Cyberbullying among young people: Laws and policies in selected Member States

SUMMARY

Cyberbullying is a growing phenomenon and a significant issue for young people across Europe and indeed the world. Unlike ‘real-world’ bullying which ends when the victim’s situation changes, such as when school ends, cyberbullying can continue for its victims at any time. Cyberbullying can reach victims through social media, text messages, false information or images spread through various methods, and can be relentless.

The ubiquity of electronic devices means children and young people are more digitally connected than ever before. The scope for children to become victims of online aggression and indeed to engage in bullying behaviour is wide. In addition, an even more worrying aspect is the exposure of children and young people to harmful material or their coercion into providing sexual images of themselves. The increase in young people’s connectivity corresponds with the rise in volume of online child sexual abuse material (CSAM) and the growth in the number of cases of minors approached online in what is known as ‘sextortion’.

Victims often feel powerless, worthless and isolated and seldom report the abuse to parents or teachers. In some cases, it can lead the victim to substance abuse, self-harm and even suicide.

Legislators are trying to keep pace with the ever-changing environment. While policies at European Union (EU) and international level are aimed at preventing cyberbullying, there have been calls for stronger EU action to prevent this form of online abuse. There are EU initiatives that address elements of the issue, but there is currently no EU-wide anti-online bullying law.

IN THIS BRIEFING

- Introduction
- International and EU legal and policy framework
- European Parliament position
- Selected EU Member States
- Elsewhere in the European Union
Introduction

There is no commonly agreed definition of cyberbullying in Europe or at international level. According to UNICEF, ‘Cyberbullying is bullying with the use of digital technologies’. A similar definition was provided by the European Commission in 2009. It defined cyberbullying as: ‘repeated verbal or psychological harassment carried out by an individual or group against others. The harassment and threats may include disseminating embarrassing photos, videos, hurtful or abusive text messages, emails, publication on social media, with the aim of causing distress, humiliation, and intimidation of one or more people. 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’.

In general terms, cyberbullying is understood as bullying taking place in digital spaces. The use of digital tools is the common feature of the different definitions, together with the intention to harm, humiliate or intimidate another individual and the repetition of the threat. Social media and the internet in general offer anonymity to perpetrators, and the possibility to spread the harmful content instantly to a far wider audience. Furthermore the information remains online, where removal can often be difficult. The rate of cyberbullying among young people is alarming. The absence of a common definition has consequences for the measurement of the phenomenon. Collection of data differs from country to country and from one study to another. Nevertheless, existing studies and data overall give a clear indication of the extent and scope of cyberbullying and its impact on victims.

Impact of cyberbullying

Children and young people’s experience online has changed considerably. For most of them, the preferred way to go online is using a smartphone. According to a 2020 Eurobarometer survey, 99% of respondents aged 15-24 had a personal mobile phone. Another survey carried out in Germany revealed that 7% of children aged 6-7 years, 27% of children aged 8-9 years and 54% of children aged 10-11 years owned a smartphone in 2020. Furthermore, children are going online at earlier ages. As digital technologies constitute an increasing part of children’s lives, more and more everyday activities are carried out online (such as doing homework, communicating with friends, listening to music, and playing games).

In a 2016 study carried out at the request of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs (LIBE), worrying trends regarding cyberbullying could already be identified from the available data. Not only does the online dimension amplify the harmful effects on teenagers who fall victim to cyberbullying, but as cyber security and children’s rights organisations warn, the internet also creates the potential for children to engage in online crimes, trolling and cyberbullying themselves.

The trend of adolescent ‘sexting’, the sending of sexually explicit images, while increasingly considered a normal part of adolescent sexual development, also increases the risk of cyberbullying. The same goes for social media platforms, which, although intended for innocent fun and education, open the door to trolling, cyberbullying, online harassment and abuse.

Globally, more than one third of young people in 30 countries participating in a 2019 UNICEF poll reported being a victim of online bullying, with one in five missing school due to cyberbullying and online violence. The poll results reveal that cyberbullying affects children worldwide, both in high-income and low-income countries, compromising their health, emotional wellbeing and academic development, and is associated with long-lasting consequences, continuing into adulthood.

In Europe, according to the EU Kids online 2020 survey, about 1 in 10 children becomes a victim of online bullying every month, and an equal number say they never feel safe online. Children’s self-reported negative online experiences have risen. The highest increase can be found among 9 to 10 year-olds (29%), which means exposure to online risks at an earlier age. Regarding cyberbullying,
girls report having been victims slightly more than boys. However, girls report being hurt and upset more than boys (89 % vs 70 %).

