Self-Injury: A Systematic Review of Longitudinal Studies', *Cyberpsychology, Behavior, and Social Networking*, Vol. 27, Issue 10, pp. 683–691, https://doi.org/10.1089/cyber.2024.0097.

Mubashir, M. and Nasrin, T. (2022), 'Locating Cyberbullying and Mental Health in the Recent Literature', *TRIPODOS*, Issue 52, pp. 91–107, https://doi.org/10.51698/tripodos.2022.52p91-107.

Murphy, C. (2024), 'Cyberbullying among young people: Laws and policies in selected Member States', June, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI(2024)762331_EN.pdf.

Myers, C.-A. and Cowie, H. (2019), ‘Cyberbullying across the lifespan of education: Issues and interventions from school to university’, *International journal of environmental research and public health*, Vol. 16, Issue 7, MDPI, p. 1217, https://www.mdpi.com/1660-4601/16/7/1217.

Nee, C., Samsudin, N., Chuan, H., Ridzuan, M., Boon, O. et al. (2023), ‘The digital defence against cyberbullying: A systematic review of tech-based approaches’, *COGENT EDUCATION*, Vol. 10, Issue 2, https://doi.org/10.1080/2331186X.2023.2288492.

Negreiro, M. (2025), ‘Children and deepfakes’, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf .

Ng, E., Chua, J. and Shorey, S. (2022), ‘The Effectiveness of Educational Interventions on Traditional Bullying and Cyberbullying Among Adolescents: A Systematic Review and Meta-Analysis’, *TRAUMA VIOLENCE & ABUSE*, Vol. 23, Issue 1, pp. 132–151, https://doi.org/10.1177/1524838020933867.

OED (2024a), ‘bully, n.[1] meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/3848296136.

OED (2024b), ‘bullying, n. meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/2706468083.

OED (2025a), ‘cyber-bullying, n. meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/4379771899.

OED (2025b), ‘cyberstalking, n. meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/5018424400.

OED (2023), ‘harassment, n. meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/1061545770.

OED (2025c), ‘mobbing, n. meanings, etymology and more’, *Oxford English Dictionary*, Oxford University Press, https://doi.org/10.1093/OED/7872996502.

Ofcom (2024), ‘A deep dive into deepfakes that demean, defraud and disinform’, Ofcom website, 23 July, accessed 20 October 2025, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform.

O’Higgins Norman, J. (2024), *School Bullying, An Inclusive Definition*, UNESCO Chair on Bullying and Cyberbullying at Dublin City University on behalf of the Working Group on Definitions of Bullying convened by UNESCO and World Anti-Bullying Forum, Dublin, https://antibullyingcentre.ie/unesco-world-anti-bullying-forum-agree-on-inclusive-definition-of-bullying/.

O’Higgins Norman, J., Heaney, D. and Donoghue, C. (2025), ‘Considering a More Inclusive Definition of Bullying: Implications for a Whole-Education Approach to Bullying’, in: Artinopoulou, V., Smith, P. K., Limber, S. P. and Breivik, K. (eds), *School Bullying and the Legacy of Dan Olweus*, 1st edition, Wiley, pp. 191–206, https://doi.org/10.1002/9781394173556.ch11.

O’Keeffe, G. S., Clarke-Pearson, K. and Council on Communications and Media (2011), ‘The Impact of Social Media on Children, Adolescents, and Families’, *Pediatrics*, Vol. 127, Issue 4, pp. 800–804, https://doi.org/10.1542/peds.2011-0054.

Olweus, D. (1994), ‘Bullying at School: Long-Term Outcomes for the Victims and an Effective School-Based Intervention Program’, in: , *Aggressive Behavior*, The Plenum Series in Social/Clinical Psychology, Springer US, Boston, MA, pp. 97–130, https://doi.org/10.1007/978-1-4757-9116-7_5.

Olweus, D. and Limber, S. P. (2018), ‘Some problems with cyberbullying research’, *Current Opinion in Psychology*, Vol. 19, pp. 139–143, https://doi.org/10.1016/j.copsyc.2017.04.012.

O’Neill, B. and Dopona, V. (2025), ‘The Better Internet for Kids (BIK) Policy Monitor Report 2025’, European Schoolnet, prepared for the European Commission, https://better-internet-for-kids.europa.eu/en/knowledge-hub/policy-monitor.

Pardo-González, E. and Souza, S. (2022), ‘What do parents think about cyberbullying? A systematic review of qualitative studies’, *REVISTA DE EDUCACION*, Issue 397, pp. 97–124, https://doi.org/10.4438/1988-592X-RE-2022-397-541.

Patchin, J. W. and Hinduja, S. (2006), ‘Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying’, *Youth Violence and Juvenile Justice*, Vol. 4, Issue 148, pp. 148–169, https://doi.org/10.4324/9781315265841-8.

Patchin, J. W. and Hinduja, S. (2025), ‘Summary of Our Cyberbullying Research (2004-2022)’, Cyberbullying Research Center, 30 June, accessed 20 October 2025, https://cyberbullying.org/summary-of-our-cyberbullying-research.

PEN America (n.d.), ‘Cyber-Mob Attacks’, Online Harassment Field Manual website, accessed 10 September 2025a, https://onlineharassmentfieldmanual.pen.org.

PEN America (n.d.), ‘Defining “Online Abuse”: A Glossary of Terms - Online Harassment Field Manual’, Online Harassment Field Manual website, accessed 24 September 2025b, https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/.

PEN America (n.d.), ‘Hateful speech’, Online Harassment Field Manual website, accessed 10 September 2025c, https://onlineharassmentfieldmanual.pen.org.

Peter, I.-K. and Petermann, F. (2018), ‘Cyberbullying: A concept analysis of defining attributes and additional influencing factors’, *Computers in Human Behavior*, Vol. 86, pp. 350–366, https://doi.org/10.1016/j.chb.2018.05.013.

Peters, M. D. J., Marnie, C., Colquhoun, H., Garritty, C. M., Hempel, S. et al. (2021), ‘Scoping reviews: reinforcing and advancing the methodology and application’, *Systematic Reviews*, Vol. 10, Issue 1, p. 263, https://doi.org/10.1186/s13643-021-01821-3.

Pew Research Center (2022), ‘Teens and Cyberbullying 2022’, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

Polanin, J. R., Espelage, D. L., Grotpeter, J. K., Ingram, K., Michaelson, L. et al. (2022), ‘A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization’, *Prevention Science*, Vol. 23, Issue 3, pp. 439–454, https://doi.org/10.1007/s11121-021-01259-y.

Predescu, E., Calugar, I. and Sipos, R. (2024), ‘Cyberbullying and Non-Suicidal Self-Injury (NSSI) in Adolescence: Exploring Moderators and Mediators through a Systematic Review’, *CHILDREN-BASEL*, Vol. 11, Issue 4, https://doi.org/10.3390/children11040410.

Quintana-Orts, C., Rey, L. and Worthington, E. (2021), 'The Relationship Between Forgiveness, Bullying, and Cyberbullying in Adolescence: A Systematic Review', *TRAUMA VIOLENCE & ABUSE*, Vol. 22, Issue 3, pp. 588–604, https://doi.org/10.1177/1524838019869098.

Ray, G., McDermott, C. D. and Nicho, M. (2024), 'Cyberbullying on Social Media: Definitions, Prevalence, and Impact Challenges', *Journal of Cybersecurity*, Vol. 10, Issue 1, p. tyae026, https://doi.org/10.1093/cybsec/tyae026.

Real Fernández, M., Navarro Soria, I., Collado-Valero, J., Lavigne-Cervan, R. and Delgado Domenech, B. (2022), 'Cyberbullying and Executive Functions in children and adolescents: a systematic review', *Revista de Educación*, Issue 397, pp. 67–92, https://doi.org/10.4438/1988-592X-RE-2022-397-540.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), (19 October 2022), OJ L 277, pp. 1–102, http://data.europa.eu/eli/reg/2022/2065/oj.

Rousay, V. (2023), 'Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms', Master's thesis, Harvard University Division of Continuing Education, https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374909.

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.

Rusillo-Magdaleno, A., Moral-García, J., Brandao-Loureiro, V. and Martínez-López, E. (2024), 'Influence and Relationship of Physical Activity before, during and after the School Day on Bullying and Cyberbullying in Young People: A Systematic Review', *EDUCATION SCIENCES*, Vol. 14, Issue 10, https://doi.org/10.3390/educsci14101094.

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, p. 100404, https://doi.org/10.1016/j.chbr.2024.100404.

Salawu, S., He, Y. and Lumsden, J. (2020), 'Approaches to Automated Detection of Cyberbullying: A Survey', *IEEE TRANSACTIONS ON AFFECTIVE COMPUTING*, Vol. 11, Issue 1, pp. 3–24, https://doi.org/10.1109/TAFFC.2017.2761757.

Schoffstall, C. L. and Cohen, R. (2011), 'Cyber Aggression: The Relation between Online Offenders and Offline Social Competence', *Social Development*, Vol. 20, Issue 3, pp. 587–604, https://doi.org/10.1111/j.1467-9507.2011.00609.x.

Schofield, D., Frantzen, V. and Kupiainen, R. (2021), 'Towards a Nordic MIL-index A feasibility study for a Nordic Media and Information Literacy Index', Norwegian University of Science and Technology, https://mediemyndigheten.se/globalassets/rapporter-och-analyser/2021/towards-a-nordic-mil-index.pdf.

Scriven, P. (2025), 'Online trolling as a dark leisure activity', *Annals of Leisure Research*, Vol. 28, Issue 2, Routledge, pp. 283–301, https://doi.org/10.1080/11745398.2024.2358764.

Shahzad, K., Khan, S., Javeed, A. and Iqbal, A. (2024), 'Factors influencing cyberbullying among citizens: a systematic review of articles published in refereed journals from 2010 to 2023', *GLOBAL KNOWLEDGE MEMORY AND COMMUNICATION*, https://doi.org/10.1108/GKMC-11-2023-0422.

Shaikh, F., Rehman, M. and Amin, A. (2020), 'Cyberbullying: A Systematic Literature Review to Identify the Factors Impelling University Students Towards Cyberbullying', *IEEE ACCESS*, Vol. 8, pp. 148031–148051, https://doi.org/10.1109/ACCESS.2020.3015669.

Slonje, R. and Smith, P. K. (2008), 'Cyberbullying: Another main type of bullying?', *Scandinavian Journal of Psychology*, Vol. 49, Issue 2, pp. 147–154, https://doi.org/10.1111/j.1467-9450.2007.00611.x.

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, 10.21953/lse.47fdeq.

Smela, B., Toumi, M., Świerk, K., Francois, C., Biernikiewicz, M. et al. (2023), 'Rapid literature review: definition and methodology', *Journal of Market Access & Health Policy*, Vol. 11, Issue 1, MDPI AG, https://doi.org/10.1080/20016689.2023.2241234.

Smith, P. K., Barrio, C. del and Tokunaga, R. S. (2013), 'Definitions of Bullying and Cyberbullying: How Useful Are  the Terms?', in: Bauman, S., Cross, D. and Walker, J. L. (eds), *Principles of cyberbullying research: definitions, measures, and methodology*, Routledge, New York, N.Y, pp. 56–72, https://doi.org/10.4324/9780203084601.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. et al. (2008), 'Cyberbullying: its nature and impact in secondary school pupils', *Journal of Child Psychology and Psychiatry*, Vol. 49, Issue 4, pp. 376–385, https://doi.org/10.1111/j.1469-7610.2007.01846.x.

Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson (2011), 'EU kids online: final report', EU Kids Online, London School of Economics & Political Science, London, UK, http://eprints.lse.ac.uk/39351/.

Stollsteiner, G. (2025), 'Hate Speech and Cyberbullying in Belgium: Critical Update Required', in: , Ferenc Mádl Institute of Comparative Law, Budapest, pp. 477–503, https://doi.org/10.47079/2025.kprhk.cyberb.4_18.

Tang, L. and Omar, S. (2023), 'Cyberbullying Using the Phenomenological Approach: A Systematic Literature Review', *JURNAL KOMUNIKASI-MALAYSIAN JOURNAL OF COMMUNICATION*, Vol. 39, Issue 4, pp. 561–580, https://doi.org/10.17576/JKMJC-2023-3904-30.

Teng, T. H., Varathan, K. D. and Crestani, F. (2024), 'A comprehensive review of cyberbullying-related content classification in online social media', *Expert Systems with Applications*, Vol. 244, p. 122644, https://doi.org/10.1016/j.eswa.2023.122644.

Thomas, H. J., Connor, J. P. and Scott, J. G. (2015), 'Integrating Traditional Bullying and Cyberbullying: Challenges of Definition and Measurement in Adolescents – a Review', *Educational Psychology Review*, Vol. 27, Issue 1, pp. 135–152, https://doi.org/10.1007/s10648-014-9261-7.

Tokunaga, R. S. (2010), 'Following you home from school: A critical review and synthesis of research on cyberbullying victimization', *Computers in Human Behavior*, Vol. 26, Issue 3, pp. 277–287, https://doi.org/10.1016/j.chb.2009.11.014.

Tozzo, P., Cuman, O., Moratto, E. and Caenazzo, L. (2022), 'Family and Educational Strategies for Cyberbullying Prevention: A Systematic Review', *INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH*, Vol. 19, Issue 16, https://doi.org/10.3390/ijerph191610452.

Tural Hesapcioglu, S. and Ercan, F. (2017), ‘Traditional and cyberbullying co-occurrence and its relationship to psychiatric symptoms’, *Pediatrics International*, Vol. 59, Issue 1, Blackwell Publishing, pp. 16–22, https://doi.org/10.1111/ped.13067.

UN General Assembly (2023), ‘Resolution adopted by the General Assembly on 15 December 2022. Protecting children from bullying’, https://documents.un.org/doc/undoc/gen/n22/760/61/pdf/n2276061.pdf.

UN General Assembly (2019), ‘Resolution adopted by the General Assembly on 17 December 2018. Protecting children from bullying’, https://documents.un.org/doc/undoc/gen/n18/446/36/pdf/n1844636.pdf.

UN General Assembly (2024), ‘Resolution adopted by the Human Rights Council on 9 October 2024. Countering cyberbullying’, https://docs.un.org/en/A/HRC/RES/57/6.

UNESCO (2019), *Behind the numbers: ending school violence and bullying*, UNESCO, Paris, https://doi.org/10.54675/TRVR4270.

UNESCO (2020), ‘Recommendations by the Scientific Committee on Preventing and Addressing School Bullying and Cyberbullying’, UNESCO & French Ministry of Education, Youth and Sports, https://unesdoc.unesco.org/ark:/48223/pf0000374794.

UNESCO (2024), *Safe to learn and thrive: Ending violence in and through education*, United Nations Educational, Scientific and Cultural Organization, Paris, https://doi.org/10.54675/LUPY3293.

UNICEF (2018), *INSPIRE Indicator Guidance and Results Framework - Ending Violence Against Children: How to define and measure change*, United Nations Children’s Fund, New York, https://www.unicef.org/media/66896/file/INSPIRE-IndicatorGuidance-ResultsFramework.pdf.

Vaccari, C. and Chadwick, A. (2020), ‘Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News’, *Social Media + Society*, Vol. 6, Issue 1, p. 2056305120903408, https://doi.org/10.1177/2056305120903408.

Vandebosch, H. and Van Cleemput, K. (2008), ‘Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters’, *CyberPsychology & Behavior*, Vol. 11, Issue 4, pp. 499–503, https://doi.org/10.1089/cpb.2007.0042.

Verdoodt, V., Lievens, E., O’Neill, B. and Dopona, V. (2025), ‘First evaluation of the European strategy for a better internet for kids (BIK+). A summary of consultations with children, young people, and expert stakeholders’, European Schoolnet, prepared for the European Commission, https://better-internet-for-kids.europa.eu/sites/default/files/2025-02/ BIK-plus-strategy-evaluation-report-February-2025.pdf.

von der Leyen, U. (2025), ‘2025 State of the Union Address by President von der Leyen’, European Commission - European Commission website, Text, 10 September, accessed 7 October 2025, https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053.

von der Leyen, U. (2024a), ‘Europe’s Choice: Political Guidelines For The Next European Commission 2024–2029’, 18 July, Strasbourg, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

von der Leyen, U. (2024b), ‘Mission letter to Glenn Micallef (Commissioner-designate for Intergenerational Fairness, Youth, Culture and Sport)’, https://commission.europa.eu/document/download/c8b8682b-ca47-461b-bc95-c98195919eb0_en?filename=Mission%20letter%20-%20MICALLEF.pdf.

von der Leyen, U. (2024c), 'Mission letter to Henna Virkkunen (Executive Vice-President-designate for Tech Sovereignty, Security and Democracy)', https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf.

von der Leyen, U. (2024d), 'Mission letter to Olivér Várhelyi (Commissioner-designate for Health and Animal Welfare)', https://commission.europa.eu/document/download/b1817a1b-e62e-4949-bbb8-ebf29b54c8bd_en?filename=Mission%20letter%20-%20VARHELYI.pdf.

