societies

MDPI

Article

Ctrl + Alt + Remedy? Child Rights, Access to Justice and Preventive Responses to Cyberbullying in the European Union

Enikő Kovács-Szépvölgyi *, Brigitta Molnár and Bernadett Szakács

Department of Modern Technology and Cyber Security Law, Deák Ferenc Faculty of Law and Political Sciences, Széchenyi István University, 1 Egyetem Square, 9026 Győr, Hungary; szakacs.bernadett@sze.hu (B.S.)
* Correspondence: szepvolgyi.eniko@ga.sze.hu

Abstract

This study examines how European Union Member States address cyberbullying affecting children through legal and policy frameworks, paying particular attention to children's rights. It employs a qualitative, document-based comparative methodology, applying a harmonized codebook to analyze definitional, legal, preventive, and reactive responses across all 27 EU Member States. The analytical framework is grounded in the EU Charter of Fundamental Rights, the EU Strategy on the Rights of the Child, the Better Internet for Kids (BIK+) initiative, and the Digital Services Act, which serve as normative benchmarks. Coding draws on EU-level harmonized sources, including Joint Research Centre outputs and the 2025 BIK policy reports, and aggregates the findings into a composite structural indicator capturing the formal regulatory and policy coverage of cyberbullying from a child rights perspective. The results indicate a high level of formal regulatory attention in most Member States, particularly regarding criminal law protection, educational prevention, and institutional reporting mechanisms. However, child-specific and child-friendly elements—such as explicit cyberbullying definitions, adapted reporting procedures, and tailored civil law remedies—remain uneven and limited. The study concludes that, despite comprehensive formal regulation, significant gaps persist in the integration of child-centered and access-to-justice-oriented mechanisms, underscoring the need for strengthened child rights approaches and further research on implementation and children's lived experiences.

Keywords: cyberbullying; children's rights; Digital Services Act; better internet for kids; regulatory frameworks; European Union policy

Check for updates

Academic Editors: Raquel Lozano-Blasco and Diego Conejo

Received: 12 February 2026
Revised: 19 March 2026
Accepted: 30 March 2026
Published: 31 March 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Children of the 21st century grow up in a digital environment that has become a natural part of their everyday lives. A significant proportion of their social relationships, learning processes and leisure activities take place in the digital space. The sharp separation between the physical and the online environment is no longer meaningful. The two spheres continuously and mutually influence each other.

Alongside the benefits of the digital environment, a wide range of risks and harms also emerge, which may directly infringe upon children's rights. For children affected by cyberbullying, the digital space may represent a potential means of escape. At the same time, problematic internet use—as highlighted by Moral-García et al.—also constitutes one of the factors contributing to the occurrence of cyberbullying. This creates a vicious circle

in which the digital environment acts both as a coping space and as a source of increased exposure to cyberbullying [1].

Cyberbullying is one of the most significant online risks affecting children. According to the widely used 4C model [2]—referred to as the 5C model in the Digital Services Act guidelines [3]—cyberbullying is classified as a contact-related risk in peer communication contexts. Estimates of the prevalence of cyberbullying vary across studies. However, large-scale surveys consistently indicate that a substantial proportion of young people are affected. Globally, more than one-third of young people report having experienced cyberbullying, based on UNICEF survey data, while European findings from the EU Kids Online study suggest that approximately one in ten children encounter online bullying on a regular basis [4]. More recent EU-level evidence, drawing on data such as the Health Behaviour in School-aged Children (HBSC) study, indicates even higher exposure rates, with around one in six children reporting victimization [5].

Cyberbullying is particularly prevalent within peer groups and, beyond the bully–victim relationship, involves additional actors such as defenders, supporters and bystanders. As a result, the phenomenon typically entails interactions involving more than two participants and is characterized by dynamically changing roles [6]. Cyberbullying also occurs beyond peer relationships. For example, it may be perpetrated by parents, as highlighted by Alkhallouf, who draws attention to the potential conflict between parents' right to freedom of expression and children's rights, including the children's right to dignity [7].