The number of children who report feeling bothered, upset, uncomfortable or scared by something they experienced on the internet has more than doubled, from 6 % in 2013 to 13 % in 2017 (and from 3 % to 13 % among 9 to 10-year-olds). The most common risk is being exposed to harmful user-generated content, to which 51 % of 11 to 17-year-olds have been exposed to at least one form in the past year, including hate messages. While most say that they feel sad, angry and full of hatred for what they have seen, the majority admit to having done nothing about it. Similarly, half of children who have witnessed someone else being bullied on the internet reportedly did nothing about it.

Teenagers’ online exchange of sexual images, which seems innocent to them because it is taking place within a circle of trusted persons, can also be problematic. According to Europol findings, the production of self-generated material is in many cases a consequence of sextortion, where persons using fake accounts approaches minors on digital platforms, coerce them into sending explicit photos or videos, and threatens to make these public.

In the past 20 years, the volume of online child sexual abuse materials (CSAM) has increased dramatically across the world, aided by greater connectivity and technological development. The same is true of child grooming, the practice of approaching children online to persuade them to produce sexual material of themselves and share it online, often in live-streaming format. Not only is CSAM crime growing in scale, but it is also growing more severe, as increasingly younger children are being exploited.

In 2022, 68 % of electronic service providers submitted reports to the United States National Centre for Missing & Exploited Children (NCMEC), sourced from chats, messaging or email services within the EU. An additional 22 % of reports came from social media or online gaming platforms with integrated messaging or chat services, while the remaining 10 % came from other listed platform types. According to the United Kingdom-based Internet Watch Foundation (IWF), 66 % of all known CSAM in 2022 was traced to an EU country. CSAM now includes an increasing volume of new self-generated images and videos. Some 98 % of reports mentioned children younger than 13 years of age. According to a 2023 report by the international hotline organisation INHOPE, self-generated content remained consistently high. A majority of the victims (83 %) featured in the 3-13 year category. The report also points to the fact that over 95 % of reports classified as illegal contained young girls as the victim. A recent Europol-assisted operation in Germany exposed an 400 000 member offender ring – the ‘Boystown’ dark web forum, showing the large scale of underground paedophile networks. For instance, the UK’s National Crime Agency estimates the number of people in the UK who pose a sexual threat to children at between 550 000 and 850 000.

**International and EU legal and policy framework**

It is clear that the safety and protection of children and young people is of significant concern to policy makers at national, European and international level. Regarding bullying and cyberbullying, a number of policy and legislatives initiatives focus on the issues, ranging from conventions to provide guidance for national governments, to placing legislative responsibilities on stakeholders in the digital environment.

The United Nations Convention on the Rights of the Child 1989 (UNCRC) stresses the importance of children’s rights and covers four broad areas: survival rights, development rights, protection rights and participation rights.

Article 19 of the Convention addresses all forms of violence against children. It considers that violence includes instances where someone attacks a person’s mental state as well as physical attacks. In view of this, verbal abuse and intimidation are considered forms of violence. It emphasises
that State Parties must have proper laws in place to prohibit violence, but it also requires states to implement administrative, social and educational measures to protect children.

Article 19 does not stand in isolation and for it to be effective, other Convention rights must also be respected. As well as being protected from violence, Article 19 of the UNCRC says children and young people should be kept safe from all forms of exploitation, sexual abuse, neglect, exposure to accidents, and violent images.

Although bullying, including cyberbullying, is not specifically mentioned, it does breach a number of the articles in the Convention. This is further emphasised under the responsibilities of adults to protect and safeguard children and young people from bullying behaviour so they may develop, participate in society and lead an assured and contented life.

In 2011 the UN Committee on the Rights of the Child published General comment No 13 (2011) on Article 19 of the UNCRC. The committee was alarmed at the extent and intensity of violence being exerted on children. It reiterated that violence was understood as all types of violence including psychological maltreatment. It highlighted the objectives of UNCRC Article 19 to stress the requirement of State Parties to fulfil their obligations and to provide all stakeholders with a basis for developing a coordinated framework for eliminating violence. It set out some analysis of Article 19, with examples of violence including mental violence, which included 'psychological bullying and hazing by adults or other children, including via information and communication technologies such as mobile phones and the internet, (known as 'cyberbullying')'.