Wang, J., Iannotti, R. J. and Nansel, T. R. (2009), 'School Bullying Among Adolescents in the United States: Physical, Verbal, Relational, and Cyber', *Journal of Adolescent Health*, Vol. 45, Issue 4, pp. 368–375, https://doi.org/10.1016/j.jadohealth.2009.03.021.

Wang, L. and Jiang, S. (2023), 'Effectiveness of Parent-Related Interventions on Cyberbullying Among Adolescents: A Systematic Review and Meta-Analysis', *TRAUMA VIOLENCE & ABUSE*, Vol. 24, Issue 5, pp. 3678–3696, https://doi.org/10.1177/15248380221137065.

Wang, L., Jiang, S., Zhou, Z., Fei, W. and Wang, W. (2024), 'Online disinhibition and adolescent cyberbullying: A systematic review', *Children and Youth Services Review*, Vol. 156, Elsevier, p. 107352, https://www.sciencedirect.com/science/article/pii/S0190740923005480.

Wegge, D., Vandebosch, H., Eggermont, S. and Pabian, S. (2016), 'Popularity Through Online Harm: The Longitudinal Associations Between Cyberbullying and Sociometric Status in Early Adolescence', *The Journal of Early Adolescence*, Vol. 36, Issue 1, pp. 86–107, https://doi.org/10.1177/0272431614556351.

WHO (2022a), 'Violence Against Children Online. What health systems and health care providers can do', https://www.who.int/publications/m/item/violence-against-children-online.

WHO (2022b), *What Works to Prevent Violence Against Children Online?*, 1st ed, World Health Organization, Geneva.

Zammit, L. (2025), 'Promoting ethical online behaviour: the perspectives of educators, experts and policymakers on cyberbullying in Maltese secondary schools', *London Review of Education*, Vol. 23, Issue 1, https://doi.org/10.14324/LRE.23.1.10.

Zhang, D., Gong, J., Liu, J., Bullock, A. and Sang, B. (2025), 'The bidirectional relationships between cyberbullying and depression: A systematic review and meta-analysis of longitudinal studies', *AGGRESSION AND VIOLENT BEHAVIOR*, Vol. 82, https://doi.org/10.1016/j.avb.2025.102052.

Zhang, W., Huang, S., Lam, L., Evans, R. and Zhu, C. (2022), 'Cyberbullying definitions and measurements in children and adolescents: Summarizing 20 years of global efforts', *Frontiers in Public Health*, Vol. 10, p. 1000504, https://doi.org/10.3389/fpubh.2022.1000504.

Zheng, G., Fan, Y., Huang, J., Lan, J. and Wang, Y. (2025), 'Parenting in Context: A Systematic Review of Family Factors and Cyberbullying Perpetration Among Adolescents', *CHILD & FAMILY SOCIAL WORK*, https://doi.org/10.1111/cfs.13281.

Zhu, C., Huang, S., Evans, R. and Zhang, W. (2021), 'Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures', *FRONTIERS IN PUBLIC HEALTH*, Vol. 9, https://doi.org/10.3389/fpubh.2021.634909.

## List of abbreviations and definitions

| Abbreviations | Definitions |
|---|---|
| AI | Artificial Intelligence |
| BIK+ | Better Internet for Kids |
| DG CNECT | Directorate-General for Communications Networks, Content and Technology |
| DG EAC | Directorate-General for Education, Youth, Sport and Culture |
| DG RTD | Directorate-General for Research and Innovation |
| EC | European Commission |
| EEA | European Economic Area |
| EEG | Electroencephalography |
| EFTA | European Free Trade Association |
| EU | European Union |
| GenAI | Generative artificial intelligence |
| HBSC | Health Behaviour in School-aged Children |
| ICTs | Information and communication technologies |
| JRC | Joint Research Centre |
| MSs | Member states |
| OECD | Organisation for Economic Co-operation and Development |
| OED | Oxford English Dictionary |
| SID | Safer Internet Day |
| SICs | Safer Internet Centres |
| UN | United Nations |
| UNESCO | United Nations Educational, Scientific and Cultural Organization |

| Abbreviations | Definitions |
|---|---|
| UNICEF | United Nations Children’s Fund |
| UNODC | United Nations Office on Drugs and Crime |
| WHO | World Health Organization |

## List of figures

## List of tables

# Annex 1. Country profiles

## EU Member States

### Belgium

| | |
|---|---|
| **Relevant legislation** | The Criminal Code contains a number of provisions that may be applicable to cyberbullying, although it is not criminalised as a specific offense. First, article 422bis of the Criminal Code, which punishes persons who menace an individual, while they knew or should have known that through their behaviour they would seriously disturb the peace of that individual. Secondly, articles 443-444 of the Criminal Code criminalise defamation and libel. Thirdly, article 448 of the Criminal Code punishes persons who offend or insult someone by means of writings or images. The perpetrator must have a malicious intent, and the insult must be public. [1]<br>A more specific offense is provided for in Article 145 §3bis of Law of 13 of June, 2005 on Electronic Communications. It refers to the use of electronic communications to cause damage and nuisance. [2] |
| **Definitions in legislation** | Law on Electronic Communications [2]:<br>Article 145 §3bis - [online harassment]:<br>A person who uses an electronic communications network or service or other electronic communications means to cause nuisance to their correspondent or to cause damage, as well as a person who sets up any device intended to commit the aforementioned infringement, or an attempt to do so , shall be punished with a fine of EUR 50 to EUR 300 and with imprisonment from fifteen days to two years, or with only one of these penalties.) <W 2007-04-25/38, art. 189, 006; Entry into force: 18-05-2007><br>According to Stollsteiner (2025, p. 489), although the word 'harassment' is not used in the law, it may be considered as a concept close enough to online harassment. |
| **Examples of initiatives** | The *Cyber Security Coalition* is a unique partnership between players from the academic world, the public authorities and the private sector to join forces to bolster Belgium's cyber security resilience and build a strong cyber security ecosystem at national level. [3]<br>In January 2024 the Belgian federal parliament approved a Resolution to Ensure Children's Online Safety. [4]<br>A biannual study called Apenstaartjaren is conducted in Flanders about the media use and media literacy of 6 to 18-year-olds [5], while Generation2024 is a major French-speaking survey on the digital practices of children and adolescents. [6]<br>CyberSquad is an initiative that empowers young people to become digital heroes by equipping them with skills to handle online risks and support their peers. [7]<br>Tejo offers accessible, free, and anonymous therapeutic support to young people. [8]<br>VRT Edubox Sexting is an educational tool developed by the Flemish public broadcaster VRT, aimed at helping teachers discuss sensitive topics like sexting, digital privacy, and online reputation with teenagers. [9]<br>The Flemish Knowledge Centre for Digital and Media Literacy, Mediawijs, host in their side a tool to support schools respond to cyberbullying, namely a Flowchart 'First aid for cyberbullying'. [10] |
| **References** | [1] 'Penal Code (Code Pénal)' (2025), https://www.ejustice.just.fgov.be/<br>[2] 'Electronic Communications Act (Wet betreffende de elektronische communicatie)' (2005), https://www.ejustice.just.fgov.be/. |

| | |
|---|---|
| | [3] The Cyber Security Coalition (n.d.), ‘The Place to be for Cyber Security Experts’, Belgium’s Cyber Security Coalition website, accessed 30 October 2025, https://cybersecuritycoalition.be/<br>[4] Chambre des représentants de Belgique / Belgische Kamer van volksvertegenwoordigers (2024), ‘RÉSOLUTION visant à garantir la sécurité en ligne des enfants / RESOLUTIE ter bevordering van de online veiligheid van kinderen’, https://www.dekamer.be/ [PDF].<br>[5] Apenstaartjaren (n.d.), ‘Mediagebruik in 2024: wat zeggen kinderen en jongeren nu zélf? \| Apenstaartjaren’, accessed 30 October 2025, https://www.apenstaartjaren.be/.<br>[6] Generation2024 (n.d.), ‘DÉCOUVREZ L’ENQUÊTE #GENERATION2024’, accessed 30 October 2025, https://generation2024.be/.<br>[7] ‘Child Focus (n.d.), ‘CYBER SQUAD’, accessed 3 November 2025, https://cybersquad.be/<br>[8] TEJO (n.d.), ‘Laat jongeren niet vallen’, accessed 30 October 2025, https://tejo.be/.<br>[9] EDUBOX (n.d.), ‘Teachable Machine’, accessed 30 October 2025, https://teachablemachine.withgoogle.com/.<br>[10] Mediawijs (n.d.), ‘Flowchart “Eerste hulp bij cyberpesten”’, accessed 30 October 2025, https://www.mediawijs.be/nl/eerstehulpbijcyberpesten. |

## Bulgaria

| | |
|---|---|
| **Relevant legislation** | Several cases of cyberbullying can be covered by the Criminal Code: Article 162 under Chapter Three Section I - Crimes Against the Equality of All Citizens (Amended, SG No. 27/2009, SG No. 33/2011, effective 27.05.2011). [1]<br>However, there is still no criminalisation of cyberbullying. In recent public discussions it has been suggested that an amendment of existing legislation with the aim of criminalising cyberbullying and increasing criminal penalties should take place. [2] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 162: [discrimination, violence or hatred by electronic information systems]:<br>Anyone who, by speech, press or other media, by electronic information systems or in another manner, propagates or incites discrimination, violence or hatred on the grounds of race, nationality or ethnic origin shall be punishable by imprisonment from one to four years and a fine from BGN 5,000 to 10,000, as well as public censure.(Amended, SG No. 27/2009, SG No. 33/2011, effective 27.05.2011). |
| **Examples of initiatives** | The Bulgarian government adopted the National Programme for the Prevention of Violence and Abuse of Children 2023-2026, outlining strategies to combat violence against children, including online threats. [3]<br>The Bulgarian National Council for Child Protection is a body of the State Agency for Child Protection and has consultive and coordination functions. [4]<br>The Cyberscout program is a two-day training on online safety for children of age 11-12 years. [5]<br>The "Steps Together" program, in which UNICEF in collaboration with the Ministry of Education and Science joined forces to support a Violence-Free School and Safe Online Environment for Every Child by reaching children - including those outside the formal education system-, education specialists and parents. The programme is a comprehensive school policy for a safe educational environment and supports the implementation of the Mechanism for Combating Bullying and Violence in Institutions in the System of Preschool and School Education. [6] |

| | |
|---|---|
| **References** | [1] Criminal Code'(2015), https://www.mlsp.government.bg/.<br>[2] Deneva, D. (2023), Cyberbullying becomes a crime (Тормозът в интернет става престъпление)', accessed 27 October 2025, https://www.standartnews.com/<br>[3] National Network for Children (n.d.), 'The Government Adopted the National Programme for the Prevention of Child Violence and Abuse (2023-2026)', accessed 30 October 2025, https://nmd.bg/en/.<br>[4] Důrzhavna agentsiya za zakrila na deteto (n.d.), 'State Agency for Child Protection - Official website', accessed 30 October 2025, https://sacp.government.bg/<br>[5] EUCPN (n.d.), 'Cyberscout Program', accessed 30 October 2025, https://eucpn.org/.<br>[6] UNICEF (n.d.), 'Steps together to stop violence at school', accessed 30 October 2025, https://www.unicef.org/bulgaria/en/. |

### Czechia

| | |
|---|---|
| **Relevant legislation** | Act 198/2009 Coll. on Equal treatment and legal remedies for protection against discrimination and amending certain laws (Anti-Discrimination Act), art. 4. [1]<br>Additionally, the Criminal Code (Act no. 40/2009 Coll.) rules on dangerous stalking (§354) and defamation (§184), and contains further provisions that may be applicable to cyberbullying: §353 dangerous threat, §180 unauthorised handling of personal data, §181 infringement of rights of another, §182 violating confidentiality of messages, §191 et seq. distribution of pornography, §175 extortion, §144 participation to suicide.<br>Also, under Act no. 251/2016 Coll. on Certain Offences: §7(1)(a) ridicule or otherwise grossly insult, (b) harm, (c) threaten, falsely accuse, act of disapproval, other abusive act. [3]<br>An amendment to the Criminal Code is expected, which will establish new criminal offences criminalising certain types of deepfakes. |
| **Definitions in legislation** | Act 198/2009 (Anti-Discrimination Act) [1]<br>Article 4.1:<br>(1) Harassment means unwanted conduct related to the grounds referred to in Section 2(3) [race, ethnic origin, nationality, sex, sexual orientation, age, disability, religion, belief],<br>(a) the intention or effect of which is to diminish the dignity of a person and to create an intimidating, hostile, humiliating, humiliating or offensive environment, or<br>(b) which can be legitimately perceived as a condition for a decision affecting the exercise of rights and obligations arising from legal relationships.<br>Criminal Code [2]:<br>Article 354 - Dangerous stalking<br>(1) Whoever stalks another person for a long time by<br>a) threats him or his close relatives with bodily harm or other harm,<br>b) seeks to be close to him or follows him,<br>c) persistently contacts him by electronic means, in writing or otherwise,<br>d) restricts him in his usual way of life, or<br>e) abuses his personal data for the purpose of obtaining personal or other contact,<br>and this conduct is likely to arouse in him a reasonable fear for his life or health or for the life and health of persons close to him, shall be punished by imprisonment for up to one year or by a ban on activity.<br>(2) The offender shall be punished by imprisonment for a term of six months to three years if he commits the act referred to in paragraph 1<br>a) against a child or a pregnant woman, |

| | |
|---|---|
| | b) with a weapon, or<br>c) with at least two persons.<br>Article 184 - Defamation<br>(1) Anyone who communicates false information about another that is capable of significantly jeopardizing his reputation among fellow citizens, in particular damaging him at work, disrupting his family relationships or causing him other serious harm, shall be punished by imprisonment for up to one year.<br>(2) The offender shall be punished by imprisonment for up to two years or by a ban on activity if he commits the act referred to in paragraph 1 through the press, film, radio, television, a publicly accessible computer network or another similarly effective means. |
| **Examples of initiatives** | In Czechia, non-legislative initiatives focus on prevention. For instance, a project called 'Regions for a safe internet' is a collaboration among state and local government bodies introduced specific actions to prevent cyberbullying (Say No and Be safe). [4]<br>A framework concept ‘Cyberbullying and other forms of cyber aggression’ is provided to support teacher intervention on risky behaviour in the school environment by the PRVoK PdF UP Olomouc Centre. [5]<br>It also carried out a survey on the Perceptions of cybercrime among children in 2018 and repeated five years later in 2023 to compare the results. [6]<br>The national strategic plan for digital education under the Digital Czechia Strategy include in the main focus areas well-being and cybersecurity in the context of digital skills development. [7] |
| **References** | [1] ‘Act on Equal Treatment and on Legal Means of Protection against Discrimination and on Amendments to Certain Acts (Anti-Discrimination Act) (Zákon o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon))’ (2009), https://www.zakonyprolidi.cz/.<br>[2] ‘Criminal Code Act (Act No. 40/2009 Coll.) (Zákon trestní zákoník (Zákon č. 40/2009 Sb.))’ (2009), https://www.e-sbirka.cz/.<br>[3] ‘LAW of 15 June 2016 on certain offences’ (2022), https://is.muni.cz/el/.<br>[4] Policie Středočeského Kraje (2019), ‘Kyberšikana \| PČR’, 20 December, accessed 30 October 2025, https://bezpecny.stredoceskykraj.cz/.<br>[5] Kopecký, K. and Szotkowski, R. (2017), ‘Kyberšikana a další formy kybernetické agrese’, https://msmt.gov.cz/<br>[6] Projektu KPBI (2023), ‘Vnímání kyberkriminality mezi dětmi (výzkumná zpráva)’, https://kr-vysocina.cz/.<br>[7] Výbor pro digitální vzdělávání pod Radou vlády pro informační společnost (2023), ‘Strategický rámec pro rozvoj digitálního vzdělávání’, https://digitalnicesko.gov.cz/. |