Although bullying and cyberbullying share common psychosocial roots, they cannot be regarded as identical phenomena and require different intervention strategies [6]. Beyond definitional differences, bullying and cyberbullying diverge in their underlying mechanisms: in face-to-face contexts, perpetrators are exposed to victims' immediate emotional reactions, which may inhibit aggression, whereas digitally mediated communication weakens these empathic constraints and contributes to the online disinhibition effect [8,9]. While offline bullying is often linked to context-specific stress responses and even physical harm, victims may find temporary safety outside the immediate setting [10,11]. By contrast, cyberbullying may limit such spatial escape and obscure perpetrator identification, thereby intensifying and prolonging victimization.

Bullying is generally defined as intentional and repeated aggressive behavior directed at a victim who has difficulty defending themselves and involves an imbalance of power. This power imbalance may stem from physical strength, age, group size or social status. Bullying may take physical, verbal or relational forms, including social exclusion or rumor spreading. It typically occurs in face-to-face contexts, most often in school environments, and is constrained by spatial and temporal boundaries, in contrast to cyberbullying [12].

Although there is no universally accepted definition of cyberbullying, existing approaches tend to converge on a set of core elements, including intentionality, repetition, and an imbalance of power, typically enacted through electronic means [13]. In the online context, the criterion of repetition is less straightforward, as a single act may persist, resurface and spread across platforms, thereby generating ongoing harm [14]. In addition, the viral nature of content sharing and even passive bystander engagement—such as liking or commenting—can reinforce power imbalances and contribute to the continuity of victimization [15]. Because of the specific characteristics of the digital environment, cyberbullying can escalate more rapidly and with greater ease, may recur without temporal limitations, and—because of the nature of content sharing—the resulting harms are often irreversible [16].

These structural characteristics extend the reach of cyberbullying beyond the confines of the digital sphere, embedding it in hybrid conflicts that unfold across both online and offline contexts [17]. Large-scale international studies highlight that cyberbullying

constitutes a distinct phenomenon requiring targeted intervention. It may lead to more severe psychological consequences than traditional bullying and significantly increases school-related stress [18].

Victims of cyberbullying in the online environment are exposed to heightened psychological, emotional and social risks. Research shows increased levels of depression, anxiety and suicidal ideation. It is also associated with social isolation, sleep disturbances and poorer academic performance. The effects of persistent or repeated online harassment may endure over the long term, particularly during childhood and adolescence [19].

All forms of cyberbullying violate children's rights. They affect the right to safety, dignity and privacy, as well as the right to education and to healthy development. The absence or inadequacy of effective protection constitutes a violation of the principle of the child's best interests [20]. Consequently, interventions concerning children require the application of a child rights-based approach, as well as the treatment of children's rights as a holistic and interconnected system.

The primary responsibility for ensuring children's upbringing and development lies with parents. At the same time, states are also obliged to ensure the effective protection of children's rights and to support parents and caregivers in fulfilling this role. Article 19 of the Convention on the Rights of the Child clearly establishes the state's positive obligation to protect children from all forms of violence [21]. Accordingly, states are required to safeguard children against all forms of physical and psychological violence, including cyberbullying. The fulfilment of this obligation requires comprehensive legislative, administrative, social and educational measures. These include prevention, support programmes, and clear procedures for identifying, reporting, investigating, and handling cases [22].

Children's rights can be understood within a specific tripartite legal relationship involving the child, the parent and the state [23]. This relationship is further complicated by the new challenges emerging in the digital environment. In interpreting this tripartite legal relationship in the digital context, the concept of the "cyberfare state model" provides an analytical framework that facilitates an understanding of the nature of state interventions [24] and of possible approaches to addressing digital risks from a child rights perspective [25].

There is currently no uniformly accepted international definition of cyberbullying. Within the European Union, Neubauer and González-García, examining education policy and prevention-oriented approaches, concluded that the regulation of cyberbullying typically relies on soft law instruments and primarily appears within legal frameworks originally designed to address traditional bullying. Their analysis further indicates that the EU would benefit from a common, consolidated, hard law-based anti-bullying framework [26].