The UN General Assembly adopted a Resolution on protecting children from bullying in 2014. It recognises the risks associated with the misuse of new information and communication technologies including vulnerability to bullying. It also acknowledges that bullying including cyberbullying can have an impact on the rights of children and can have negative effects on children affected by or involved in bullying.

The UN Committee on the Rights of the Child published General comment No 25 (2021) on children's rights in relation to the digital environment. The committee emphasises that the rights of every child must be respected, protected and fulfilled in the digital environment. It notes the risks posed to children, of violation or abuse occurring through digital technology. It highlights that children and young people may be discriminated against and receive hateful communications through the use of technology. States must take measures to protect them from risks such as violent and sexual content, cyber-aggression, harassment, sexual exploitation and abuse.

The 2022 UN General Assembly Resolution on protecting children from bullying reaffirms the Convention on the Rights of the Child. It recognises that bullying, including cyberbullying, has a negative impact and is a main concern for children. It calls on member states to take appropriate action to tackle the issue and provide support to children.

The Organisation for Economic Co-operation and Development (OECD) adopted its Recommendation of the Council on Children in the Digital Environment in 2012 and subsequently revised it in 2021. The recommendation outlines policy recommendations to assist governments develop national frameworks to address the issue.

The Council of Europe's 2022-2027 Strategies on the Rights of the Child is part of its overall mission and builds on previous strategies. In relation to digital technology and protecting children online, it requests that states regulate national law to safeguard children from violence, including grooming, sexual and peer violence and cyber-sexism, as well as from exposure to pornographic and other harmful content, cyberbullying and online hate speech. It also invites business and industry to fulfil their responsibilities in relation to children in this area.

The Committee of Ministers of the Council of Europe (CoE) published Guidelines to respect, protect and fulfill the rights of the child in the digital environment (CM/Rec(2018)7) in 2018. The recommendations were addressed to CoE member states. It will assist states and stakeholders in
adopting an approach to ensuring children’s safety in the digital world and help ensure that national policies address technological development.

In 2023, the European Commission published a Communication on a comprehensive approach to mental health, changing the way mental health is addressed in the EU and bringing a new strategic approach to mental health. The document emphasises (see pages 9 and 10) boosting the mental health of children and young people and points to possible negative mental health effects of digitalisation.

In May 2022, the European Commission published a new European strategy for a better internet for kids (BIK+). It is designed to protect children online and built on the 2012 strategy for a better internet for children. The BIK+ strategy is very much a part of the 2021 EU strategy on the rights of the child, an initiative under the 2022 European Year of Youth. The strategy sets out positions and actions on protecting children from harmful content online, empowering them with the skills to navigate safely and responsibly online and giving them a voice in the creation of digital safe spaces. The strategy aims to continue to feed into policy and framework development across Member States.

The Commission put forward the EU strategy on the rights of the child in 2021. It addresses challenges and proposes actions on the protection and fulfilment of children. It presents six thematic areas, with the focus of the fifth theme on a digital and information society. It recognises that in the digital environment, children can be exposed to harmful or illegal content, such as child sexual abuse or exploitation materials, pornography and adult content. It establishes a process to develop a set of principles to which online industries must adhere. It seeks to strengthen the fight against online child sexual abuse. It commits to promoting accessibility to information technologies, to allow children to experience all of the positive aspects of the digital world.

The European Commission launched the 2021-2027 digital education action plan at the end of 2020, to address the benefits and risks of digitalisation. It too recognises the risks that exist in an increasingly digital society; that young people are vulnerable to cyberbullying and harassment and can be exposed to harmful and disturbing content online. The strategy is designed to develop the digital competence of all learners, which will enable young people to acquire the knowledge and skills to interact digitally in a way that is respectful of people’s rights and dignity and uses technology responsibly. At its November 2022 meeting, the Education, Youth, Culture and Sport Council approved Council conclusions on supporting wellbeing in digital education.

The revised Audio-visual Media Services Directive (AVMSD) was adopted in 2018. It sets out requirements in relation to the provision of audio-visual media and addresses aspects such as prohibition of hate speech, discrimination based on disability and the protection of minors. As part of the revision, certain obligations were placed on video-sharing platforms to protect minors from harmful content and all users from content inciting violence or hatred. The directive takes account of the way in which individuals, particularly the young, engage with media content, with a shift to watching content online and on different devices, and brings video-sharing platforms under the directive’s scope.