## Denmark

| | |
|---|---|
| **Relevant legislation** | The Criminal Code contains a number of provisions that may be applicable to cyberbullying (e.g., under chapter 26 on crimes against personal freedom (section 260), and chapter 27 on peace and defamation (sections 267 and 268). [1]<br>The Educational Environment Act Executive order about pupil and student educational environment added in 2017, refers to primary and upper secondary schools (LBK nr 316 of 05/04/2017). It was introduced here that each educational institution and school board should establish an antibullying strategy, including a strategy against cyberbullying (Art. 1 b). [2] |

| | |
|---|---|
| | The Working Environment Authority executive order 1406 of 26 September 2020 on Psychosocial Working Environment considers bullying and sexual harassment as offensive behaviour in the working context, and harassment as work-related violence. [3] |
| **Definitions in legislation** | Criminal code [1]:<br>Section 267 – [defamation]<br>Anyone who makes or disseminates a statement or other communication or performs an act that is likely to violate someone's honour shall be punished for defamation by a fine or imprisonment for up to 1 year, cf. sections 268 and 269. [...]<br>Section 268 – [defamation through mass media]<br>The penalty mentioned in § 267 may increase to imprisonment for up to 2 years if 1) a serious accusation is untrue or 2) an accusation is made or disseminated through the content of a mass media, and the accusation is likely to cause significant harm to the injured party.<br>Working Environment Authority executive order [3]:<br>Section 23 – offensive behaviour<br>In this Executive Order, offensive behaviour is defined as a situation where one or more persons grossly or several times expose one or more other persons in the company to bullying, sexual harassment or other degrading behaviour in the workplace. The behaviour must be perceived as degrading by the person being subject to this behaviour.<br>[...] Subsection (3) Offensive behaviour may involve a risk to health or safety, cf. Section 24.<br>Section 25 – work-related violence<br>In this Executive Order, work-related violence is defined as the situation where persons who are not employees or employers of the company, including citizens and customers, use violence against employees or employers. Violence is defined as<br>1. physical violence in the form of attacks against the body and<br>2. psychological violence in the form of threats and other offensive behaviour, including harassment.<br>Subsection (2). Subsection (1) also includes robbery.<br>Subsection (3) Work-related violence can take place both during work and outside working hours. |
| **Examples of initiatives** | In 2023, the Danish government established a Commission on Wellbeing for Children and Youth, which was tasked to investigate the reasons why some children and young people experience low well-being, and to make recommendations on how to contribute to greater well-being among children and young people in Denmark. [4]<br>The ‘Alliance for safe digital lives for children and youth’, was also initiated with the aim to develop voluntary but binding agreements across national actors within industry, civil society and governmental bodies towards vigorous enforcement on digital safety for children.<br>The independent Danish Media Council is a part of a national project on media literacy for young people and children at the age of 5-25 especially focusing on children and young people in vulnerable positions. [5]<br>There are a number of national surveys about digital technologies' use such as 'The survey Young Consumers and Social Media' [6], a randomized field experiment with 250 children aged 13-17, as well as the 'Media and Information Literacy Index across the Nordic countries'. [7] |

| | |
|---|---|
| | Statistics Denmark provides substantive information on bullying among children and adults in Denmark. [8] |
| **References** | [1] ‘Promulgation of the Criminal Code’ (2024), https://legislationline.org/.<br>[2] ‘Proclamation of the Act on the Educational Environment of Pupils and Students (Bekendtgørelse af lov om elevers og studerendes undervisningsmiljø)’ (2017), https://www.retsinformation.dk/.<br>[3] ‘Executive order on psychosocial working environment’ (2020), http://at.dk/en/regulations/.<br>[4] Trivselskommissionen (n.d.), ‘Trivselskommissionen’, accessed 30 October 2025, https://www.trivselskommissionen.dk/.<br>[5] On Undervisning (n.d.), ‘On platform’, accessed 30 October 2025, https://on-undervisning.dk/.<br>[6] Konkurrence- og Forbrugerstyrelsen (2025), ‘Unge forbrugere og sociale medier’, 6 February, accessed 30 October 2025, https://kfst.dk/.<br>[7] MEDLiE (Media Literacy and Education Research Group) (2021), ‘Towards a Nordic MIL index - A feasibility study for a Nordic Media and Information Literacy Index’, https://mediemyndigheten.se/.<br>[8] On Undervisning (n.d.), ‘On platform’, accessed 30 October 2025, https://on-undervisning.dk/. |

## Germany

| | |
|---|---|
| **Relevant legislation** | Articles in the Criminal Code may apply to cyberbullying when committed with electronic means, such as section 238 (Stalking). Other relevant sections include: section 240 (Using threats or force to cause a person to do, suffer or omit an act), section 241 (Threatening the commission of a felony), section 176 (Child abuse), section 185 (Insult), section 186 (Defamation), section 187 (Intentional defamation), section 201 (Violation of the privacy of the spoken word) and section 201a (Violation of intimate privacy by taking photographs).<br>In particular, section 238 (Stalking) and section 176 (Child abuse) explicitly include conduct by means of telecommunications or by using personal data of a person. [1]<br>In addition, sections on the Youth Protection Act (JuSchG): Section 3-Protection of minors in the media, Section 4-Federal Centre for the Protection of Children and Young People in the Media and Section 15-Media harmful to minors. [2] |
| **Definitions in legislation** | Criminal Code [1]:<br>Section 238 – Stalking [by means of telecommunications]<br>(1) Whoever, without being authorised to do so, stalks another person in a manner suited to not insignificantly restricting that person’s lifestyle by repeatedly<br>1. seeking the other person’s physical proximity,<br>2. trying to establish contact with the other person by means of telecommunications or other means of communication or through third parties,<br>3. improperly using the other person’s personal data for the purpose of<br>a) ordering goods or services for that person or<br>b) inducing third parties to make contact with that person,<br>4. threatening the other person, one of his or her relatives, or someone close to him or her with causing injury to life or physical integrity, health or liberty,<br>5. committing an offence under section 202a, 202b or 202c to the detriment of that person, one of his or her relatives or another person close to him or her,<br>6. disseminating or making available to the public a depiction of that person, one of his |

| | |
|---|---|
| | or her relatives or another person close to him or her,<br>7. disseminating or making available to the public content (section 11 (3)) suited to disparaging or negatively affecting public opinion about that person by feigning that person's authorship or<br>8. committing an act comparable with nos. 1 to 7<br>incurs a penalty of imprisonment for a term not exceeding three years or a fine.<br>(2) In particularly serious cases under subsection (1) nos. 1 to 7, stalking incurs a penalty of imprisonment for a term of between three months and five years. An especially serious case typically occurs where the offender<br>1. by committing the offence causes damage to the health of the victim, a relative of or another person close to the victim,<br>2. places the victim, a relative of or another person close to the victim in danger of death or at risk of serious damage to health on account of the act,<br>3. stalks the victim by committing a large number of acts constituting an offence over a period of at least six months,<br>4. uses a computer program in the commission of an act constituting an offence under subsection (1) no. 5 whose purpose is to digitally spy on other persons,<br>5. uses a depiction obtained through one of the acts constituting an offence under subsection (1) no. 5 in the commission of an act constituting an offence under subsection (1) no. 6,<br>6. uses content (section 11 (3)) obtained through one of the acts constituting an offence under subsection (1) no. 5 in the commission of an act constituting an offence under subsection (1) no. 7 or<br>7. is over 21 years of age and the victim is under 16 years of age.<br>(3) If the offender causes the death of the victim, a relative of or another person close to the victim, the penalty is imprisonment for a term of between one year and 10 years. |
| **Examples of initiatives** | In 2016 the 2nd Cybermobbing Congress was hosted under the auspices of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth. Besides, the private association "Alliance against Cybermobbing" (Bündnis gegen Cybermobbing) is a partner of the "Coalition for Digital Security" of the initiative "Deutschland sicher im Netz" under the auspices of the Federal Ministry of the Interior. [https://buendnis-gegen-cybermobbing.de/3], [4]<br>The Youth Media Protection Index (Jugendmedienschutzindex) examines how the protection of children and young people from negative online experiences is reflected in the concerns, attitudes, skills and actions of parents and children and young people themselves. [5]<br>A good example for the involvement of young people is the Advisory Board at the Federal Agency for Child and Youth Protection in the Media (BzKJ). It supports the Federal Agency in further developing the protection of children and young people in the media.<br>The 'Growing up well with media' initiative supports and pools the activities of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth in the area of protecting children and young people in media to strengthen the media skills of children, young people, parents and professionals. [6]<br>JUUUPORT is an online counselling platform founded in 2010 that offers peer-to-peer support for young people experiencing online problems. Teenage and young adult volunteers from all over Germany, so-called JUUUPORT scouts, confidentially help their peers with problems such as cyberbullying, media addiction or sexual harassment. [7] |
| **References** | [1] 'German Criminal Code (Strafgesetzbuch – StGB)' (2021), https://www.gesetze-im-internet.de/englisch_stgb/.<br>[2] 'Protection of Young Persons Act' (2002), https://www.bibb.de/. |

| | |
|---|---|
| | [3] Council of Europe (n.d.), ‘Cyberviolence - Initiatives, policies, strategies - Germany: Action against cybermobbing’, Cyberviolence website, accessed 30 October 2025, https://www.coe.int/en/web/cyberviolence/.<br>[4] Bündnis gegen Cybermobbing (2025), accessed 3 November 2025, https://buendnis-gegen-cybermobbing.de/.<br>[5] Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (n.d.), ‘Jugendmedienschutzindex 2022’, FSM website, accessed 30 October 2025, https://www.fsm.de/.<br>[6] Gutes Aufwachsen mit Medien (n.d.), ‘Für positive Erfahrungen in der digitalen Welt’, Gutes Aufwachsen mit Medien website, accessed 30 October 2025, https://www.gutes-aufwachsen-mit-medien.de/.<br>[7] JUUUPORT (n.d.), ‘Hilfe bei Cybermobbing und anderen Problemen im Netz’, accessed 30 October 2025, https://www.juuuport.de/. |

## Estonia

| | |
|---|---|
| **Relevant legislation** | The following Penal code articles could be applied to cyberbullying: 120–Threat, 137 – Private surveillance, 151 – Incitement to hatred, $153^1$– Sexual harassment, 156 – Violation of confidentiality of communication/messages, $157^2$–Illegal use of another person’s identity, $157^3$–Harassment stalking. [1] |
| **Definitions in legislation** | Penal code [1]:<br>Article $157^3$– Harassment stalking:<br>(1) Repeated or continuous contact with another person, following him or her or otherwise interfering with the private life of another person against his or her will, if the purpose or effect of this is to intimidate, humiliate or otherwise significantly disturb the other person, if the elements of the offence provided for in § 137 of this Code are not met [without a legal right to conduct surveillance for the purpose of collecting data about him or her], shall be punished by a fine or imprisonment for up to one year. |
| **Examples of initiatives** | The Violence Prevention Agreement by the Ministry of Justice and Digital Affairs covers the prevention and combating of various forms of interpersonal violence. The main focus is on violence against children, while new topics include violence against the elderly and mental violence. Hate crimes, which have received less attention so far, have also been addressed to some extent. [2]<br>The Estonian Union for Child Welfare conducted a survey on bullying among more than a 1,000 children and adolescents (grades 4-12) in 2016. |
| **References** | [1] ‘Penal Code (Karistusseadustik)’ (2025), https://legislationline.org/.<br>[2] Ministry of Justice and Digital Affairs (n.d.), ‘The Violence Prevention Agreement’, accessed 30 October 2025, https://www.justdigi.ee/. |

## Ireland

| | |
|---|---|
| **Relevant legislation** | The Non-Fatal Offences Against the Person Act, 1997 legislates on harassment. [1]<br>The Irish Harassment, Harmful Communications and Related Offences Act 2020 covers a range of online abusive practices, also in relation to cyberbullying, such as the publication and distribution of a person’s intimate images without the persons’ consent and the sending of abusive messages with intention to harm the recipient. [2]<br>The Incitement to Violence or Hatred and Hate Offences Act 2022 (criminal justice) is meant to protect specific characteristics of persons or groups of persons, among which race, nationality, religion, gender, sex characteristics, sexual orientation or disability. |

| | |
|---|---|
| | Communicating material through an information system is considered in some of the offenses (e.g. of incitement to violence and hatred). [3]<br>Ireland has recently published draft legislation to reform Ireland's defamation laws, Draft General Scheme of the Defamation (Amendment) Bill, which addresses challenges posed by the digital environment, including online defamation. [4] |
| **Definitions in legislation** | Non-Fatal Offences Against the Person Act, 1997 [1]:<br>Article 10 – Harassment<br>(1) Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.<br>(2) For the purposes of this section a person harasses another where—<br>(a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and<br>(b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.<br>(3) Where a person is guilty of an offence under subsection (1), the court may, in addition to or as an alternative to any other penalty, order that the person shall not, for such period as the court may specify, communicate by any means with the other person or that the person shall not approach within such distance as the court shall specify of the place of residence or employment of the other person.<br>(4) A person who fails to comply with the terms of an order under subsection (3) shall be guilty of an offence.<br>(5) If on the evidence the court is not satisfied that the person should be convicted of an offence under subsection (1), the court may nevertheless make an order under subsection (3) upon an application to it in that behalf if, having regard to the evidence, the court is satisfied that it is in the interests of justice so to do.<br>(6) A person guilty of an offence under this section shall be liable—<br>(a) on summary conviction to a fine not exceeding £1,500 or to imprisonment for a term not exceeding 12 months or to both, or<br>(b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both.<br><br>Harassment, Harmful Communications and Related Offences Act 2020 [2]:<br>Section 2- Distributing, publishing or threatening to distribute or publish intimate image without consent with intent to cause harm or being reckless as to whether harm is caused<br>Article 2.<br>(1) A person who distributes, publishes or threatens to distribute or publish an intimate image of another person—<br>(a) without that other person's consent, and<br>(b) with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person,<br>is guilty of an offence.<br>(2) For the purposes of subsection (1), a person causes harm to another person where—<br>(a) he or she, by his or her acts, intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person, and<br>(b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person.<br>Section 4-Distributing, publishing or sending threatening or grossly offensive communication.<br>Article 4. |

| | |
|---|---|
| | (1) A person who—<br>(a) by any means—<br>(i) distributes or publishes any threatening or grossly offensive communication about another person, or<br>(ii) sends any threatening or grossly offensive communication to another person, and<br>(b) with intent by so distributing, publishing or sending to cause harm,<br>is guilty of an offence.<br>(2) For the purposes of subsection (1), a person intends to cause harm where he or she, by his or her acts, intentionally seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person. |
| **Examples of initiatives** | A whole of Government approach to digital regulation and children's online safety is contained within the National Digital Strategy - Harnessing Digital: The Digital Ireland Framework. [5]<br>A nationwide campaign was launched in Ireland based on the tragic experience of a child who tragically took her own life in 2018 as a result of cyberbullying. This led to the 2021 introduction of the Harassment, Harmful Communications and Related Offenses Act, better known as 'Coco's Law', which is intended to cover a range of online abusive practices. [6]<br>The Department of Education has introduced the 'Bí Cineálta' ('Be Kind') procedures to prevent and address bullying behaviour in primary, post-primary, and special schools across Ireland. [7]<br>The DCU Anti-Bullying Centre (ABC) is a national university designated research centre located within DCU's Institute of Education. It supports the implementation of the Government of Ireland's Action Plan on Bullying (2022), Action Plan for Online Safety (2018-2019), Wellbeing Policy Statement and Framework for Practice (2018-2024), and the WRC/HSA Joint Code of Practice on the Prevention and Resolution of Bullying at Work (2021). [8]<br>A National Survey of Children, their Parents and Adults regarding Online Safety (2021). [9] |
| **References** | [1] Non-Fatal Offences Against the Person Act (1997), https://www.irishstatutebook.ie/<br>[2] 'Harassment, Harmful Communications and Related Offences Act 2020' (2020), Office of the Attorney General, https://www.irishstatutebook.ie/.<br>[3] 'Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022' (2022), https://data.oireachtas.ie/.<br>[4] 'Defamation (Amendment) Act 2023' (2023), https://www.gov.ie/.<br>[5] Department of the Taoiseach (n.d.), 'Harnessing Digital - The Digital Ireland Framework', gov.ie website, accessed 30 October 2025, https://www.gov.ie/.<br>[6] Oireachtas (2020), 'Harassment, Harmful Communications and Related Offences Act 2020', https://data.oireachtas.ie/.<br>[7] Scoil Naomh Buithe (n.d.), 'Bí Cinealta - Scoil Naomh Buithe (A Guide for Parents and Guardians)', accessed 30 October 2025, https://www.tenurens.ie/policies/bi-cinealta/.<br>[8] Dublin City University (2025), 'DCU Anti-Bullying Centre', 6 December, accessed 3 November 2025, https://www.dcu.ie/antibullyingcentre.<br>[8] Department of Culture, Communications and Sport (2021), 'Report of a National Survey of Children, their Parents and Adults regarding Online Safety', gov.ie website, accessed 30 October 2025, https://www.gov.ie/. |