Child rights-oriented analyses addressing cyberbullying generally focus on a single branch of law or a specific national regulatory context [27]. This is also reflected in child rights approaches within the literature, which emphasize the need for a complex and integrated response to digital risks and harms affecting children, but typically do not extend to a comparative examination of remedial and access-to-justice structures [28].

For states to fulfil their protective obligations arising from the Convention on the Rights of the Child within the framework of the rule of law, an integrated approach is required that combines the management of digital risks and harms with effective remedies for violations of children's rights.

This study aims to provide a comparative analysis of how European Union Member States address cyberbullying affecting children within their legal and policy frameworks. It focuses on the extent to which these frameworks incorporate a child rights-based approach and ensure access to effective remedies. By developing a structured analytical framework, the study contributes to identifying systemic patterns and gaps in formal regulatory responses across the EU.

2. Materials and Methods

This study employs a qualitative, document-based and comparative methodology to examine the legal and policy responses developed by European Union Member States to address cyberbullying affecting children [26,29]. This methodological approach was selected to enable a structured and comparable assessment of formal regulatory responses across EU Member States. By focusing on harmonized EU-level sources and predefined variables, the study ensures consistency and reduces subjectivity in cross-country comparison.

The aim of the research is not to measure the effectiveness of individual measures, but rather to explore the extent to which national regulatory and policy frameworks ensure the application of a child rights-based approach and provide the normative conditions for the right to effective remedies in the digital environment. The analysis covers all 27 EU Member States and applies a harmonized coding scheme. Full EU-wide coverage enables the identification of structural patterns and reduces the risk of selection bias in the comparative analysis [30,31]. The analysis focuses on normative elements relating to the definitional treatment of cyberbullying, criminal and civil law protection, as well as the institutionalization of preventive and reactive measures.

2.1. Normative Framework

In European states, the protection of children in the online environment is jointly established through international legal instruments (such as the United Nations Convention on the Rights of the Child), European Union law, and national regulatory frameworks. Although EU Member States apply diverse regulatory approaches, a common characteristic is the strong emphasis placed on legal responses to cyberbullying, victim support, prevention, and education. This study is grounded in the Charter of Fundamental Rights of the European Union, the EU Strategy on the Rights of the Child, the Better Internet for Kids (BIK+) initiative, and the Digital Services Act (DSA). Together, these instruments serve as benchmarks for assessing whether national approaches are child rights-centered, prevention-oriented, and supportive of access to effective remedies.

The European Union has adopted an EU-level action plan on cyberbullying [32,33]. However, the EU's competence in this field is limited, as the regulation and management of cyberbullying primarily fall within the competence of the Member States. The Union holds only a supplementary competence in this area, meaning that it may support, coordinate or complement national measures, but may not adopt comprehensive regulation that would displace Member State authority. At the same time, the EU may exert a stronger influence on the protection of children through indirect means. The Victims' Rights Directive, the EU's human rights obligations, as well as the principles of proportionality and subsidiarity, all provide scope for certain forms of intervention. In addition, Article 83 of the Treaty on the Functioning of the European Union may provide a legal basis for the EU—subject to the fulfilment of specific conditions—to introduce minimum rules in criminal law addressing certain forms of cyberbullying, where this is justified by the need to combat cross-border crime or to ensure the attainment of EU objectives [34].

Article 24 of the Charter of Fundamental Rights of the European Union provides that children are entitled to such protection and care as is necessary for their well-being, to freely express their views, and to have those views taken into consideration in accordance with their age and maturity, while in all actions relating to children—whether undertaken by public authorities or private institutions—the child's best interests must be a primary consideration [35].

Within the framework of the EU Strategy on the Rights of the Child adopted in 2021, the European Commission committed to strengthening children's awareness of their rights, involving children in policy development, and ensuring that EU legal and policy documents

are accessible in child-friendly formats. This commitment was further reinforced by the establishment of the EU Children's Participation Platform in 2022 [36]. Building on this, the Commission developed the updated digital strategy Better Internet for Kids (BIK+) [37], which serves as a normative reference point for the present study by placing protection, empowerment and participation at the center of children's digital rights.