The Digital Services Act (DSA) regulates online platforms and intermediaries. The intention of the act is to safeguard users by placing obligations on providers to address illegal content and harmful activities online and protect consumers’ fundamental rights online. Taken together with the Digital Markets Act, which will regulate large digital platforms, providing services, such as online search engines, app stores, and messenger services, it aims to create a safer digital space.

European Parliament position

Over the past decade, the European Parliament has addressed the issue of cyberbullying on several occasions, amongst others, in connection with the Convention on the Rights of the Child, Digital Services Act, and proposals on consumer protection in online video games and shaping a digital
education policy. Most recently, in May 2023, Parliament discussed the issue with Commissioner for Justice, Didier Reynders, who among other things has responsibility for consumer protection and digital affairs. Also present at the plenary debate was Jackie Fox, the mother of the late Nicole Fox (known as Coco), from Ireland, who tragically took her own life in 2018 as a result of cyberbullying. Based on this personal tragic experience, Jackie Fox launched a nationwide campaign in Ireland, which 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. During the debate, several Members argued for a similar EU-level initiative to make illegal online what is illegal offline. The European Parliament also called on Member States to develop strategies to protect children from online bullying and child sexual abuse in connection with the European Child Guarantee, in a resolution in 2021.

A 2023 resolution on the new European strategy for a better internet for kids (BIK+), stressed the risks and threats that children face in a constantly evolving digital environment including, but not limited to ‘online child sexual abuse and solicitation (grooming), cyber hate, different forms of cyberbullying, sexualised content, violent images, content that promotes eating disorders, and disinformation’ and the fact that those behaviours affect the physical and mental health of children. Parliament called on the Member States to invest in protecting children from bullying and cyberbullying and on the ‘Commission to develop, in coordination with the European Education Area, a European strategy against bullying and cyberbullying in schools’. Parliament has also stressed the importance of digital education to address cyberbullying and other forms of online violence.

Already in 2022, Parliament had warned of the risks linked to hate speech and cyberbullying. The same year, in a resolution on extending the list of EU crimes to hate speech and hate crime, Parliament called on the Commission and the Member States in particular to protect children and young people from hate speech and hate crimes, including bullying in schools and cyberbullying. A call to Member States to address online violence such as incitement to hatred, racism, online child sexual abuse, gender-based violence and cyberbullying, was also included in the 2022 resolution on the European Year of Youth. Another 2023 Parliament resolution recalled the impact of bullying and cyberbullying on children and young people’s mental health and how cyberbullying victims are at higher risk of depression and suicide. Parliament called on the Commission to focus on young people’s mental health and in particular on bullying and cyber-bullying in schools when designing the European mental health strategy. In another 2021 resolution, Parliament called on the Commission to develop an EU action plan for online service providers and tech companies to keep children safe online.

Selected EU Member States

Cyberbullying policies of a number of Member States (Austria, France, Ireland, Italy, Romania and Slovakia) have been selected to illustrate some clearly defined policies and frameworks which have been put in place at national level. They are highlighted with the aim of providing a snapshot of current approaches to cyberbullying and to provide clarity in both analysis and comparison of the direction of national debates and approaches being taken at Member State level.

Ireland

The term cyberbullying is not specifically defined in legislation in Ireland and there is no specific offence of cyberbullying; however, much of what is understood as cyberbullying is dealt with by other legislation. The law in Ireland to ban online harassment is informally known as ‘Coco’s Law’ (see above). Accordingly, the offence in relation to harassment and harmful communications is addressed both in online and offline situations in the Harassment, Harmful Communications and Related Offences Act 2020. The act provides for two offences, firstly, to address the phenomenon of revenge porn by making the recording, distribution or publication of intimate images without consent an offence. Secondly, the Act also addresses cyberbullying, making the distribution,
Cyberbullying among young people: Laws and policies in selected Member States

Publication or sending of threatening or grossly offensive communications or messages with the intent to cause harm, without a requirement for persistence, an offence. It also criminalises the sending of once-off threatening or abusive messages where the intent was to cause harm to the recipient. In addition, the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 is currently before Seanad Éireann (upper house of the parliament). Section 18 of the bill addresses the distribution or display of material which is threatening, abusive, insulting or obscene, aggravated by hatred. In the sphere of civil law, Ireland has recently published draft legislation to reform Ireland’s defamation laws, Draft General Scheme of the Defamation (Amendment) Bill. The proposed legislation addresses challenges faced in an increasingly complicated digital environment. The bill addresses a number of complex issues including the ability to tackle online defamation. Ireland is part of the EU Safer Internet initiative and provides a number of services through partnerships, including awareness raising, helplines and a hotline.