## Greece

| | |
|---|---|
| **Relevant legislation** | In Greece, the Law No. 5029 of 10 March 2023 on Arrangements to prevent and address violence and bullying in schools and other classrooms introduces actions and regulations to prevent, identify and address violence and bullying in schools, including electronic or online violence. [1]<br>Additionally, several articles from the Greek Penal Code can be applied to cyberbullying, e.g., art. 333 on threat explicitly applies when committed through electronic means. [2] |
| **Definitions in legislation** | Law No. 5029 of 10 March 2023 [1]:<br>Article 4 - [electronic/online] School violence and bullying:<br>Any form of physical, verbal, psychological, emotional, social, racist, sexual, electronic, online or other violence and delinquent behaviour that affects the school community and disrupts the educational process constitutes intra-school violence and bullying, and in particular:<br>a) the insult to the dignity, honour and self-respect of the student,<br>b) the systematic or intentional or repeated threat and insult to the personality, physical integrity or mental balance of students,<br>c) the unwanted, aggressive behaviour that occurs between school-age children and the corresponding behaviour of teachers that includes a real or perceived imbalance of power,<br>d) the obstruction of the smooth conduct of classes and the violent exclusion of students either from the educational process or from their participation in daily school life, as well as the social exclusion, threats and psychological violence in students' contacts with their classmates,<br>e) the imposition by force and coercion of actions or omissions against the will of students,<br>f) any form of violent or degrading behaviour or encouragement to commit violent acts that disrupt school peace and harm the prestige of the educational community,<br>g) bullying or the manifestation of racist behaviours capable of disrupting mental balance and harming students with special characteristics,<br>h) insults, discrimination or harassment on the basis of religious beliefs, ethnic origin, race, gender, sexual orientation, gender identity, expression or characteristics of gender, disability, health status and physical or other real situation of the student.<br>This applies accordingly to forms of violence and behaviours manifested towards teachers and other members of the educational community.<br>Penal code [2]:<br>Article 333 – Threat [via telecommunication or electronic mean]<br>1. Anyone who causes terror or anxiety to another by threatening him with violence or other illegal act or omission is punished with imprisonment of up to one year or a fine. The penalty referred to in the previous paragraph shall also be imposed on anyone who, without threat of violence or other illegal act, causes terror or anxiety to another person by persistently pursuing or following him, such as in particular by seeking constant contact with the use of telecommunications or electronic means or by repeated visits to his family, social or work environment, despite his expressed contrary will.<br>2. Imprisonment of up to three years or a fine shall be imposed if the act is committed against a minor or a person who is unable to defend himself, provided that these persons are under the custody or protection of the offender by law, court decision or |

| | |
|---|---|
| | factual situation, live with him or her or have an employment or service relationship with him. The same penalty is imposed when the act is committed against a spouse during the marriage or against a partner during the cohabitation.<br>3. For the criminal prosecution of the act referred to in paragraph 1, a complaint shall be required. |
| **Examples of initiatives** | A study on the ‘Attitudes and Behaviours of Children on the Internet.’ by the KMOP (Centre for the Study and Organisation of Programmes). The study was completed in October 2024, with a sample of students aged 9-11. [3]<br>A special platform for reporting incidents of school violence and bullying has been launched by the government. [4] |
| **References** | [1] ‘Actions and programs to prevent and address school violence and bullying (Δράσεις και Προγράμματα για την πρόληψη και την αντιμετώπιση της ενδοσχολικής βίας και του εκφοβισμού)’ (2023), https://www.esos.gr/.<br>[2] ‘Article 333 - Criminal Code (Law 4619/2019) - Threat (Άρθρο 333 - Ποινικός Κώδικας (Νόμος 4619/2019) - Απειλή)’ (2019), https://www.lawspot.gr/.<br>[3] KMOP (n.d.), ‘Προστατεύουμε τα παιδιά – Κάνουμε τη γνώση δύναμη’, accessed 30 October 2025, https://www.kmop.gr/child-protection/.<br>[4] Diéfthynsi Ypodomón kai Diktýon tou I.T.Y.E ‘Diófantos’ (n.d.), ‘STAMATAME MAZI TO BULLYING’, accessed 30 October 2025, https://stop-bullying.gov.gr/ |

## Spain

| | |
|---|---|
| **Relevant legislation** | Law 1/2015 of 30 March amending the Criminal Code (Art. 172 ter) introduced the offence od harassment (updated on 07/09/2022, which came into force on 07/10/2022 and on 01/03/2023, with entry into force on 02/03/2023). Other Criminal Code provisions protect against unauthorised sharing of images or recordings (art. 197.7) and hate crimes on social media (art. 510). [1]<br>In June 2024, the Spanish government proposed a Draft Organic Law for the Protection of Children in Digital Environments to enhance online safety for minors. In September 2025, the Congress of Deputies approved the processing of the law. Among the main measures contemplated by the law are the increase in the minimum age for social media registration to 16 (currently 14) and the obligation for manufacturers of devices that allow internet access to establish free protection measures for minors, such as a parental control system. In addition, educational centres must also expressly regulate the use of cell phones, computers, tablets, or any other digital device in the classroom and in other activities. The law also introduces important modifications to the Criminal Code. First, the prohibition of access to or communication in digital environments is added to the list of penalties. Furthermore, a new crime is established: the indiscriminate provision of pornographic material to minors, and deepfakes with sexual or seriously humiliating content are classified as content that violates moral integrity. Finally, the minister emphasized that the law establishes online deception of minors (grooming) as an aggravating factor in some crimes against sexual freedom. [2]<br>Schools and all their staff are responsible for preventing and also investigating all forms of harassment or offensive behaviour, explicitly including cyberbullying, according to the Organic Law 2/2006, of May 3, on Education. [3] |
| **Definitions in legislation** | Penal code [1]:<br>Article 172 ter - [Harassment, incl. through any method of communication]<br>1. Whoever harasses a person by insistently and repeatedly engaging in any of the following behaviours, without being legitimately authorised, and, in this manner, |

| | |
|---|---|
| | severely alters his daily life, shall be punished with a prison sentence of three months to two years or a fine of six to twenty-four months:<br>a) Monitoring, pursuing or seeking his physical proximity;<br>b) Establishing or trying to establish contact with him through any method of communication, or through third parties;<br>c) Through the inappropriate use of his personal data to purchase products or merchandise, or to sign up to services, or having third parties contact him;<br>d) Infringing upon his freedom or his property, or upon the freedom or property of another person who is close to him. In the case of an especially vulnerable individual due to his age, illness or situation, a prison sentence of six months to two years shall be imposed.<br>2. If the offended person is one of those referred to in Section 2 of Article 173 [family members or other persons integrated into the core family life of the offender], a prison sentence of one to two years shall be imposed, or community service from sixty to one hundred and twenty days. In this case, the formal complaint referred to in Section 4 of this Article shall not be required.<br>3. The punishments outlined in this Article shall be imposed without prejudice to those that could correspond to the criminal offences to which the acts of physical or psychological violence could have given rise to.<br>4. An individual may only be prosecuted for the deeds described in this Article if the injured party or his legal representative files a formal complaint.<br>5. Anyone who, without the consent of the owner, uses the image of a person to make advertisements or open false profiles on social networks, contact pages or any means of public dissemination, causing the same situation of harassment, harassment or humiliation, shall be punished with a prison sentence of three months to one year or a fine of six to twelve months. If the victim of the crime is a minor or a person with a disability, the upper half of the sentence will be applied. |
| **Examples of initiatives** | The Expert Committee for Protection of Minors in Digital Environments includes a working group on children's participation. [4]<br>The Common Framework for Digital Teaching Competence outlines the skills and knowledge that teachers should possess to integrate technology into teaching effectively, including aspects related to online safety. [5]<br>‘Responsables en las Redes’ is a series of courses designed for upper primary school students, aimed at raising awareness about the importance of acting responsibly on social media. [6]<br>Spain’s National Observatory of Technology and Society has published the survey The Use of Technologies by Minors in Spain (edition 2024) analysing the relationship between minors and digital technologies. [7]<br>The Orange Foundation and Save the Children Spain, conducted a survey on Children and Adolescents in Digital Environments, based on interviews with more than 2,500 people and the participation of 17 experts in the field. [8] |
| **References** | [1] ‘Organic Law 10/1995, of November 23, of the Penal Code (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal)’ (2024), https://www.boe.es/<br>[2] ‘Congress approves the organic law for the protection of minors in digital environments (El Congreso da luz verde a la tramitación de la ley orgánica para la protección de los menores en entornos digitales)’ (2025), accessed 28 October 2025, https://www.mpr.gob.es/.<br>[3] ‘Organic Law 2/2006, of May 3, on Education (Ley Orgánica 2/2006, de 3 de mayo, de Educación)’ (2006), https://boe.es/. |

| | |
|---|---|
| | [4] Ministerio de Juventud e Infancia (n.d.), ‘Committee of Experts for the Creation of Safe Digital Environments for Children and Youth’, accessed 31 October 2025, https://www.juventudeinfancia.gob.es/.<br>[5] Spanish Ministry of Education and Vocational Training and Educational Administrations of the Autonomous Communities of Spain (2022), ‘Spanish Framework for the Digital Competence of Teachers’, https://intef.es/.<br>[6] Influencers Trust Project (n.d.), ‘Fomentando la Responsabilidad en las redes sociales’, Influencerstrustproject website, accessed 31 October 2025, https://www.influencerstrustlabeleu.org/.<br>[7] Observatorio Nacional de Tecnología y Sociedad (2024), ‘El uso de las tecnologías por menores en España’, Observatorio Nacional de Tecnología y Sociedad, https://www.ontsi.es/<br>[8] Save the Children and Fundación Orange (n.d.), ‘Infancia y Adolescencia en Entornos Digitales’, https://fundacionorange.es/. |

## France

| | |
|---|---|
| **Relevant legislation** | Law No. 2022-299 of March 2, 2022 aimed at combating school bullying amended the Education Code (L.111-6) and Criminal Code’s article 222-33-2 on harassment, including 222-33-2-1 “harassment of one’s spouse” and 222-33-2-2 “harassment through a digital or electronic medium” and article 222-22-3 on “school harassment”.<br>Other articles that may be applied to cyberbullying when committed by electronic means include: art. 223-13 and 223-14 on inducing suicide, art. 226-1 on invasion of private life, ar. 226-2 on unauthorised sharing of documents or recordings, including of sexual nature. [1], [2] |
| **Definitions in legislation** | Criminal Code [1]:<br>Art. 222-33-2 harassment [in the workplace]:<br>Harassing another person through repeated comments or behaviours that have the purpose or effect of degrading working conditions likely to violate their rights and dignity, impair their physical or mental health, or compromise their professional future, is punishable by two years' imprisonment and a fine of €30,000.<br>Art. 222-33-2-2 (amended by Law 2024-247 of March 21) – harassment [through a digital or electronic medium]<br>The act of harassing a person by repeated words or behaviour having as their object or effect a deterioration in their living conditions resulting in an alteration of their physical or mental health is punishable by one year's imprisonment and a fine of €15,000 when these acts have caused total incapacity for work of less than or equal to eight days or have not resulted in any incapacity for work.<br>The offence is also constituted:<br>a) When these words or behaviour are imposed on the same victim by several persons, in a concerted manner or at the instigation of one of them, even though each of these persons has not acted repeatedly;<br>(b) When these words or behaviour are imposed on the same victim, successively, by several persons who, even in the absence of consultation, know that these words or behaviour characterise repetition.<br>The acts mentioned in the first to fourth paragraphs are punishable by two years' imprisonment and a fine of €30,000:<br>1. When they have caused total incapacity for work for more than eight days; |

| | |
|---|---|
| | 2. When they have been committed against a minor;<br>3. When they have been committed against a person whose particular vulnerability, due to his or her age, illness, infirmity, physical or mental deficiency or pregnancy, is apparent or known to the perpetrator;<br>4. When they have been committed through the use of an online public communication service or through a digital or electronic medium;<br>4bis. When they have been committed against the holder of an elective office;<br>5. When a minor was present and was present.<br>The acts mentioned in the first to fourth paragraphs are punishable by three years' imprisonment and a fine of €45,000 when they are committed in two of the circumstances mentioned in 1° to 5°.<br>Art. 222-33-2-3 (amended by Law 2022-299) [2] – school harassment/school bullying:<br>Acts of psychological harassment defined in the first four paragraphs of Article 222-33-2-2 constitute school harassment when they are committed against a pupil by any person studying or exercising a professional activity within the same educational establishment.<br>School bullying is punishable by three years' imprisonment and a fine of €45,000 when it has caused total incapacity for work of less than or equal to eight days or has not resulted in any incapacity for work.<br>The penalties are increased to five years' imprisonment and a fine of €75,000 when the facts have caused total incapacity for work for more than eight days.<br>The penalties are increased to ten years' imprisonment and a fine of €150,000 when the facts have led the victim to commit suicide or attempt suicide.<br>This article shall also apply when the commission of the acts mentioned in the first paragraph of this article continues while the perpetrator or victim is no longer studying or practising within the establishment. |
| **Examples of initiatives** | An interministerial plan to combat harassment in schools was adopted in September 2023. Measures implemented against harassment in schools include dedicated lessons to prevent bullying and cyberbullying from the third class to the high school, systematic recording of instances of harassment, designation of harassment coordinators, training of staff to fight against bullying, and an annual barometer of harassment in schools. [3]<br>The anti-bullying programme at school, pHARe, is a comprehensive plan for preventing and dealing with bullying. [4] |
| **References** | [1] 'Penal Code (Code Pénal)' (2025), https://www.legifrance.gouv.fr/<br>[2] 'LAW No. 2022-299 of March 2, 2022 aimed at combating school bullying (1) (LOI n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire (1))' (2022), https://www.legifrance.gouv.fr/<br>[3] Ministère de l'Éducation Nationale (n.d.), 'Politique de lutte contre le harcèlement à l'Ecole', Ministère de l'Éducation nationale website, accessed 30 October 2025b, https://www.education.gouv.fr/<br>[4] Ministère de l'Éducation Nationale (n.d.), 'Phare : un dispositif de lutte contre le harcèlement à l'école', Ministère de l'Éducation nationale website, accessed 30 October 2025a, https://www.education.gouv.fr/ |

## Croatia

| | |
|---|---|
| **Relevant legislation** | Cyberbullying is not currently covered by Croatian legislation. However, the Criminal Code addresses several offenses that may also apply to cyberbullying: Art. 143 – Unauthorised audio recording and eavesdropping (including making use of the recordings), Art. 144 - Unauthorised Taking of Pictures (including using the pictures or making them available), Art. 147 – Insult, Art. 148 – Defamation, Art. 149 - (Intentional) Defamation, Art. 156 - Sexual Harassment.<br>In particular, offenses under articles 147-149 are considered aggravated, leading to higher fines, when they are committed through the press, radio, television, computer system or network, at a public gathering or in some other way, thus making them accessible to a large number of persons. [1] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 147 – Insult [through computer system or network]<br>(1) Whoever insults another, shall be punished by a fine of up to ninety daily units.<br>(2) Whoever commits the offence referred to in paragraph 1 of this Article through the press, radio, television, computer system or network, at a public gathering or in some other way, thus making the insult accessible to a large number of persons, shall be punished by a fine of up to one hundred and eighty daily unit.<br>Article 149 - Libel [through computer system or network]<br>(1) Whoever, in front of another, makes an untrue factual statement about someone that may be detrimental to his honour or reputation, knowing that it is untrue, shall be punished by a fine of up to three hundred and sixty daily units.<br>(2) Whoever commits an act referred to in paragraph 1 of this article through the press, radio, television, computer system or network, at a public gathering or in any other way that has made it accessible to a large number of persons, shall be punished by a fine of up to five hundred daily units. |
| **Examples of initiatives** | The Ministry of Labor, Pension System, Family and Social Policy published a Protocol on Proceedings in cases of violence among children and youth (Zagreb, March 2024), where a reference to cyberbullying was included providing a definition as well as prevention guidelines. [2]<br>The Ministry of the Interior of the Republic of Croatia leads the National Cyber Security Strategy, including education, research, development and raising the awareness of security in cyberspace. In the Ministry website Cyberbullying (Zlostavljanje Putem Interneta) is included under the option of Online report of child abuse. [3]<br>The Government has published a 2020-2024 action plan for preventing violence in schools [4], and there are guides on electronic sexual violence and cyberbullying on and among children and young people. [5]<br>The Agency for Electronic Media and UNICEF founded the portal medijskapismenost.hr. The portal is a platform for promoting media literacy and providing support to everyone who participates in media education, primarily children and young people, but also adults. [6] |
| **References** | [1] ‘Criminal law (Kazneni zakon)’ (n.d.), https://www.zakon.hr/z/98/kazneni-zakon.<br>[2] MINISTARSTVO RADA, MIROVINSKOGA SUSTAVA, OBITELJI I SOCIJALNE POLITIKE (2024a), ‘Protokol o postupanju u slučaju nasilja među djecom i mladima’, https://mrosp.gov.hr/.<br>[3] Ministarstvo unutarnjih poslova (n.d.), ‘Zlostavljanje putem interneta’, mup.gov.hr website, accessed 30 October 2025, https://mup.gov.hr/online-prijave/online-prijava-zlostavljanja-djeteta-red-button/zlostavljanje-putem-interneta/281672.<br>[4] Ministarstvo znanosti, obrazovanja i mladih (2020), ‘Akcijski plan za prevenciju nasilja u skolama za razdoblje od 2020. do 2024’, |

| | |
|---|---|
| | https://mzom.gov.hr/UserDocsImages/dokumenti/StrucnaTijela/Akcijski%20plan%20za%20prevenciju%20nasilja%20u%20skolama%20za%20razdoblje%20od%202020.%20do%202024.%20godine.pdf.<br>[5] Udruga za unapređenje kvalitete življenja LET (2021), 'Vršnjačko elektroničko nasilje (cyberbullying)', https://udruga-let.hr/wp-content/uploads/2021/05/Edukacijski-priruc%CC%8Cnik-Cyberbullyinga-24-str.-20210525-WEB.pdf.<br>[6] Agencija za elektroničke medije (n.d.), 'Medijska pismenost', accessed 30 October 2025, https://www.medijskapismenost.hr/. |