2.2. Analytical Framework

The BIK+ strategy serves as a normative reference point for the coding dimensions of this study and conceptualizes responses to cyberbullying as an integrated system of preventive and reactive measures. This approach is reflected in the research through distinct groups of variables covering educational prevention (PREV_EDU), explicit national strategies (PREV_STRAT), institutionalized reporting and support channels (HOTLINE), and reporting mechanisms that are specifically designed to be understandable and accessible for children (CHILD_FRIEND). Furthermore, in alignment with the Digital Services Act, the strategy articulates children's access to effective support and remedies as a normative expectation. This reinforces both the study's access-to-justice focus and the interpretative framework applied to the access-to-remedy dimension.

The inclusion of definitional dimensions in the coding scheme was based on the JRC findings and the relevant scholarly literature, given that a unified and legally binding international definition of cyberbullying is currently lacking [38,39]. Accordingly, the research coded as separate variables the existence of an explicit definition of cyberbullying (DEF_EXIST) and the normative source of that definition (DEF_SOURCE). Building on this definitional framework, criminal and civil law responses were also coded, including the existence of a specific criminal offence addressing cyberbullying (CRIM_SPEC), the applicability of general criminal law provisions (CRIM_GEN), child-specific criminal law safeguards (CHILD_SPEC), as well as personality rights protection and child-friendly civil law remedies (CIV_EXIST, CIV_CHILD).

The policy guidelines set out in the BIK+ strategy are rendered enforceable through the binding platform obligations established by the Digital Services Act (DSA), concerning reporting, content removal and access-to-remedy mechanisms [40]. The DSA's horizontal due diligence obligations—including the requirement to provide easily accessible notice-and-action systems, transparent complaint-handling procedures, and effective access to remedies—constitute a direct normative basis for the coding of institutionalized reporting channels (HOTLINE) and child-friendly reporting mechanisms (CHILD_FRIEND).

2.3. Data Sources and Data Collection

Data collection was conducted on the basis of three parallel yet comparable groups of sources: the European Commission's Joint Research Centre (JRC) analysis Cyberbullying: Insights from Science, Policy and Legislation [30], the 2025 report published within the framework of the Better Internet for Kids (BIK+) initiative [31], and the related country reports and policy maps [41]. The analysis did not involve an independent or direct review of national legislation or policy documents. This approach was chosen to ensure comparability across Member States, as harmonized EU-level sources provide consistent and systematically collected information.

Coding was carried out exclusively based on the JRC findings, the BIK 2025 report, and the BIK policy maps, which provide harmonized, EU-level assessments of Member States' legal and policy responses to cyberbullying. Across all three source groups, data collection followed a uniform set of variables, enabling comparison across analytical levels as well as an assessment of consistency between the sources. This approach ensures methodological consistency and comparability across Member States, particularly considering the absence

of a common definition and the variation of national legal and policy approaches identified in EU-level analyses [4,30].

The analysis was conducted through manual coding using a predefined codebook. During the coding process, each variable was assigned clear numerical values based on either binary or ordinal scales. Variables were coded exclusively based on explicit legal or policy provisions. The study does not aim to assess implementation or practical operation but rather records the formal existence of regulatory and institutional elements. Table 1 presents the variables used to code national legal and policy responses to cyberbullying. These variables constitute the direct building blocks of the composite CB level indicator. All variables capture the formal existence of legal or policy measures and do not assess their implementation or effectiveness.

Table 1. Coding variables for the analysis of national legal and policy responses to cyberbullying affecting children.

Code	Meaning	Values/Interpretation
DEF_EXIST	Existence of a cyberbullying definition	0 = none; 1 = implicit (covered under general online harassment or violence concepts); 2 = explicit (stand-alone cyberbullying definition)
DEF_SOURCE	Normative source of the definition	0 = none; 1 = soft law (strategy, policy document, guidelines); 2 = hard law (legislation)
CRIM_SPEC	Specific criminal offence addressing cyberbullying	0 = no; 1 = yes
CRIM_GEN	Cyberbullying prosecutable under general criminal law	0 = no; 1 = yes
CHILD_SPEC	Child-specific criminal law protection	0 = no; 1 = yes
CIV_EXIST	Civil law/personality rights protection available	0 = no; 1 = yes
CIV_CHILD	Child-friendly civil procedures or special rules	0 = no; 1 = yes
PREV_EDU	Educational prevention at national level	0 = none; 1 = recommended; 2 = mandatory
PREV_STRAT	National strategy explicitly addressing cyberbullying	0 = no; 1 = yes
HOTLINE	National reporting hotline for cyberbullying	0 = no; 1 = yes
CHILD_FRIEND	Child-friendly reporting mechanism	0 = no; 1 = yes