France

In France a recent bill has been passed to step up the fight against cyber-bullying, particularly in schools. The French Education Code (Article 111-6) states that: ‘No pupil or student may be subjected to acts of harassment resulting from comments or behaviour committed within the educational establishment or outside school or university life, with the aim or effect of undermining his or her dignity, altering his or her physical or mental health, or degrading his or her learning conditions. Such acts may constitute the offence of school harassment as defined in article 222-33-2-3 of the French penal code’. According to the French administration, harassment via the internet, known as cyberstalking, is a crime punishable by a fine and/or imprisonment of up to 10 years. Penalties are more severe if the victim is aged under 15 years. The frequency of comments and their insulting, obscene or threatening content constitutes harassment. Online harassment is punishable whether the exchanges are public or private. The offence also occurs when the remarks or behaviours are directed toward the same victim by several persons where they know that the comments or behaviours characterise a repetition. Consideration in sentencing takes account of circumstances, including, but not limited to, when committed on a minor under 15 years of age or when a minor was present and assisted.

The legislation dealing with cases of ‘revenge porn’ is provided for in articles 226-1 and 226-2 of the Penal Code, which concern words or images of a sexual nature issued in a public or private place. Here, the penalties have been increased to two years’ imprisonment and a €60 000 fine. New legislation was enacted on 7 July 2023 to establish a digital majority and combat online hate. It is designed to protect children and establishes a digital age of majority of 15 years. There are also measures to prevent and prosecute online crimes such as cyberbullying.

Italy

In Italy, the definition of cyberbullying was introduced in 2017 with Law no 71 of 29 May 2017 on ‘Provisions for the protection of minors for the prevention and contrast of the phenomenon of cyberbullying’. The law defines cyberbullying as ‘any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data to the detriment of minors, carried out electronically, as well as the dissemination of online content also concerning one or more members of the minor’s family whose intentional and predominant purpose is to isolate a child or group of minors by engaging in serious abuse, harmful attack, or ridicule’ (Article 1(2)). To be distinguished from isolated or occasional incidents the conduct of cyberbullying must 1) be carried out electronically; 2) be to the detriment of a minor; 3) have the precise purpose of isolating one or more minors identified as targets; 4) result in serious prejudice to the person. Article 2 also provides for the possibility to request the operator of the site or the owner of the social network immediately obscure, block or remove illegal content published online.
There is no specific criminal offence of cyberbullying in Italy. However, several crimes could apply under the penal code in presence of one of the conducts referred to in Article 2 of Law no 71 of 29 May: defamation (Article 595) in cases of disparaging messages. The crime of harassment or disturbance to persons (Article 660) or threat (Article 612), where such messages are threatening, persecutory acts could also be considered if the act is conducted in a systematic manner. Substitution of person could apply (Article 494) where a fake account is used, or in certain circumstances, abusive access to a computer system (Article 615-ter). Illicit dissemination of sexually explicit images or videos (Article 612-ter) in cases of ‘revenge porn’. Other crimes might also apply, such as child pornography (Articles 600-ter and 600-quater of the penal code), consideration could be given to unlawful processing of data, sanctioned by Article 167, of Legislative Decree No 196/2003; unlawful interference in private life (Penal Code Article 615-bis); extortion (Article 629), or fraud (Article 640), when aggression against victim's property is also present. Finally, in some cases of exceptional gravity, the crime of incitement to suicide (Article 580) cannot be excluded. According to Italian law, if the criminal act is committed by minors, Penal Code Article 97 absolutely excludes the notion of criminal responsibility for children aged under 14 years, instead requiring an evaluation of competence for offenders aged between 14 and 18 years, providing mitigated sanction for those deemed not responsible (Penal Code Article 98). As for the forms of protection in civil law, each of the conducts attributable to cyberbullying are considered likely to cause prejudice to the victim, which could result in liability for financial or non-financial damages.