## Italy

| | |
|---|---|
| **Relevant legislation** | Law 71 of 29 May 2017 on "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying", passed after some tragic cases of cyberbullying and violence against women in which victims have committed suicide. The Law has a strong focus on the protection of minors. It introduces preventive and corrective measures involving schools, families, and institutions.<br>Keypoints of the law 71/2017 can be summarized as: definition of cyberbullying; right to request removal of harmful content; escalation to the Data Protection Authority after 48 hours; appointment of a cyberbullying coordinator in every school; implementation of educational and awareness programs in schools; mediation measures involving students and families; formal warning (admonition) by the Police Commissioner for minors over 14; promotion of national awareness campaigns; collaboration between schools, authorities, and civil society; focus on prevention and protection of minors; support for victims and families through reporting channels. [1]<br>The Italian Penal Code includes the specific offence for stalking ("persecutory conducts") (article 612-bis), explicitly referring to the option of being committed through computer or electronic means.<br>Other offenses include: illicit dissemination of sexually explicit images or videos (art. 612-ter), and illegal dissemination of content generated or altered with artificial intelligence systems (art. 612-quarter). [2] |
| **Definitions in legislation** | Law 71/2017 [1]:<br>Art.1.2 - Cyberbullying:<br>For the purposes of this law, "cyberbullying" means any form of pressure, aggression, harassment, blackmail, injury, denigration, defamation, identity theft, alteration, illegal acquisition, manipulation, or unlawful processing of personal data against minors, carried out electronically, as well as the dissemination of online content targeting one or more members of the minor's family, whose intentional and predominant purpose is to isolate a minor or a group of minors by committing serious abuse, a harmful attack, or ridicule them.<br>Penal Code [2]:<br>Art. 612-bis – Stalking:<br>Unless the act constitutes a more serious crime, anyone who, through repeated conduct, threatens or harasses someone in such a way as to cause a long-lasting and serious state of anxiety or fear, or to generate a well-founded fear for their own safety or that of a close relative or a person linked to them by an emotional relationship, or to force them to alter their lifestyle, shall be punished with imprisonment (from one year to six years and six months), or if the act is committed through computer or electronic means.<br>The penalty is increased if the act is committed by a spouse, even if separated or divorced, or by a person who is or has been linked by an emotional relationship to the |

| | |
|---|---|
| | injured party, or if the act is committed through computer or telematic means. The penalty is increased by up to half if the offense is committed against a minor, a pregnant woman, or a person with a disability as defined in Article 3 of Law No. 104 of February 5, 1992, or with weapons or by a disguised person.<br>The offense is punishable upon complaint by the injured party. The deadline for filing a complaint is six months. The complaint can only be withdrawn during the proceedings. The complaint is, however, irrevocable if the offense was committed through repeated threats as described in Article 612, paragraph 2. However, prosecution is ex officio if the offense is committed against a minor or a person with a disability as defined in Article 3 of Law No. 104 of February 5, 1992. 104, as well as when the act is connected to another crime for which proceedings must be initiated ex officio. |
| **Examples of initiatives** | The Ministry of Education has launched a specific campaign to address cyberbullying, creating a permanent observatory for every region of Italy and publishing educational materials (text and multimedia) on a specific website. [3]<br>Italy has incorporated online safety education into the national school curriculum at primary, lower secondary, and upper secondary levels through Civic Education, ICT, and Media Literacy programs. Topics include safe internet use, cyberbullying prevention, data privacy, misinformation awareness, and cybersecurity. [4]<br>'Vita da Socia' is an Italian awareness campaign in cooperation with the Ministry of Education and the Ministry of Interior to educate young people about the safe and responsible use of the internet and social media, including cyberbullying. [5] |
| **References** | [1] 'LAW 29 May 2017, n. 71: Provisions for the protection of minors for the prevention and fight against cyberbullying (LEGGE 29 maggio 2017, n. 71: Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo)' (2017), https://www.gazzettaufficiale.it/.<br>[2] 'ROYAL DECREE 19 October 1930, n. 1398: Approval of the final text of the Criminal Code (REGIO DECRETO 19 ottobre 1930: n. 1398 Approvazione del testo definitivo del Codice Penale)' (1930), https://www.gazzettaufficiale.it/.<br>[3] Italian Digital Media Observatory (n.d.), 'IDMO – Italian Digital Media Observatory', accessed 30 October 2025, https://www.idmo.it/en/.<br>[4] Ministry of Education, University and Research (2016), 'National Plan for Digital Education', https://www.istruzione.it/.<br>[5] European Commission (n.d.), 'Media literacy and safe use of new media - Italy', accessed 30 October 2025, https://national-policies.eacea.ec.europa.eu/. |

## Cyprus

| | |
|---|---|
| **Relevant legislation** | Law 2021 (L.114(I)/2021) on 'Protection from Harassment and Stalking' introduces both criminal and civil offenses of harassment and stalking. Although there is no explicit reference to electronic means, it may apply to cyberbullying. [1]<br>Moreover, there is a proposal for amendment still pending, the Criminal Code (Amendment) (No. 2) Law of 2022 for "The Criminalization of Bullying (School, Workplace, Military and Sports Bullying) and Related Issues Law". [2] |
| **Definitions in legislation** | Law 2021 (L.114(I)/2021) [1]:<br>Art. 3 - Harassment<br>(1) A person who engages in conduct that causes harassment, while knowing or should have known that such conduct causes harassment, is guilty of a criminal offence and, in the event of conviction, is liable to a term of imprisonment not exceeding two |

(2) years or to a fine not exceeding five thousand euros (€5,000) or to both, provided that the act is not punished more severely than the provisions of any other Law in force.

(2) In a case where the harassment referred to in subsection (1) consists of causing the victim to fear that violence will be used against him and/or against a member of his family and/or against his property, the person who engages in such conduct shall, on conviction, be liable to a term of imprisonment not exceeding five (5) years or to a fine not exceeding ten thousand euros (€10,000) or to both, provided that the act is not punished more severely than the provisions of any other Law in force.

(3) For the purposes of subsection (1), a person shall be deemed to have known that the conduct which he or she is engaging in is causing harassment if a reasonable person under the same circumstances would consider that such conduct is causing harassment.

(4) [...]

Art. 4 - Harassing surveillance/tracking (Παρενοχλητική παρακολούθηση)

(1) A person who engages in conduct that constitutes surveillance and causes harassment, while knowing or ought to have known that such conduct causes harassment, is guilty of a criminal offence and, in the event of conviction, is liable to a term of imprisonment not exceeding two (2) years or to a fine not exceeding five thousand euros (€5,000) or to both, provided that the act is not punished more severely than the provisions of any other Law in force.

(2) In a case where the harassment caused, in accordance with the provisions of subsection (1), consists of causing the victim to fear that violence will be used against him and/or against a member of his family and/or against his property or consists of causing him serious concern or serious anxiety, which has a substantial negative effect on the performance of the victim's daily activities, the person who carries out the said conduct is subject, in the event of conviction, to a prison sentence not exceeding five (5) years or to a fine not exceeding ten thousand euros (€10,000) or to both penalties, provided that the act is not punished more severely than the provisions of any other Law in force.

(3) For the purposes of subsection (1), a person shall be deemed to have known that the conduct he or she is engaging in is causing harassment if a reasonable person under the same circumstances would consider that the conduct is causing harassment.

(4) For the purposes of this Article, conduct constituting surveillance shall be deemed to be

[...]

(c) monitoring the use of e-mail and/or any other electronic communication of another person or sending posts on social media relating to the personal life of the victim or interfering with the victim's posts on the internet.

(5) [...]

Art. 7 - Civil offense of harassment and stalking

(1) A person who engages in conduct that causes harassment, while knowing or ought to have known that such behaviour causes harassment, commits the civil offense of harassment.

(2) A person who engages in conduct that constitutes surveillance and causes harassment, even though he or she knows or ought to have known that such conduct causes harassment, commits the civil offence of stalking.

It is understood that, for the purposes of this paragraph, the conduct provided for in subparagraph (4) of Article 4 constitutes surveillance.

(3) For the purposes of subparagraphs (1) and (2), a person shall be deemed to have known that the conduct he or she is engaging in is causing harassment if a

| | |
|---|---|
| | reasonable person in the same circumstances would consider that such conduct is causing harassment. |
| **Examples of initiatives** | The Cybersecurity Strategy of Cyprus includes Action 14 specifically referring to a better internet for kids where Cyberbullying (*διαδικτυακός εκφοβισμός*) is one of the priorities. [3]<br>Schools need to follow a specific protocol and guidelines in addressing cyberbullying issued by the Ministry of Education. [4].<br>The subject of digital competence has been introduced to primary school curriculum with cyberbullying one of the units. [5]<br>The Cyprus Pedagogical Institute introduced various actions on the safe use of the internet. [6] The programme esafe schools [7] promote among others a school action plan including combating cyberbullying. The Young Coaches for the Internet programme [8] updated to Digital Pioneers [9] aims to involve children in creating a safer and better internet promoting as well a video competition addressing various aspects of internet safety. |
| **References** | [1] 'The Protection from Harassment and Harassing Surveillance Law of 2021 (Ο περί της Προστασίας από Παρενόχληση και Παρενοχλητική Παρακολούθηση Νόμος του 2021)' (2021), https://www.cylaw.org/.<br>[2] 'Proposal for a law amending the Criminal Code (Πρόταση νόμου που τροποποιεί τον ποινικό κώδικα)' (2022), https://www.nomoplatform.cy/.<br>[3] Ypoomáda 1 tis Drásis 14 tis Stratigikís Kyvernoasfáleias tis Kypriakís Dimokratías (2017), 'ETHNIKI STRATIGIKI GIA ENA KALYTERO DIADIKTYO GIA TA PAIDIA STIN KYPRO (ASFALEIA STO DIADIKTYO GIA PAIDIA, EKPAIDEUTIKOUS KAI GONEIS) 2018-2023', https://cyberalert.cy/.<br>[4] Ypourgeío Paideías, Athlitismoú kai Neolaías (2020), 'Politikí tou Scholeíou DIACHEIRISI SCHOLIKOU EKFOVISMOU', https://enimerosi.moec.gov.cy/.<br>[5] Paidagogikó Instituúto (2019), 'Psifiakí Ikanótita - Mathisiakés Eisigíseis (gia tin Ε΄ kai tin Στ΄ táxi Dimotikís Ekpaídefsis)', https://internetsafety.pi.ac.cy/<br>[6] Paidagogikó Instituúto (n.d.), 'asfáleia sto diadíktyo', Internet Safety website, accessed 30 October 2025a, https://internetsafety.pi.ac.cy/.<br>[7] Paidagogikó Instituúto (n.d.), 'Asfalés Scholeío gia to Diadíktyo', eSafe Schools website, accessed 3 November 2025, https://esafeschools.pi.ac.cy/.<br>[8] Paidagogikó Instituúto (n.d.), 'Prógramma Mikroí ekpaideftés gia to Diadíktyo', Young Coaches website, accessed 30 October 2025b, https://youngcoaches.pi.ac.cy/.<br>[9] Paidagogikó Instituúto (n.d.), 'Prógramma Psifiakoí Protopóroi', Digital Pioneers website, accessed 30 October 2025c, https://digitalpioneers.pi.ac.cy/. |

## Latvia

| | |
|---|---|
| **Relevant legislation** | While Latvia does not have specific legislation on cyberbullying, it can fall under defamation-related criminal and civil law jurisdiction:<br>Criminal Law includes several articles applicable to cyberbullying when committed with electronic means, although the articles do not make explicit mention to electronic means: section 132-Threatening to commit murder and to inflict serious bodily injury; section $132^{1}$ Persecution; section 144. Violating the confidentiality of correspondence and information to be transmitted over telecommunications networks; section 145. Illegal activities involving personal data of natural person; section 150-Incitement of social hatred and enmity (including based on race, ethnic origin, or other grounds); section 157-Defamation, with more severe penalty for defamation in mass media. [1] |

| | |
|---|---|
| | Under the Civil Law, Article 1635 indicates that every delict, that is, every wrongful act per se, as a result of which harm has been caused (also moral injury) shall give the person who suffered the harm therefrom the right to claim satisfaction from the infringer, insofar as he or she may be held at fault for such act.. By moral injury is understood physical or mental suffering, which are caused as a result of unlawful acts committed to the non-financial rights or non-financial benefit delicts of the person who suffered the harm. The amount of compensation for moral injury shall be determined by a court at its own discretion, taking into account the seriousness and the consequences of the moral injury. If the unlawful acts referred to in Paragraph two of this section are expressed as criminal offences against a person's life, health, morals, inviolability of gender, freedom, honour, dignity or against the family, or minors, it is presumed that the person who suffered the harm as a result of such acts has been done moral injury. In other cases, moral injury shall be proved by the person who suffered the harm. (Note. The term act is used here within the widest meaning, including not only acts, but also the failure to act, that is, inaction.)<br>Under the Civil Law, Article 1635 refers to the right of the injured party to claim compensation from the offender, for every unlawful act that causes damage (including moral damage). Moral damage refers to physical or emotional suffering caused by a violation of non-material rights or values. If the unlawful act is a criminal offense against a person's life, health, morals, sexual integrity, freedom, honour, dignity, family, or a minor, it is presumed that moral damage has occurred. [2]<br>The Law on the protection of the children's rights protects against several types of behaviour, including physical and emotional violence against a child (section 81). [3] |
| **Definitions in legislation** | Criminal Code [1]:<br>Section 132.$^{1}$ Persecution<br>(1) For multiple or prolonged tracking, observation, expression of threats to another person or unwanted communication with such person, if he or she has had grounds to fear for the safety of himself or herself or his or her relatives-<br>shall be punishable by imprisonment for up to one year, or by temporary imprisonment, or by probation supervision.<br>(2) For the same acts, if they have been committed against a person with whom the perpetrator of the criminal offence is in the first or second degree of kinship, or against a spouse or former spouse, or against a person with whom the perpetrator of the criminal offence is or has been in a permanent intimate relationship, or against a person with whom the perpetrator of the criminal offence has a joint (undivided) household -<br>shall be punishable by imprisonment for up to three years, or by temporary imprisonment, or by probation supervision.<br>Section 157 – Defamation [in mass media]<br>(1) For deliberately false, disgraceful dissemination of fictions in printed or otherwise reproduced compositions, as well as orally, if it has been committed in public (defamation) -<br>shall be punishable by probation supervision or by community service or by a fine.<br>(2) For defamation in a mass media -<br>shall be punishable by temporary imprisonment or by probation supervision, or by community service, or by a fine.<br>Law on the Protection of the Children's Rights [3]:<br>Section 1 (12) - emotional abuse:<br>The infringement of the self-respect of a child or psychological coercion (threatening him or her, swearing, humiliating him or her, abusing a relative of the child in his or her presence or otherwise harming the emotional development thereof). |

|  |  |
|---|---|
| **Examples of initiatives** | The Digital Transformation Guidelines 2021-2027 include ‘Digital skills and education’ and ‘Digital security and trust’ to ensure the public's awareness and education on child safety online and improve digital literacy. [4]<br>A 2023 study about bullying and violence in schools is among a number of government initiatives to address bullying and mobbing. Another one is the Finnish 'KiVa' initiative, which was opened to Latvian schools in September 2023. [5] |
| **References** | [1] ‘Criminal Law (Krimināllikums)’ (1998), https://likumi.lv/<br>[2] ‘Civil law (Civillikums)’ (1992), https://likumi.lv/<br>[3] ‘Law on the Protection of the Children’s Rights (Bērnu tiesību aizsardzības likums)’ (1998a), https://likumi.lv/<br>[4] Ministry of Smart Administration and Regional Development (n.d.), ‘Latvian Digital Transformation Guidelines for 2021-2027 – Accellation of Digital Capacities for Future Society and Economy’, accessed 30 October 2025, https://www.varam.gov.lv/<br>[5] China-CEE Institute (2023), ‘Latvia social briefing: Violence in Latvian Schools is a Major Concern’, 29 March, accessed 30 October 2025, https://china-cee.eu/ |