The observed discrepancies between the data sources can be explained by differences in data collection timing. The BIK Policy Monitor is based on a structured survey conducted during the 2024/25 data collection cycle, between November 2024 and February 2025, reflecting country-reported information at a specific point in time [31]. In contrast, the JRC report draws on a multi-method approach combining literature review, bibliometric analysis and policy review, relying on datasets covering a longer period, with bibliometric data extending up to 2025 [30].

These differences in timing, together with variations in methodological design and definitional scope, mean that the sources capture different stages and aspects of national regulatory developments. This helps explain observed divergences in the data and should be considered when interpreting the aggregation approach applied in this study.

2.4. Multi-Level Source Validation and Consistency Assessment

The research was based on the combined use of multiple EU-level harmonized data sources. Parallel coding of the JRC findings, the Better Internet for Kids [31] report, and the associated policy maps enabled the assessment of cross-source consistency. During the coding process, a uniform set of variables was applied across all sources.

For each Member State, the CB level was computed as an additive, unweighted sum of the coded variables. Country-specific scores were determined using a maximum-value rule across sources: for each variable, the highest value identified in either the JRC findings or the BIK dataset was retained. This approach captures the highest formally identifiable level of legal and policy coverage and reduces the risk of underestimating national frameworks due to differences in data collection or reporting practices.

The composite CB score is based on 11 variables coded on binary (0–1) and ordinal (0–2) scales. Ordinal coding was applied to reflect differences in normative strength, with higher values assigned to more binding legal forms (e.g., hard law compared to soft law). As a result, the total score ranges from 0 to 14 and was normalized to a 0–5 scale for comparability, with all variables equally weighted.

Based on these scores, the CB level classifies Member States into five categories (low, emerging, moderate, high, and very high), reflecting the extent of formal regulatory coverage across the examined dimensions. The classification relies on predefined threshold ranges (0–1; 1–2; 2–3; 3–4; 4–5) and serves as an analytical tool for structured comparison rather than as a normative benchmark.

3. Results

3.1. Coverage Patterns Based on BIK 2025 Aggregated Data

Among the 27 Member States, at least one variable shows a discrepancy between the aggregated findings of the BIK 2025 report and the corresponding country reports in 21 cases. These discrepancies are almost exclusively unidirectional: across several variables, the country reports indicate higher levels of coverage than the aggregated BIK 2025 assessment. This suggests that the BIK 2025 data aggregation adopts a more conservative approach, while the country reports capture more fine-grained, national-level details.

Based on the data available in the BIK 2025 report, Member State coverage varies markedly across individual variables. General criminal law protection (CRIM_GEN) and the existence of institutionalized reporting channels (HOTLINE) are identifiable in all 27 EU Member States, while educational and preventive measures (PREV_EDU) are also widely present, appearing in 26 Member States. Civil law remedies (CIV_EXIST) and national strategies explicitly addressing cyberbullying (PREV_STRAT), however, are available in only 17 Member States, while child-specific civil law protection (CIV_CHILD) can be identified in just 9 Member States. The lowest levels of coverage are observed in relation to the existence of an explicit (hard law-based) cyberbullying definition (DEF_EXIST, DEF_SOURCE) and child-friendly procedural or reporting mechanisms (CHILD_FRIEND), which are present in only 4 Member States. Specific, stand-alone criminal offences addressing cyberbullying (CRIM_SPEC) and dedicated child-specific legal safeguards (CHILD_SPEC) are identifiable in only 2 Member States.

This pattern suggests that while general and preventive instruments are widely institutionalized, explicit and child-specific regulatory responses remain limited across Member States, a trend that is also reflected in Table 2.