Austria

In January 2016, under Article 107c of the Austrian Criminal Code ‘Continuous harassment by means of telecommunications or a computer system’ became a punishable offence. In 2021, a legislative package against online hate entered into force. It contained several concrete measures to better protect victims and to make it easier for them to take legal action against hate online. At the same time, the new legislation expanded the range of claims under civil law and media law. The new legislation introduced a mandate procedure in civil law, which allows victims to quickly request the removal of online content on the condition that it significantly violates their personal rights in a way that impairs human dignity. The mandate procedure is also available to prevent the sending of such content via a messenger service. To this end, it is possible to obtain an injunction from the district court without a prior hearing. The situation whereby criminal offences such as defamation requiring private prosecutions, meaning victims had to initiate prosecution themselves, has been changed as authorities now investigate the accused person based on a request at a regional court. Victims are provided with increased psychosocial and legal support to cope with stress during criminal proceedings and it is no longer the case in an acquittal, or if proceedings are discontinued, that victims have to pay for the costs of the proceedings. Previously, insulting, threatening, exposing or harassing a person online was only punishable if it took place continuously. Today, a single act can be enough to be punishable. The scope of application for incitement to hatred has been extended, where incitement to hatred against individuals is now considered an offence. Following changes to media law, compensation fees were increased where people's personal rights were violated. It also became easier and more transparent to report content to communication platform providers. Content, depending on the nature, has to be deleted within 24 hours to 7 days. Communication platform providers are required to designate an authorised representative as the contact person for Austrian authorities, companies and citizens. Fines for communication platform providers in case of repeated non-compliance with legal provisions against online hate have been increased. Fines up to €10 million are possible.

Romania

In Romania, cyberbullying is specifically criminalised only in the area of domestic violence. Law no 106/2020 amending and complementing Law no 217/2003 on preventing and combating domestic violence introduces the concept of ‘cyber violence’ in the sphere of ‘domestic violence’. The definition is: ‘cyber violence’ means online harassment, gender-based online hate messages, online
Cyberbullying among young people: Laws and policies in selected Member States

tracking, online threats, non-consensual publication of information and intimate graphic content, illegal interception of private communications and data, and any other form of misuse of information and communication technology via computers, smart phones or other similar devices that use telecommunications or connect to the internet and may transmit and use social or email platforms in order to shame, humiliate, scare, threaten, silence the victim. For other crimes of cyberbullying outside the scope of domestic violence, the relevant provisions of the Criminal Code on threats, blackmail and stalking apply (Articles 206 to 208). However, only the article on stalking refers to the use of 'means of remote communication'. In the articles on threats and blackmail, there is no explicit cyber-dimension. Cyberbullying in a school context is addressed through Law no 1/2011 on national education, which provides for the prohibition in schools of any action that could endanger the physical or psychological health and wellbeing of children (Article 7), and for measures to address bullying, particularly teacher training (Article 56).

The Detailed Rules for implementing the provisions of Articles 7(1) and 56, and of point 6 of the Annex to National Education Law No 1/2011 on psychological violence – bullying, of 27 May 2020, provide for a specific definition of cyberbullying: 'cyberbullying consists of actions that are carried out through internet, computer, tablet, mobile phone networks and may include elements of online harassment, along with illegal and/or offensive content that relates to any behaviour mediated by technology, identified in the social media, websites, messaging space. This form of violence is not limited to repeated behaviour of the type: emails, posts, messages, images, films with abusive/misleading/offensive content, but it also means the deliberate exclusion/marginalisation of a child in the online space, the breaking of a personal email account password, conducted on online social groups and networks or through other forms of online electronic communication.' The Romanian Civil Code does not specifically include cyberbullying. Some of its provisions are, however, relevant, namely Article 71 on the protection of private life and Article 72 on the respect of dignity and the prohibition of any harm to the honour and reputation of a person without consent.

Slovakia

In Slovakia, cyberbullying is addressed by amendment to the 27 May 2021 Criminal Code. It is defined as ‘dangerous online bullying’, mainly under point § 360b on dangerous electronic harassment (cyberbullying). This crime via information and communication technologies includes sending harassing, or offensive emails and text messages, creating defamatory pages and blogs, or publishing photos and videos with the aim of damaging the identity of the person in question. There are four main groups of cyberbullying: cyberstalking, ‘flaming’, sexting, ‘happy slapping’. Sentencing may be increased where the crime had ‘a special motive or if the victim is a protected person’, and in the case of significant damage or the intention to obtain a significant benefit, or in the case of a repeated offence. The legislation defines dangerous electronic harassment committed by someone:

1. (1) Who intentionally, through an electronic communication service, computer system or computer network, substantially impair the quality of life of another person.
   - humiliates them for a long time, intimidates them, acts illegally on his behalf or otherwise harasses them for a long time, or
   - without permission publishes or makes available to a third person a video, audio or video-audio recording of their expression of a personal nature, obtained without their consent, capable of significantly endangering their reputation or causing other serious damage to their rights.