### Lithuania

|  |  |
|---|---|
| **Relevant legislation** | Law on Fundamentals of Protection of the Rights of the Child (I-1234 of 14 March 1996) includes bullying as a form of psychological violence against children. [1]<br>Criminal code’s articles 512 on Sexual harassment and 152$^1$ on Grooming of a person under the age of sixteen years may also constitute cyberbullying if committed through electronic means. [2] |
| **Definitions in legislation** | Law on Fundamentals of Protection of the Rights of the Child [1]:<br>Article 3. Forms of violence against children:<br>2) psychological violence – intentional systematic violation of the child's right to identity, humiliation of the child, bullying, intimidation, disruption of activities necessary for the normal development of the child, promotion of anti-social behaviour or other behaviour (acts or omissions) of non-physical contact, as a result of which the child died, his or her health or normal development was disturbed or endangered the life, health, normal development of the child or the honour and/or dignity of the child was degraded. Appropriate and justified assessment of the child's knowledge and abilities and other actions aimed at assessing the development of the child's normal development are not considered psychological violence; |
| **Examples of initiatives** | Occasional research on problematic usage of internet by the Digital Ethics Centre (Skaitmeninės etikos centras). [3] |
| **References** | [1] ‘Law of the Republic of Lithuania on the basis of the protection of children’s rights (Lietuvos Respublikos vaiko teisių apsaugos pagrindų įstatymas)’ (2025), https://e-seimas.lrs.lt/.<br>[2] ‘Criminal Code’ (2018), https://vatesi.lrv.lt/public/canonical/1697012277/1045/Criminal_Code.pdf<br>[3] Media vaikai (n.d.), ‘PUI RECOGNITION. Research: The adaptation of instruments to identify problematic internet use in adolescents for prevention and intervention purposes’, mediavaikai website, accessed 30 October 2025, https://www.mediavaikai.lt/pin-atpazinimas-apie. |

### Luxembourg

| | |
|---|---|
| **Relevant legislation** | Criminal code Chapter IV-2.-Obsessive harassment (L. 5 June 2009) [1] |
| **Definitions in legislation** | Criminal code [1]:<br>Art. 442-2 - *harcèlement obsessionnel*:<br>Anyone who repeatedly harasses a person when he knew or should have known that he would seriously affect the peace of the person targeted by this behaviour will be punished by a prison sentence of fifteen days to two years and a fine of 251 to 3,000 euros, or by one of these penalties only.<br>The offence provided for in this article may be prosecuted only on the complaint of the victim, his legal representative or his beneficiaries. |
| **Examples of initiatives** | Luxembourg includes internet safety training in the 'digital sciences' subject in secondary schools.<br>The BEE SECURE RADAR collects data on information and communication technology (ICT) by children and young people in Luxembourg since 2022 also in relation to cyberbullying. [2], [3] |
| **References** | [1] 'Penal Code (Code pénal)' (2020), https://data.legilux.public.lu/<br>[2] BEE SECURE (n.d.), 'BEE SECURE Radar 2025', BEE SECURE website, accessed 30 October 2025, https://www.bee-secure.lu/<br>[3] BEE SECURE (2025), 'BEE SECURE RADAR 2025 - Current trends in young people's use of information and communication technologies', https://www.bee-secure.lu/ |

### Hungary

| | |
|---|---|
| **Relevant legislation** | On 17 December 2024, Hungary's Parliament adopted the Act LXXVIII of 2024 on the Suppression of Internet Aggression, which aims to curb online aggression. The Act entered into force on the 1st of January 2025 and amended existing legislation in a number of areas, introducing new obligations and procedural rules. The provision was added to Act C of 2012 on the Criminal Code to criminalise aggression on the Internet (new article 332/A). Under the new legislation, it is a criminal offence to publicly publish content on an electronic communications network that incites violent acts. [1] |
| **Definitions in legislation** | Criminal Code [1] :<br>Article 332/A - Internet aggression<br>(1) Any person who uses or publishes in public via an electronic communications network an expression, representation or image or sound recording that expresses an intention or wish to commit a punishable act of violence against an identifiable person or persons,<br>a) causing death, or<br>b) committed with particular cruelty,<br>shall be liable to imprisonment for a term not exceeding one year for a misdemeanor, if a more serious crime is not committed.<br>(2) Any person who commits the crime specified in paragraph (1) for the purpose of disseminating knowledge, education, science, art or for the purpose of informing about historical or contemporary events shall not be liable to punishment, provided that the act is not capable of instilling fear. |

| | |
|---|---|
| **Examples of initiatives** | Hungary's Digital Education Strategy, adopted in 2016, covers all levels of the education system and aims to create equal opportunities and a secure digital environment. [2]<br>The Public Education Strategy 2021 - 2030 includes a focus on 'supporting the digital culture of the pupils and teachers and the safe use of the Internet. [3]<br>The Digital Child Protection Strategy of Hungary with reference to harassment or bullying. [4]<br>The National Media and Infocommunications Authority (NMHH) established the Magic Valley Media Literacy Training Centres to support media literacy education for 9-16-year-olds and they published a guide "Cyberbullying - Hurting Others Is Not Cool". [5] |
| **References** | [1] 'Act C of 2012 on the Criminal Code (2012. évi C. törvény a Büntető Törvénykönyvről)' (2025), https://njt.hu/jogszabaly/<br>[2] Digital Success Programme (2016a), 'DIGITAL EDUCATION STRATEGY OF HUNGARY', https://digitalisjoletprogram.hu/<br>[3] Emberi Erőforrások Minisztériuma (2020), 'Köznevelési stratégia 2021-2030', https://2015-2019.kormany.hu/<br>[4] Digital Success Programme (2016b), 'The Digital Child Protection Strategy of Hungary', https://2015-2019.kormany.hu/.<br>[5] Bűvösvölgy médiaértés-oktató központ (n.d.), 'Kiadvány: Cyberbullying - Mást bántani nem menő' [Hungaru], accessed 30 October 2025, https://buvosvolgy.hu/. |

## Malta

| | |
|---|---|
| **Relevant legislation** | Criminal Code (Chapter 9) deals with harassment (art. 251A), stalking (251AA), cyberstalking (251BB, included in 2025 amendment) and cyberbullying (251BC, included in 2025 amendment). [1], [2] |
| **Definitions in legislation** | Criminal Code [1], [2]:<br>Article 251BB – Cyberstalking:<br>(1) Any person who with intention to cause physical or mental harm to another person, including self-harm or to arouse apprehension or fear in the other person for his or her own safety or that of any other person, does any of the following acts shall be guilty of an offence against this article:<br>(a) stalks another person by contacting another person through the use of a computer or other electronic communication device or by any other digital or communication device whatsoever;<br>(b) causes an unauthorised computer function in a computer owned or used by another person;<br>(c) traces the other person's use of the internet or other electronic communication.<br>(2) For the purpose of this article, a person whose course of conduct is in question ought to know that it will cause physical or mental harm to another person, including self harm or that it will arouse apprehension or fear in the other person for his own safety or that of any other person, if a reasonable person in possession of the said information would think that the course of conduct would cause any one of the said consequences on the other person on that occasion.<br>(3) A person found guilty of an offence under this article shall be liable to imprisonment for a term for one(1) year to five (5) years, or to a fine (multa) not exceeding thirty thousand euro (€30,000), or to both such fine and imprisonment.<br>(4) The provision of sub-article (1) shall not apply to conduct engaged in by a person performing official duties […]. |

| | |
|---|---|
| | (5) It shall constitute a defence to the charge, for the accused to prove that the course of conduct was engaged without malicious intent [...].<br>(6) The punishment shall be increased by one degree where any one or more of the following circumstances results:<br>(a) where the harm is caused to a person under age or a person who is vulnerable as a result of his mental capacity; or<br>(b) where the offence is committed by two (2) or more persons acting together.<br>Article 251BC - Cyberbullying:<br>(1) Any person who, with intention to cause physical or mental harm to another person, including self harm or to cause apprehension or fear in the other person for his safety or that of any other person, does any of the following acts shall be guilty of an offence against this article:<br>(a) threatens, intimidates or uses abusive or offensive words directed to the other person by means of the use of a computer or other electronic communication device or by any other digital or communication device whatsoever;<br>(b) performs abusive or offensive acts to the person or directs abusive or offensive acts towards the other person by means of the use of a computer or other electronic communication device or by any other digital or communication device whatsoever.<br>(2) For the purpose of this article, a person whose course of conduct is in question ought to know that it will cause physical or mental harm to another person, including self harm or it will cause apprehension or fear in the other person for his own safety or that of any other person, if a reasonable person in possession of the said information would think that the course of conduct would cause any one of the said consequences on the other person on that occasion.<br>(3) A person found guilty of an offence under this article shall be liable to imprisonment for a term for one (1) year to five (5) years, or to a fine (multa) not exceeding thirty thousand euro (€30,000), or to both such fine and imprisonment.<br>(4) The punishment shall be increased by one degree where any one or more of the following circumstances results:<br>(a) where the harm is caused to a person under age or a person who is vulnerable as a result of his mental capacity; or<br>(b) where the offence is committed by two or more persons acting together. |
| **Examples of initiatives** | The Children's Policy Framework 2024-2030 includes measures that address the risks of online abuse, such as cyberbullying and exposure to harmful content. It incorporates elements of mental health support and aims to provide a protective framework for children in the digital space. |
| **References** | [1] 'Criminal Code' (2025), https://legislation.mt/.<br>[2] 'ACT No. XXVII of 2025 to further amend the Criminal Code, Cap. 9.' (2025), https://legislation.mt/.<br>[3] Ministry for Social Policy and Children's Rights (2024), 'Childrens Policy Framework 2024-2030', https://familja.gov.mt/ |

## Netherlands

| | |
|---|---|
| **Relevant legislation** | The criminal code includes offenses applicable to cyberbullying when committed with electronic means, e,g,: harassment (section 426bis), threat (section 284), stalking (section 285b) or doxing (dissemination of personal data for intimidation) (285d). [1]<br>Also, the Netherlands introduced in 2015 the School Safety Act, under which schools have the duty to ensure a safe school environment, including the obligation to use a recognised |

| | |
|---|---|
| | anti-bullying programme, have a counsellor and anti-bullying coordinator and monitor the safety and wellbeing of children at school. [2] |
| **Definitions in legislation** | Criminal Code [1]:<br>Section 426a - [stalking]<br>Any person who unlawfully imposes on the public highway another in his freedom of movement obstructs or with one or more others is liable to another person against his will or continues to follow him in an annoying manner, will be punished by the with imprisonment for a maximum of one month or a fine of the second category.<br>Section 285b – [harassment]<br>Any person who unlawfully, systematically, intentionally infringes on someone else's personal with the intention of forcing the other person to do something, not to do or to do something. to tolerate or to frighten them, as guilty of harassment, shall be punished with a imprisonment of up to three years or a fine of the fourth category.<br>Prosecution shall not take place except on complaint by the person against whom the crime has been committed. |
| **Examples of initiatives** | The government commissioned a study in 2022, to explore options for proactively intervening in the online environment to prevent harm and to protect people's, including children's, fundamental rights. [3]<br>Youth Council on Digitalisation, a cooperation between UNICEF Netherlands and the Ministry of the Interior and Kingdom Relations, comprises children of 11-17 years advising the Minister for Digitalisation on digitalisation topics they encounter in their daily lives. The outcomes of the youth council sessions are input for national policy on the protection of children in the digital world. [4]<br>'Stichting School en Veiligheid' offers information and advice for schools on how they can respond to cyberbullying. [5] |
| **References** | [1] 'Criminal Code (Wetboek van Strafrecht)' (2025), https://wetten.overheid.nl/.<br>[2] 'Act of 4 June 2015 amending certain education laws in connection with the introduction of the obligation for schools to ensure safety at school (Wet van 4 juni 2015 tot wijziging van enige onderwijswetten in verband met het invoeren van de verplichting voor scholen zorg te dragen voor de veiligheid op school)' (2015), Ministerie van Justitie, https://zoek.officielebekendmakingen.nl/.<br>[3] Rathenau Instituut (2022), 'Harmful Behaviour Online - An investigation of harmful and immoral behaviour online in the Netherlands', https://www.rathenau.nl/<br>[4] UNICEF (n.d.), 'Youth Council for Digitalization', UNICEF website, accessed 30 October 2025, https://www.unicef.nl/<br>[5] School & Veiligheid (n.d.), 'Een veilige school, daar zorg je samen voor!', School & Veiligheid website, accessed 30 October 2025, https://www.schoolenveiligheid.nl/. |

## Austria

| | |
|---|---|
| **Relevant legislation** | In the Austrian 'Federal law consolidated: Criminal Code', in addition to articles related to Dangerous threat (§107), Persistent persecution/stalking (§107a), Continued use of violence (§107b), and Deception (§108). Additionally, §107c-Persistent harassment by means of telecommunication or a computer system was introduced since December 30, 2020 and updated on September 20, 2022 [1] |

| | |
|---|---|
| **Definitions in legislation** | Criminal Code [1]:<br>Article 107c. ‘Persistent harassment by means of telecommunication or a computer system’:<br>(1) Anyone who, by means of telecommunications or using a computer system in a manner likely to unreasonably impair a person's lifestyle,<br>1. commits a criminal offense against a person's honour in a manner that is perceptible to a large number of people for a prolonged period of time, or<br>2. makes a fact or image of a person's most private sphere perceptible to a large number of people for a prolonged period of time without their consent,<br>shall be punished with imprisonment for up to one year or a fine of up to 720 daily rates.<br>(2) If the act results in the suicide or attempted suicide of the injured person within the meaning of paragraph 1, if the perpetrator repeatedly commits acts directed against the injured person within the meaning of paragraph 1 within a period exceeding one year, or if the duration of perceptibility pursuant to paragraph 1 exceeds one year, the perpetrator shall be punished with imprisonment of up to three years.<br>Article 107a - Persistent Persecution [by means of telecommunications]<br>(1) Anyone who unlawfully and persistently persecutes a person (paragraph 2) shall be punished with imprisonment for up to one year or a fine of up to 720 daily rates.<br>(2) Persistent persecution is defined as anyone who, in a manner likely to unreasonably impair that person's lifestyle, persistently and for a prolonged period of time,<br>1. visits the person's physical proximity,<br>2. establishes contact with that person by means of telecommunications or other means of communication or through third parties,<br>3. orders goods or services for that person using their personal data,<br>4. causes third parties to contact that person using their personal data, or<br>5. publishes facts or images of the person's most personal life without their consent.<br>(3) If the period of the offence referred to in paragraph 1 exceeds one year or if the offence results in the suicide or attempted suicide of the person prosecuted within the meaning of paragraph 2, the offender shall be punished with imprisonment of up to three years. |
| **Examples of initiatives** | In Austria there are various initiatives in relation to the use of digital technologies at various levels (e.g., government, civil society) such as 'The initiative eEducation Austria’ of the Federal Ministry of Education. Its primary goal to advance digital and ICT-based competencies throughout all schools in Austria starting from primary to upper secondary schools. [2]<br>Another example is the ‘ZARA: Digitale Zivilcourage’ (Civil courage online and offline) initiative which offers various activities that encourage bystanders to challenge online hate speech and to develop digital 'civil courage' (e.g., speaking up against a victim's bullies, perpetrators, or harassers). [3] |
| **References** | [1] ‘Federal law consolidated: Complete legal provisions for the Criminal Code, version of 28 October 2025 (Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 28.10.2025)’ (2025), https://www.ris.bka.gv.at/.<br>[2] Federal Ministry of Education (n.d.), ‘About eEducation - eEducation’, accessed 27 October 2025, https://eeducation.at/.<br>[3] ZARA (n.d.), ‘ZARA - Zivilcourage & Anti-Rassismus-Arbeit’, accessed 27 October 2025, https://zara.or.at/en/. |