Table 2. Member States identified in the BIK 2025 aggregated dataset by variable.

Code	Member States
DEF_EXIST/DEF_SOURCE	Austria, Belgium, France, Italy
CRIM_GEN	All 27 Member States
CRIM_SPEC	Austria, Hungary
CHILD_SPEC	Austria, France
CIV_EXIST	Austria, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Portugal, Romania, Spain, Sweden
CIV_CHILD	Austria, Estonia, France, Germany, Ireland, Italy, Portugal, Slovenia, Spain
PREV_EDU	All Member States except Slovenia
PREV_STRAT	Austria, Belgium, Cyprus, France, Germany, Hungary, Ireland, Italy, Latvia, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain
HOTLINE	All 27 Member States
CHILD_FRIEND	Austria, Belgium, Estonia, Germany

3.2. Divergences Between Aggregated Findings and Country Reports

An examination of the country reports reveals that the coverage of normative elements addressing cyberbullying is, in several cases, higher than that indicated by the aggregated BIK 2025 assessment, as reflected in the country-level data presented in Table 3. The aggregated BIK 2025 assessment appears to rely on more restrictive or standardized coding criteria, whereas the country reports often identify additional national-level elements, including implicit or sector-specific measures.

Table 3. Member States identified in the BIK 2025 dataset by variable, country-level data based on country profiles.

Code	Member States
DEF_EXIST/DEF_SOURCE	Austria, Belgium, Croatia, France, Greece, Ireland, Italy
CRIM_GEN	All Member States except Greece
CRIM_SPEC	Austria, Hungary
CHILD_SPEC	Austria, Belgium, Croatia, Cyprus, France, Ireland, Latvia, Spain
CIV_EXIST	All Member States except Hungary
CIV_CHILD	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Lithuania, Malta, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden
PREV_EDU	All 27 Member States
PREV_STRAT	Austria, Belgium, Bulgaria, Cyprus, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden
HOTLINE	All Member States except Denmark, France, and Italy
CHILD_FRIEND	Austria, Belgium, Croatia, Cyprus, Estonia, Germany

Regarding general, horizontal instruments, general criminal law protection (CRIM_GEN) is identifiable in 26 Member States, institutionalized reporting channels (HOTLINE) in 24 Member States, and educational and preventive measures (PREV_EDU) in all 27 Member States. Taken together, these findings confirm that general criminal and preventive instru-

ments are widely established across Member States, even where aggregated assessments differ in scope.

A markedly different pattern emerges with respect to remedial and strategic elements. According to the country reports, civil law remedies (CIV_EXIST) are present in 26 Member States, national strategies addressing cyberbullying (PREV_STRAT) in 22 Member States, and child-specific civil law protection (CIV_CHILD) likewise in 22 Member States. These figures exceed the coverage levels reported in the BIK 2025 assessment.

Child-specific and explicit normative elements nonetheless remain the most limited in terms of diffusion. The existence of an explicit cyberbullying definition (DEF_EXIST, DEF_SOURCE) is identifiable in 7 Member States, child-friendly procedural or reporting mechanisms (CHILD_FRIEND) are identifiable in 6 Member States, and child-specific legal protection (CHILD_SPEC) is identifiable in 8 Member States.

These findings indicate that, in most cases, country-level reporting captures a broader and more nuanced range of regulatory elements than aggregated datasets.

3.3. Comparison with JRC Findings

According to the JRC findings, the coverage of normative elements addressing cyberbullying across Member States follows a distinct pattern when compared to both the BIK 2025 report and the country reports, particularly with respect to explicit definitional and reactive mechanisms. Among general legal and preventive instruments, the existence of a cyberbullying definition (DEF_EXIST, DEF_SOURCE) is identifiable in all 27 Member States, at least at the level of soft law. General criminal law protection (CRIM_GEN) is present in 26 Member States. Educational and preventive measures (PREV_EDU) are also widely established, appearing in 25 Member States.

At the same time, the coverage of remedial and strategic elements proves to be more moderate. Civil law remedies (CIV_EXIST) are present in 20 Member States, while child-specific civil law protection (CIV_CHILD) appears in 16 Member States. National strategies addressing cyberbullying (PREV_STRAT) are identifiable in only 12 Member States based on the JRC findings.