2. The offender shall be punished by imprisonment for one to four years if they commit the act referred to in paragraph 1 on a protected person, or from a special motive.

3. The offender shall be punished by imprisonment for two to six years if they commit the act referred to in paragraph 1 a) and causes considerable damage with it, b) with the intention of obtaining a substantial benefit for themselves or another, or c) they had been convicted of such an act within the preceding twenty-four months.'
Several other provisions, existing prior to 2021, under the Criminal Code could also tackle cyberbullying: dangerous stalking (§ 360a), cyberstalking (§ 360b); blackmail (§ 189); coercion (§ 192); sexual abuse (§ 201, § 201a, § 201b); defamation (§ 373); damage to the rights of others (§ 376); child pornography – production, dissemination, storage and participation in child pornography performances (§ 368 to § 370); denial and approval of the Holocaust and the crimes of political regimes (§ 422d); defamation of nation, race and belief (Section 423); incitement to national, racial and ethnic hatred (§ 424); inciting, defaming and threatening persons because they belong to a certain race, nation, nationality, skin colour, ethnic group or family (§ 424a).

Elsewhere in the European Union

Overall, it appears that most Member States increasingly recognise the severity and scale of the problem. Yet, so far, these concerns have not necessarily been translated into legislative initiatives to tackling cyberbullying, and even in those EU Member States where there are such legislative initiatives, approaches and scope vary. Some interesting developments can be noted. For instance, in Greece, new legislation was introduced in 2023 concerning bullying at school, regulating among other things, the cyber aspect of violence and delinquent behaviour that negatively affects the school community and disrupts the educational process.

In Cyprus, legislative initiatives were introduced in September 2022, with a view to establishing a specific law in relation to the offence of bullying, which consists of physical and/or psychological abuse and insult to the dignity of persons. Since mid-2021, new legislation was introduced aimed at reinforcing and aiding protection from harassment and stalking (Law 114(I)/2021).

In Czechia, non-legislative initiatives focus on prevention. For instance, a project called ‘Regions for a safe internet’ targeting school children, and projects such as ‘Say no!’ and ‘Be safe’ linking schools, school establishments and police, were introduced to prevent cyberbullying.

Finland has targeted schools with its KiVa anti-bullying programme, a Ministry of Education and Culture initiative. The programme is also used in various countries in Europe, as well as some schools, such as the European School Network. In 2021, a citizens' initiative was launched, without success, to recognise bullying in the Criminal Code, and link it to cyberbullying, as an act of mental and physical violence. The Finnish Safer Internet Centre 2021–2022 (FISIC) developed several projects aimed at improving children’s, young people’s and adults’ media skills.

In Denmark, the government announced several initiatives that deal with the issue of cyberbullying in its 2021 government paper ‘Social media responsibility – stricter requirements for social media and digital education of children and young people’. The paper announced the tightening of requirements for social media platforms and strengthening children and young people’s digital education by means of 13 targeted initiatives.

In Estonia, non-legislative initiatives were adopted to prevent bullying (including cyberbullying) in schools and promote safer use of the internet, by providing training sessions, assistance and counselling and raising awareness.

In Hungary, in 2018, at the very beginning of the precedent parliamentary cycle (2018-2022), the idea of criminalising cyberbullying in the Penal code was discussed, however no action was finalised.

In Latvia, a 2023 study about bullying and violence in schools concluded that more than 40% of pupils regularly experience bullying. In addition, the government launched a number of initiatives to address bullying and mobbing. One of these is the Finnish ‘KiVa’ initiative, which was opened to Latvian schools in September 2023.

In Lithuania, a 2021 proposal was introduced, but later withdrawn, to amend the Codes of Criminal and Administrative Offences proposing administrative responsibility (instead of criminal liability) for hate speech, in particular mockery and scorn.
In **Luxembourg**, Article 444-2 of the Luxembourg penal code defines the criminal offence of 'obsessive bullying' as: 'Anyone who repeatedly harasses a person when he knew or ought to have known that he would seriously affect the peace of mind of the person concerned by this behaviour'.

There is no specific criminal offence of cyberbullying in **Malta**. It is dealt with under the provisions of the Criminal Code (Chapter 9) dealing with harassment, stalking and threatening behaviour. A bill was introduced in 2021, aiming to introduce the specific offences of cyberstalking and cyberbullying. However, the bill lapsed automatically when Parliament was dissolved in 2022.