### Poland

| | |
|---|---|
| **Relevant legislation** | Under the Law 535/2023, of 9 March, on amending the Law of 29 July 2005 on combating domestic violence and some other acts, the term 'domestic violence' covers actions 'including by means of electronic communication'. [1]<br>In 2011, Poland incorporated in the Criminal Code the offense of stalking or persistent harassment (art. 190a), which applies to cyberbullying when committed through electronic means, although not explicitly mentioned.<br>Additionally, other articles of the Criminal Code may also apply to cyberbullying when committed through electronic means, e.g.: art. 118 and 119 (homicide, serious detriment to health and threat on the basis of ethnic, racial, political or religious grounds), art. 157 and 160 (causing or exposing to bodily injury or an impairment to health), art. 190 and 191 (threat), art. 216 (insult, included using mass media). [2]<br>Parliamentary Team to Combat Hate Speech held its first meeting in June 2024 and has since been actively working to address online hate and cyberbullying. One of its key initiatives is the introduction of the "ślepy pozew" (blind lawsuit) – a legal mechanism designed to empower victims to take action against anonymous online offenders. This proposal allows individuals to file lawsuits against unidentified perpetrators by naming them as "unknown persons" in court proceedings. [3] |
| **Definitions in legislation** | Law of 29 July 2005 on combating domestic violence (Amended by Law 535/2023, of 9 March) [1]:<br>Article 2.1:<br>1) 'domestic violence' means a one-off or repeated intentional act or injunctiveness that exploits a physical, mental or economic advantage affecting the personal rights or interests of a person suffering domestic violence, in particular:<br>a) putting that person at risk of loss of life, health or property,<br>b) violating his dignity, bodily integrity or freedom, including sexual freedom,<br>c) causing damage to his or her physical or mental health, causing suffering or harm to that person,<br>d) restricting or depriving that person of access to financial resources or to the possibility of working or gaining financial autonomy,<br>e) seriously injurious to his or her privacy or causing him or her a feeling of danger, humiliation or terrible, including by means of electronic communication.<br>Criminal Code [2]:<br>Article 190a. Stalking / persistent harassment:<br>1. Whoever, by persistently harassing another person or a person closest to him/her, arouses in him/her a sense of threat, humiliation or anguish justified by the circumstances, or significantly violates his/her privacy,<br>is subject to imprisonment from 6 months to 8 years.<br>2. The same penalty applies to anyone who, impersonating another person, uses their image, other personal data or other data by means of which they are publicly identified, thereby causing material or personal damage to them.<br>3. If the consequence of the act specified in § 1 or 2 is that the victim takes his own life, the offender is subject to imprisonment for a term of 2 to 15 years<br>4. The prosecution of the crime specified in § 1 or 2 shall take place at the request of the aggrieved party. |
| **Examples of initiatives** | The Ministry of the Interior and Administration and the Police are responsible for developing policies in the area of preventing and combating crime – including crimes related to child sexual abuse online, hate speech, cyberbullying and the like. |

| | |
|---|---|
| | In September 2025, Poland will introduce an optional health education course in schools, covering topics such as physical health, mental well-being, and sexual education. This initiative aims to enhance students' overall health awareness and address issues like cyberbullying through preventive education. The curriculum will be available to students in grades 4–8 of primary schools and grades 1–3 of secondary schools.<br>The Cyber Spot project is an initiative which focuses on establishing digital councils across the country in schools, enabling young people to take the lead in educating their peers about online safety. [3] |
| **References** | [1] 'ACT of March 9, 2023 amending the Act on Counteracting Domestic Violence and Certain Other Acts (USTAWA z dnia 9 marca 2023 r. o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych innych ustaw)' (2023), https://isap.sejm.gov.pl/.<br>[2] 'Criminal Code (Kodeks karny)' (2025), https://sip.lex.pl/.<br>[3] European Commission (2025), 'Better Internet for Kids (BIK) Policy monitor country profile 2025: POLAND', https://better-internet-for-kids.europa.eu/. |

## Portugal

| | |
|---|---|
| **Relevant legislation** | The Portuguese Penal Code includes a number of offenses that may apply to cyberbullying when they are committed through electronic means (e.g. stalking, disseminating intimate images, publishing unauthorised information, data or images, defamation, threat, coercion, etc.) [1]<br>The Portuguese Charter on Human Rights in the Digital Age approved by law 27/2021 of 17 May also addresses the topic of security in the use of Internet, especially for children and young people. [2]<br>Law No 51/2012 on Student Statute and School Ethics combats school violence. [3] |
| **Definitions in legislation** | Penal Code [1]:<br>Article 154-A Stalking<br>1. Anyone who repeatedly pursues or harasses another person, by any means, directly or indirectly, in a manner likely to cause them fear or anxiety or impair their freedom of determination, shall be punished with a prison sentence of up to 3 years or a fine, if a more severe penalty is not applicable under another legal provision.<br>2. An attempt is punishable.<br>3. In the cases provided for in § 1, the accused may be subject to additional penalties of prohibiting contact with the victim for a period of 6 months to 3 years and requiring them to attend specific programs to prevent behaviour typical of stalking.<br>4. The additional penalty of prohibiting contact with the victim must include removal from the victim's residence or workplace, and its enforcement must be monitored by remote monitoring techniques.<br>5. Criminal proceedings are subject to a complaint.<br>Article 193.- Disseminating, through social media, the internet, or other means of broad public dissemination<br>Anyone who, without consent, disseminates or contributes to the dissemination, through social media, the internet, or other means of broad public dissemination, of images, photographs, or recordings that violate the private lives of individuals, particularly family privacy or sexual life, is punished with a prison sentence of up to 5 years. |

| | |
|---|---|
| **Examples of initiatives** | The government's initiative 'Portugal's School Without Bullying' promotes an antibullying action especially among young people. [4]<br>The Working Group to Combat Bullying in Schools national report presents data on cyberbullying in schools. [5]<br>The Digital Academy for Parents Program is an initiative inviting parents and guardians of children of Primary and Secondary Education since 2020 to attend training sessions promoting digital skills and safety. [6] |
| **References** | [1] 'Penal Code (Código Penal)' (2025), https://diariodarepublica.pt/.<br>[2] 'Charter of Human Rights in the Digital Age (Carta Portuguesa de Direitos Humanos na Era Digital)' (2021), https://milobs.pt/<br>[3] 'Student Statute and School Ethics, repealing Law No. 30/2002 of 20 December (Estatuto do Aluno e Ética Escolar, revogando a Lei n.o 30/2002, de 20 de dezembro)' (2012), https://diariodarepublica.pt/<br>[4] Escola Sem Bullying, Escola Sem Violência (n.d.), 'Escola Sem Bullying \| Escola Sem Violência', accessed 30 October 2025, https://www.sembullyingsemviolencia.edu.gov.pt/<br>[5] Grupo de Trabalho de Combate ao Bullying nas Escolas (2025), 'Relatório do Grupo de Trabalho de Combate ao Bullying nas Escolas', https://www.portugal.gov.pt/<br>[6] E-REDES (n.d.), 'Digital Academy for Parents', accessed 30 October 2025, https://www.e-redes.pt/ |

## Romania

| | |
|---|---|
| **Relevant legislation** | Cyber violence is a crime in the context of domestic violence (Law no 106/2020 amending and complementing Law no 217/2003 on preventing and combating domestic violence). [1]<br>In the Law no 1/2011 on National Education (Legea educației naționale nr. 1/2011), as consolidated in August 2018, cyberbullying is addressed in a school context with provisions for the prohibition of any action that could endanger the physical or psychological health and wellbeing of children in schools (Article 7) [2]. Order 4343 of May 27, 2020, approves norms of application of provisions of art. 7, and provides operational definitions of bullying and cyberbullying. [3]<br>For other crimes of cyberbullying outside the scope of domestic violence, relevant provisions of the Criminal Code can be applied on threats, blackmail and harassment apply (articles 206 to 208). The article on harassment mentions to the use of 'means of remote communication'. [4] |
| **Definitions in legislation** | Law no 217/2003 on preventing and combating domestic violence [1]:<br>Article 4.1.h) - cyberviolence –<br>online harassment, gender-based hate speech, online stalking, online threats, non-consensual publication of intimate information and graphic content, unlawful access to interception of communications and private data, and any other form of misuse of information and communication technology through computers, smart mobile phones or other similar devices that use telecommunications or can connect to Internet and can transmit and use social or email platforms with the aim of shaming, humiliating, scaring, threatening, silencing the victim.<br>Norms of application of provisions of art. 7 of Law no 1/2011 on National Education [3]:<br>Article 1 on meanings:<br>a) psychological violence - bullying is the action or series of physical, verbal, relational and/or cybernetic actions, in a social context that is difficult to avoid, committed |

| | |
|---|---|
| | intentionally, which involve an imbalance of power, result in the attainment of dignity or the creation of an atmosphere of intimidation, hostile, degrading, humiliating or offensive, directed against a person or a group of people and aim at aspects of discrimination and social exclusion, which may be related to belonging to a certain race, nationality, ethnicity, religion, social category or to a disadvantaged category or to the beliefs, sex or sexual orientation, personal characteristics, action or series of actions, behaviours that take place in educational establishments and in all spaces intended for education and professional training. The term psychological violence - bullying is excluded from violent relationships between adults and children and violent relationships between adults within the school;<br>c) Cyber psychological violence or cyberbullying consists of actions that are carried out through the internet, computer, tablet, mobile phone and can include elements of online harassment, along with illegal and/or offensive content that refers to any technology-mediated behaviour, identified in the space of social media, websites, messaging. This form of violence is not limited to repeated behaviours such as: emails, posts, messages, images, films with abusive/offensive/offensive content, this also means the deliberate exclusion/marginalization of a child in the online space, the breaking of a personal email account password, carried out on online groups and social networks or through other forms of online electronic communication.<br>Criminal code [4], Article 208 Harassment:<br>(1) The act of a person who repeatedly follows, without right or legitimate interest, a person or supervises his home, workplace or other places frequented by him, thus causing him a state of fear, shall be punished by imprisonment from 3 to 6 months or a fine.<br>(2) Making telephone calls or communications by means of remote transmission, which, by frequency or content, causes fear to a person, shall be punished by imprisonment from one month to 3 months or by a fine, if the act does not constitute a more serious crime.<br>($2^1$) If the acts provided for in paragraphs (1) and (2) are committed against a minor, the special limits of the punishment shall be increased by one third.<br>(3) The criminal action is initiated upon the prior complaint of the injured person. |
| **Examples of initiatives** | The National Authority for the Protection of Child Rights and Adoption (NAPCRA) since 2008 has been contributing to strengthening online safety awareness, such as promoting training on child online protection through the Internet Safety Hour Programme, as well as to monitoring the prevention and combating of any form of violence against children, including online violence. [5]<br>Among other studies on the use of the internet, a study on the impact of cyberbullying was conducted in 2023, by ‘Save the Children Romania’. [6] |
| **References** | [1] ‘LAW no. 106 of 3 July 2020 on the amendment and completion of Law no. 217/2003 on preventing and combating domestic violence (LEGE nr. 106 din 3 iulie 2020 privind modificarea și completarea Legii nr. 217/2003 pentru prevenirea și combaterea violenței domestice)’ (2020), https://legislatie.just.ro/.<br>[2] ‘National Education Law No. 1/2011 (Legea educației naționale nr. 1/2011)’ (2011), https://www.edu.ro/.<br>[3] ‘Methodological Rules related to the National Education Law no. 1/2011, regarding psychological violence - bullying (NORME METODOLOGICE la Legea educației naționale nr. 1/2011, privind violența psihologică - bullying)’ (2020), https://legislatie.just.ro/.<br>[4] ‘PENAL CODE of 17 July 2009 (LAW no. 286/2009) (CODUL PENAL din 17 iulie 2009 (LEGEA nr. 286/2009))’ (2009), https://legislatie.just.ro/. |

| | |
|---|---|
| | [5] Ministerul Muncii, Familiei, Tineretului și Solidarității Sociale (n.d.), 'Autorității Naționale pentru Protecția Drepturilor Copilului și Adopție (ANPDCA)', accessed 31 October 2025, https://copii.gov.ro/1/.<br>[6] Salvați copiii (2023), 'Studiu privind impactul fenomenului cyberbullying asupra copiilor și adolescenților', https://oradenet.ro/. |

## Slovenia

| | |
|---|---|
| **Relevant legislation** | There is no specific criminal provision for cyberbullying, however, article 134.a of the Slovenian Criminal Code deals with stalking (via electronic means of communication). Other offenses applicable to cyberbullying include: threat (art. 135), unauthorised image recording (and sharing) (art. 138), unauthorised publication of private documents (art. 140) and misuse of personal data (art. 143). [1] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 134a - Stalking [via electronic means of communication]<br>(1) Whoever stalks another person or a close relative by repeatedly observing, pursuing or intrusive efforts to establish direct contact or contact via electronic means of communication and thereby causes fear or danger in that person or a close relative shall be punished by a fine or imprisonment for a term of up to two years.<br>(2) If the person being stalked is a minor or a weak person, the perpetrator shall be punished by a fine or imprisonment for a term of up to three years.<br>(3) Prosecution for the act referred to in the first and second paragraphs of this Article shall be initiated upon a motion. |
| **Examples of initiatives** | Under the goals of the Cyber Security Strategy (introduced from 2016), cyber security topics, including cyberbullying, online hate speech, etc., were included in primary and secondary school curricula.<br>A Massive Open Online Course (MOOC) dedicated to online safety has been offered by ARNES through the Cybersafe project. [2]<br>The guardian of the rights of viewers, listeners and readers as well as users issued by Radiotelevizija Slovenia is an example of a self-regulatory mechanism that contributes to efforts to reduce and eliminate hate speech online. [3] |
| **References** | [1] 'Criminal Code (Kazenski zakonik)' (2008), https://pisrs.si/.<br>[2] Building teachers competence about cyber violence against girls consortium (n.d.), 'Activities \| Cybersafe mooc', accessed 31 October 2025, https://cybermooc.splet.arnes.si/.<br>[3] Programski svet RTV Slovenija (2021), 'PRAVILNIK O DELOVANJU VARUHA PRAVIC GLEDALCEV, POSLUŠALCEV IN BRALCEV TER UPORABNIKOV PROGRAMSKIH VSEBIN RADIOTELEVIZIJE SLOVENIJA', https://img.rtvslo.si/. |

## Slovakia

| | |
|---|---|
| **Relevant legislation** | Cyberbullying is referred under article 360b Dangerous electronic harassment of the revised Criminal Code, included in 2021 effective as of 31.12.2021. [1] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 360b – Dangerous electronic harassment |

| | |
|---|---|
| | (1) Whoever intentionally, through an electronic communication service, computer system or computer network, significantly impairs the quality of life of another person by<br>a) long-term humiliating, intimidating, acting unlawfully on their behalf or otherwise harassing them for a long time, or<br>b) unlawfully publishing or making available to a third party a visual, audio or audio-visual recording of their personal expression obtained with their consent, which is capable of significantly endangering their reputation or causing them other serious harm to their rights,<br>shall be punished by imprisonment for up to three years.<br>(2) The offender shall be punished by imprisonment for one to four years if he commits the act referred to in paragraph 1<br>a) on a protected person, or<br>b) for a special motive.<br>(3) A person shall be liable to imprisonment for a term of two to six years if he commits the act referred to in paragraph 1<br>a) and thereby causes considerable damage,<br>b) with the intention of obtaining for himself or another a considerable benefit, or<br>c) even though he has been convicted of such an act in the previous twenty-four months. |
| **Examples of initiatives** | The National Coordination Centre for Resolving the Issues of Violence against Children (NCC) established an inter-ministerial working group on the National Strategy for the Protection of Children in the Digital Environment and introduced an Action Plan for the National Strategy for the Protection of Children in the Digital Environment for the period 2024 – 2025. [2]<br>The new National Curriculum for Primary Education addresses digital literacy as part of the key cross-cutting literacies, including how to behave safely in an online environment. [3]<br>The National Project DiTEdu provides teacher training and lesson plans for teaching cybersecurity and online safety. [4] |
| **References** | [1] 'Act 300 of 20 May 2005, Criminal Code (300 zákon z 20. mája 2005, Trestný zákon)' (2021), https://www.slov-lex.sk/.<br>[2] Národné koordinačné stredisko pre riešenie problematiky násilia na deťoch (2024), 'Akčný plán k Národnej koncepcii ochrany detí v digitálnom priestore na roky 2024 – 2025', https://detstvobeznasilia.gov.sk/.<br>[3] Eurydice (n.d.), 'Slovakia: Reform of the national curriculum for primary and lower secondary education', accessed 31 October 2025, https://eurydice.eacea.ec.europa.eu/.<br>[4] DigiEDU (n.d.), 'DigiEDU \| DigiEDU', accessed 31 October 2025, https://digiedu.sk/. |