In **the Netherlands**, under the 2015 School Safety Act, schools have a duty to ensure a safe school environment. This includes: 1) use a recognised anti-bullying programme that meets the legal criteria, 2) have a council and anti-bullying coordinator, and 3) monitor the safety and wellbeing of students at school. In addition, the Netherlands have a range of non-legislative tools to specifically tackle cyberbullying, from awareness raising, reporting and media literacy initiatives to a children's rights code, aimed at helping developers and designers implement children's rights when designing and developing apps, games, smart devices and other digital technology. The government also 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.

No specific initiatives were taken in **Poland** to target cyberbullying, in the sense of peer aggression among children. However, under the Law of 9 March 2023 on amending the act on combating domestic violence and some other acts, the term 'domestic violence' covers actions 'significantly violating the person's privacy or causing them to feel threatened, humiliated, or distressed, including actions taken through electronic communication means'.

There is no specific criminal offence of cyberbullying in **Portugal**. However, under the Portuguese Penal Code, cyberbullying conduct can be classified as a crime or combination of crimes. In addition, Law no 51/2012 established the Student’s Statute and School Ethics, criminalising school violence. Even though cyberbullying is not defined in this Law, the then Minister for Education mentioned this legislation would also apply to cyberbullying cases.

In **Slovenia**, there is no specific criminal provision for cyberbullying, however Article 134.a of the Slovenian Criminal Code deals with stalking and Article 143 covers misuse of personal data. 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.

No specific criminal provision deals with cyberbullying in **Spain**. The Law 1/2015 of 30 March amending the Criminal Code introduced an offence related to harassment, punishing behaviours that seriously undermine the freedom and safety of the victim, such as subjecting them to constant surveillance, stalking, or other forms of harassment. A series of legal instruments address cyberbullying, including Organic Law 8/2021, which provides comprehensive protection against violence for children and adolescents.

In **Sweden**, cyberbullying is not a criminal offence, however there are provisions in the Penal Code that criminalise offensive acts when they take place on the internet (e.g. slander, defamation, unauthorised invasion of privacy). The Instrument of Governance, one of the four fundamental acts constituting the Swedish Constitution, was reformed in 2010, to include a stronger protection of personal integrity.

**Belgium** addresses cyberbullying both through legislative and non-legislative means, including education and awareness-raising campaigns, as well as prevention, reporting and support systems with the objective of creating a safer and more inclusive digital environment. The Belgian Criminal Code includes provisions that criminalise acts such as stalking, defamation, and harassment, whether committed online or offline. Stalking is the most relevant, as most forms of cyberbullying fall under the legal qualification of stalking. These legal measures provide a basis for prosecuting offenders and holding them accountable for their actions. In addition, a victim can invoke the Law
on electronic communications of 13 June 2005. Article 145, § 3bis of this law deals with stalking via telecommunications and may include a case of cyberbullying.

In Bulgaria, criminalisation of cyberbullying has been suggested in a number of recent public discussions. On 26 April 2023, at a public discussion forum in Plovdiv, councillors to the then caretaker Minister of the Interior noted that an amendment of existing legislation with the aim of criminalising cyberbullying and increasing criminal penalties was being discussed and prepared.

There is no specific criminal offence of cyberbullying in Croatia, however, the Criminal Code does deal with offences committed that could be considered cyberbullying. The cyber-dimension of a crime may be punished as an aggravated circumstance. For example, Article 144a of the Criminal Code, deals with unauthorised sharing of a sexually explicit recording. Likewise, if someone knowingly slanders someone, they can be fined under Article 149 of the Criminal Code, with the fine being increased if this is done using a computer system or network. Cyberbullying is not explicitly addressed by civil law, but the Croatian Civil Obligations Act could apply. The Government has published a 2020-2024 action plan for preventing violence in schools, and there are guides on electronic sexual violence on and among children and young people, such as #react and cyberbullying.

MAIN REFERENCES

Murphy C., Understanding cybercrime, EPRS, March 2024.
Negreiro M., Combating child sexual abuse online, EPRS, December 2023.
Cyberbullying among young people, Policy Department, Directorate General for Internal Policies, 2016.

ENDNOTES

1 The following EPRS policy analysts contributed to the country analyses in this section: Verena Kern, Philippe Perchoc, Colin Murphy, Micaela Del Monte, Ionel Zamfir, Branislav Stanček.