## Finland

| | |
|---|---|
| **Relevant legislation** | Several articles in the Criminal Code can be applied to cyberbullying. Relevant offences, which may be committed also online, include:<br>— assault (Chapter 21, Section 5; this offence may injure also the mental health of a person),<br>— harassing communications, dissemination of information violating personal privacy, aggravated dissemination of information violating personal privacy, defamation and aggravated defamation (Chapter 24, Sections 1a, 8, 8a, 9 and 10),<br>— stalking and coercion (Chapter 25, Sections 7a and 8) and |

| | |
|---|---|
| | — extortion and aggravated extortion (Chapter 31, Sections 3 and 4). [1]<br>The Pupil and Student Welfare Act lays down provisions on the right to student welfare with pupils in education referred to in the Basic Education Act (628/1998) and students in education referred to in the Upper Secondary School Act (629/1998) [2] and the Act on Vocational Education and Training (630/1998). It promotes the well-being, healthiness and safety of the educational institution community and study environment. |
| **Definitions in legislation** | Criminal code [1], [3]:<br>Section 1a - Harassing communications<br>A person who, with intent to disturb, repeatedly sends messages or calls another person so that the act is conducive to causing that person considerable disturbance or harm shall be sentenced for harassing communications to a fine or to imprisonment for at most six months.<br>Section 7a - Stalking<br>A person who repeatedly threatens, follows, observes, contacts or in some other manner comparable to these unlawfully stalks another person so that this is conducive to causing fear or anxiety in the person being stalked shall, unless an equally or more severe punishment for the act is provided elsewhere by law, be sentenced for stalking to a fine or to imprisonment for at most two years. |
| **Examples of initiatives** | The aim of the Non-Violent Childhoods Action Plan 2020–2025 by the Ministry of Social Affairs and Health is to prevent violence against children aged 0–17 in different growth and operating environments. This also includes digital environments. [4]<br>The Finnish Agency for Education has guidelines for preventing bullying and harassment: Anti-bullying work in schools and educational institutions and Prevention of bullying, harassment, discrimination and violence. The National Development Programme for Youth Work and Youth Policy 2020-2023 also discusses youth empowerment and participation, as well as preventing bullying and grooming. [5] |
| **References** | [1] 'Criminal Code' (2021), https://www.finlex.fi/.<br>[2] 'Act on General Upper Secondary Education' (2018), https://www.finlex.fi/.<br>[3] 'Laws amending the Criminal Code's Coercive Measures Act (laeiksi rikoslain pakkokeinolain muuttamisesta)' (n.d.), https://www.finlex.fi/.<br>[4] Finnish Institute for Health and Welfare (n.d.), 'Non-Violent Childhoods Action Plan', THL website, accessed 30 October 2025, https://thl.fi/.<br>[5] Finnish National Agency for Education (n.d.), 'Kiusaamisen ja väkivallan tunnistaminen, ennaltaehkäisy ja puuttuminen', accessed 30 October 2025, https://www.oph.fi/. |

### Sweden

| | |
|---|---|
| **Relevant legislation** | There are provisions in the Penal Code that criminalise offensive acts that may be considered cyberbullying when they take place on the internet (e.g. stalking (chapter 4.4b), slander or aggravated defamation (chapter 5.1 and 2), impersonation (chapter 4.6b), offensive photography (chapter 4.6a). [1]<br>Schools and all their staff are responsible for preventing and also investigating all forms of harassment or offensive behaviour according to the School Act (2010:800), Chapter 6. Measures against abusive treatment. [2]<br>The Discrimination Act 2008:567 tackles harassment as a form of discrimination and defines it in section 4. [3] |

| | |
|---|---|
| **Definitions in legislation** | Penal Code [1]:<br>Chapter 4, Section 4b – [Unlawful persecution]:<br>Anyone who stalks a person by committing or otherwise participating in criminal acts that constitute<br>1. assault according to Chapter 3, Section 5 or an attempt to commit such a crime that is not minor,<br>2. unlawful coercion according to Chapter 4, Section 4, first paragraph,<br>3. unlawful threats according to Chapter 4, Section 5, first paragraph,<br>4. breach of the peace according to Chapter 4, Section 6, first paragraph or unlawful trespass according to Chapter 4, Section 6, second paragraph,<br>5. offensive photography according to Chapter 4, Section 6 a,<br>6. unlawful use of identity according to Chapter 4, Section 6 b,<br>7. unlawful invasion of privacy according to Chapter 4, Section 6 c,<br>8. molestation according to Chapter 4, Section 7,<br>9. incitement to suicide or negligent incitement to suicide according to Chapter 4, Section 6 b, 7 a §,<br>10. defamation or aggravated defamation according to Chapter 5 § 1 or 2,<br>11. sexual harassment of a child according to Chapter 6 § 10, first paragraph or sexual harassment according to Chapter 6 § 10, second paragraph,<br>12. damage according to Chapter 12 § 1 or attempted such an offence,<br>13. minor damage according to Chapter 12 § 2,<br>14. violence or threats against an official according to Chapter 17 § 1, first paragraph or attempted such an offence,<br>15. assault against an official according to Chapter 17 § 2, first and second paragraphs or attempted such an offence,<br>16. insult against an official according to Chapter 17 § 1, first and second paragraphs or attempted such an offence, Section 3, or<br>17. violation of a contact ban or violation of an extended or specially extended contact ban pursuant to Section 24 of the Contact Ban Act (1988:688)<br>shall be punished, if each of the acts has constituted a repeated violation of the person's privacy, by imprisonment for unlawful persecution for a maximum of four years. Act (2025:579).<br>Discrimination Act [3]:<br>Section 4 on meanings:<br>4. Harassment: conduct that violates a person’s dignity and that is associated with one of the grounds of discrimination sex, transgender identity or expression, ethnicity, religion or other belief, disability, sexual orientation or age. |
| **Examples of initiatives** | The Swedish Agency for the Media monitors media usage among children and young people in three bi-annual reports titled Småungar & medier (Small Children and the Media), Ungar & medier (Kids and the Media), and Föräldrar & medier (Parents and the Media). [4]<br>The Swedish Public Health Agency published general recommendations and guidelines on digital media use for children and young people, including reducing vulnerability and risk of harassment and bullying. [5] |

| | |
|---|---|
| | Teaching online safety has been integrated into the national curriculum for primary and junior high schools referring to a “complex world that students need to learn how to navigate.” [6]<br>The Swedish National Agency for Education provides material for teachers regarding online safety to enhance the teachers' understanding of online safety, including harassment on digital platforms. The national initiative to ensure teacher training on online safety through the Safe Internet Use-training module (‘Säker användning av nätet’) also covers the topic of cyberbullying. [7] |
| **References** | [1] ‘Criminal Code (1962:700) (Brottsbalk (1962:700))’ (2025), https://www.riksdagen.se/.<br>[2] ‘School Law (2010:800) (Skollag (2010:800))’ (2025), https://www.riksdagen.se/.<br>[3] ‘Discrimination Act, 2008:567’ (2024), https://www.do.se/.<br>[4] Folkhälsomyndigheten (2025), ‘Skärmanvändning och hälsa’, 6 October, accessed 31 October 2025, https://www.folkhalsomyndigheten.se/.<br>[5] Svenska Mediemyndigheten (2025), ‘Svenska nyhetsmedier ökar sina intäkter’, 29 October, accessed 31 October 2025, https://mediemyndigheten.se/.<br>[6] Skolverket (n.d.), ‘Läroplan för grundskolan samt för förskoleklassen och fritidshemmet’, text, accessed 31 October 2025a, https://www.skolverket.se/.<br>[7] Skolverket (n.d.), ‘Säker användning av nätet’, text, accessed 31 October 2025b, https://www.skolverket.se/. |

## Other States in the EEA

### Iceland

| | |
|---|---|
| **Relevant legislation** | Provisions under General Criminal Law on violations of personal freedom and personal privacy (Ch. XXIV and XXV) may be applied to cyberbullying if they are committed through electronic means (e.g. threat (art. 233), insult and denigration (art. 233b), defamation (art. 234). Also, some offenses under Chapter XXII – sexual offences explicitly mention the use of “Internet or by means of other information technology or telecommunications equipment”, e.g. in relation to production or consumption of pornography (art. 210a), or contacting children to have sexual intercourse (Art. 202.gr). [1]<br>There are also references in the Act on Working Environment, Health and Safety in Workplaces, No. 46/1980 (updated in Law collection edition 156a. Icelandic laws as of April 30, 2025, on the Conditions, Health and Safety in the Workplace, 1980 No. 46 May 28); and on the Regulation on measures against victimisation, sexual harassment, gender-based harassment, and violence in workplaces. [2], [3] |
| **Definitions in legislation** | Regulation on measures against victimisation, sexual harassment, gender-based harassment and violence in workplaces [3]:<br>Article 3 on definitions:<br>b) Bullying: Repeated behavior that is generally intended to cause distress to the person being bullied, such as belittling, insulting, hurting, threatening, or causing fear. This does not include differences of opinion or differences of interest.’<br>c) Gender-based harassment: Conduct connected with the gender of the person who experiences it and has the purpose, or the effect, of offending the person’s dignity and creating situations that are threatening, hostile, degrading, humiliating or insulting to the person.<br>e) Violence: Conduct of any type that leads to, or could lead to, physical or psychological injury or suffering on the part of the person who experiences it, and also the threat of such conduct, coercion or random deprivation of freedom. |

| | |
|---|---|
| **Examples of initiatives** | The Presidential Committee of the Althing (Parliament) has, in consultation with party groups, approved a policy and action plan against bullying, an important milestone in work that has taken place at the Althing over the past years to combat bullying. [4]<br>The Icelandic Youth Study collects data on the welfare and attitudes of children and young people including their use of social and digital media. [5]<br>Iceland incorporated information and media literacy, as well as digital citizenship, in its most recent curriculum update.<br>‘The Algorithm that Raises Me Up’ programme targets 13- to 18-year-olds in schools in Iceland on media literacy, including dealing with harassment from strangers~~.~~ [6], [7]<br>The Internet traffic School (Netumferðarskólinn) is part of the government's action plan for cybersecurity, including children online safety. [8] |
| **References** | [1] ‘The General Penal Code’ (2018), https://www.government.is/.<br>[2] ‘Act on Working Environment, Health and Safety in Workplaces, No. 46/1980’ (2018), https://www.government.is/.<br>[3] ‘Regulation on measures against bullying, sexual harassment, gender-based harassment and violence in the workplace (Reglugerð um aðgerðir gegn einelti, kynferðislegri áreitni, kynbundinni áreitni og ofbeldi á vinnustöðum)’ (n.d.), https://www.government.is/.<br>[4] Althingi (n.d.), ‘Strategy and Action Plan against Bullying, Sexual and Gender-based Harassment and other Demeaning Conduct where Members of the Althingi are Involved’, Alþingi website, accessed 31 October 2025, https://www.althingi.is/.<br>[5] Háskóli Íslands (n.d.), ‘Íslenska æskulýðsrannsóknin’, accessed 31 October 2025, https://iae.is/.<br>[6] Reykjavik (n.d.), ‘Bullying in school and recreational activities’, accessed 31 October 2025, https://reykjavik.is/.<br>[7] Sæmundarskóli (2025), ‘Sæmundarskóli’, 28 October, accessed 31 October 2025, https://saemundarskoli.reykjavik.is/.<br>[8] Netumferðarskólinn (2024), ‘Netumferðarskólinn’, accessed 31 October 2025, https://netumferdarskolinn.is/. |

## Liechtenstein

| | |
|---|---|
| **Relevant legislation** | Cyberbullying is not defined in its own specific law in Liechtenstein, but it is addressed through various existing laws, similar to how bullying is treated in general.<br>Provisions applied in its Criminal Code include §105–Coercion, §106-Aggravated coercion, §107-Dangerous threat, §111–Defamation, §112-False accusation, or §115–Insult.<br>More particularly under §107-Dangerous threat, two more articles apply to cyberbullying: §107a-Persistent stalking (inserted in 2007 and amended in 2019) and §107c-Continuous harassment by way of electronic communication or a computer system (inserted in 2019). [1] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 107a – Persistent stalking [by means of electronic communication or by use of other means of communication]<br>1) Any person who unlawfully and persistently stalks another person (paragraph 2) shall be punished with imprisonment of up to two years.153<br>2) A person persistently stalks another person if such person, in a manner capable of causing unreasonable interference with the lifestyle of such other person, for an extended period of time continuously |

| | |
|---|---|
| | 1. establishes physical proximity with such other person,<br>2. establishes contact with such other person by means of electronic communication or by use of other means of communication or through third parties,<br>3. orders merchandise or services for such other person and, for this purpose, uses such other person's personal data, or<br>4. causes third parties to contact the other person and, for this purpose, uses such other person's personal data.<br>3) If the act results in the suicide or an attempted suicide of the person stalked pursuant to paragraph 2, the perpetrator shall be punished with imprisonment of up to three years.<br>Article 107c – Continuous harassment by way of electronic communication or a computer system:<br>1) Any person who, by way of electronic communication or by using a computer system, in a manner capable of causing unreasonable interference with the lifestyle of the other person, continuously and over a longer period of time,<br>1. damages the honour of the other person in a manner perceivable for a larger number of persons, or<br>2. makes facts or video recordings of the highly personal area of life without such other person's consent perceivable for a larger number of persons.<br>shall be punished with imprisonment of up to one year or with a monetary penalty of up to 720 daily rates.<br>2) If the act results in the suicide or an attempted suicide of the person injured pursuant to paragraph 1, the perpetrator shall be punished with imprisonment of up to three years. |
| **Examples of initiatives** | The Government of Liechtenstein established an expert group on media competences that coordinates the various institutions and actors in the field of youth protection and social media. One of the topics the expert group covers is "Cyber-mobbing". [2]<br>In 2016 the expert group on media competences started a new prevention program that convey information about digital media, Cybermobbing, Cybergrooming, Sexting, Data protection in an interactive and age-appropriate way. [3] |
| **References** | [1] 'Criminal Code (StGB) of 24 June 1987 (Strafgesetzbuch (StGB) vom 24. Juni 1987)' (2023), https://www.gesetze.li/<br>[2] Fachgruppe Medienkompetenz (n.d.), 'Fachgruppe Medienkompetenz', accessed 31 October 2025, https://www.medienkompetenz.li/<br>[3] Schulamt Fürstentum Liechtenstein (n.d.), 'MedienPräventionsPerformance', MedienPräventionsPerformance website, accessed 31 October 2025, https://www.angeklickt.li |

## Norway

| | |
|---|---|
| **Relevant legislation** | Cyberbullying can be covered by provisions in the Penal Code, such as harassing conduct (articles 266 and 266a) or violation of privacy, e.g. by sharing of offensive images (articles 267a, 267b). [1]<br>In addition, the Norwegian Education Act states that all pupils are entitled to a good physical and psychosocial environment conductive to health, well-being and learning. The Act enshrines that the school must have a zero tolerance for violations such as bullying (including cyberbullying), violence, discrimination and harassment. It also imposes an |

| | |
|---|---|
| | obligation on people working at the school to act against violations such as bullying, violence, discrimination and harassment. See the Education act chapter 12. [2] |
| **Definitions in legislation** | Criminal Code [1]:<br>Article 266 - Reckless behaviour:<br>Anyone who, by intimidating or harassing behaviour or other reckless behaviour, pursues a person or otherwise violates the peace of another person, shall be punished by a fine or imprisonment for up to 2 years.<br>Article 266a - Serious personal persecution<br>Anyone who repeatedly threatens, follows, observes, contacts or through other comparable actions pursues another person in a manner that is likely to cause fear or anxiety, shall be punished with imprisonment for up to 4 years. |
| **Examples of initiatives** | The National Strategy for a safe digital upbringing (Rett på nett) (2021) establishes important principles for the authorities' further work for children and young people's digital lives, covering a broad range of topics, including online protection, privacy, digital competence and participation. [3]<br>The National Strategy for a coordinated effort on the prevention of internet related abuse against children (2021) is part of the Government's broader efforts to promote a safe digital childhood. [4]<br>The Norwegian Media Authority collects data on children and young people's everyday media life every other year while it assists children and youth to have a safer and better digital life. [5]<br>Since 2009, Telenor, the Norwegian Media Authority, the Red Cross and Kids and the Media have worked together against digital bullying through "Use your head", a dialogue-based awareness drive. They conducted a survey (2011) on digital bullying. [6] |
| **References** | [1] 'Penal Code (Criminal Code) Chapter 24. Protection of personal freedom and peace (Lov om straff (straffeloven) - Kapittel 24. Vern av den personlige frihet og fred) [Norway]' (2009), https://lovdata.no/.<br>[2] Ministry of Education and Research [Norway] (n.d.), 'Act relating to Primary and Secondary Education and Training (the Education Act)', accessed 3 November 2025, https://lovdata.no/.<br>[3] Barne-og familiedepartementet [Norway] (2021), 'Rett på nett - Nasjonal strategi for trygg digital oppvekst', Regjeringen.no website, Rapport, regjeringen.no, 3 September, accessed 31 October 2025, https://www.regjeringen.no/.<br>[4] Justis-og beredskapsdepartementet [Norway] (2021), 'Forebygging og bekjempelse av internettrelaterte overgrep mot barn', Regjeringen.no website, Plan, regjeringen.no, 15 August, accessed 31 October 2025, https://www.regjeringen.no/.<br>[5] Medietilsynet [Norway] (n.d.), 'Barn og medier', Medietilsynet website, accessed 31 October 2025, https://www.medietilsynet.no/.<br>[6] Analist.be (n.d.), 'Telenor fights digital bullying [Norway]', accessed 31 October 2025, https://www.analist.be/. |

## Getting in touch with the EU

### In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

### On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

## Finding information about the EU

### Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

### EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

### EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

### EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

# Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

Scan the QR code to visit:

**The Joint Research Centre: EU Science Hub**
https://joint-research-centre.ec.europa.eu

Publications Office
of the European Union