The most limited coverage is observed in relation to child-specific and reactive mechanisms. Specific, stand-alone criminal offences (CRIM_SPEC) are identifiable in 3 Member States, child-friendly procedural or reporting mechanisms (CHILD_FRIEND) likewise in 3 Member States, while child-specific legal protection (CHILD_SPEC) appears in 11 Member States. The detailed country-level data based on the JRC findings are presented in Table 4.

These discrepancies are illustrated in Table 5 below. Overall, the JRC analysis places greater emphasis on explicit legal and definitional frameworks, while the BIK 2025 report identifies horizontal, institutionalized solutions—such as reporting channels and preventive measures—as broadly established. The country reports, in turn, more frequently identify fragmented, implicit and child-specific remedial elements.

These differences can partly be explained by variations in data collection and methodological approaches, with the BIK Policy Monitor reflecting country-reported data from the 2024/25 survey cycle, while the JRC analysis draws on multi-source evidence covering a longer period. Overall, the differences across datasets highlight how methodological choices and definitional approaches significantly influence the perceived level of regulatory coverage.

Table 4. Member States identified in the JRC dataset by variable.

Code	Member States
DEF_EXIST/DEF_SOURCE	All 27 Member States
CRIM_GEN	All Member States except Malta
CRIM_SPEC	Austria, Hungary, Malta
CHILD_SPEC	Austria, Czech Republic, France, Germany, Greece, Italy, Lithuania, Malta, Romania, Slovenia, Spain
CIV_EXIST	Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Netherlands, Poland, Portugal, Romania, Spain, Sweden
CIV_CHILD	Austria, Belgium, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Netherlands, Portugal, Romania, Spain, Sweden
PREV_EDU	All Member States except Estonia and Lithuania
PREV_STRAT	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Portugal
HOTLINE	Austria, Belgium, Croatia, Denmark, Finland, France, Germany, Greece, Portugal
CHILD_FRIEND	Austria, Belgium, Croatia

Table 5. Divergences in the coverage of cyberbullying-related legal and policy responses across EU Member States based on JRC findings, BIK 2025 aggregated data and country reports.

Code	BIK2025 (n = 27)	Country Report BIK (n = 27)	JRC (n = 27)
DEF_EXIST/DEF_SOURCE	4	7	27
CRIM_GEN	27	26	26
CRIM_SPEC	2	2	3
CHILD_SPEC	2	8	11
CIV_EXIST	17	26	20
CIV_CHILD	9	22	16
PREV_EDU	26	27	25
PREV_STRAT	17	22	12
HOTLINE	27	24	9
CHILD_FRIEND	4	6	3

3.4. CB Level Scores and Classification

The composite CB level scores and corresponding category classifications for each Member State are presented in Table 6. The results indicate that most Member States exhibit a relatively high level of formal regulatory and policy coverage. However, this overall pattern is primarily driven by the widespread presence of general legal and preventive instruments, while more targeted, child-specific and explicit regulatory elements remain less developed. No Member States fall into the low or emerging categories, and most countries cluster in the high and very high segments of the scale.

Table 6. CB level scores and category classification of EU Member States based on the composite indicator.

Country	CB Score	Category
Austria	5.00	Very high
Belgium	4.28	Very high
Bulgaria	3.57	High
Croatia	3.92	High
Cyprus	4.28	Very high
Czech Republic	3.92	High

Table 6. *Cont.*

Country	CB Score	Category
Denmark	3.57	High
Estonia	3.57	High
Finland	3.57	High
France	4.28	Very high
Germany	4.28	Very high
Greece	3.92	High
Hungary	3.21	High
Ireland	4.28	Very high
Italy	4.28	Very high
Latvia	3.57	High
Lithuania	3.21	High
Luxembourg	2.85	Moderate
Malta	4.67	Very high
Netherlands	3.92	High
Poland	2.85	Moderate
Portugal	3.21	High
Romania	3.92	High
Slovakia	3.92	High
Slovenia	3.92	High
Spain	4.28	Very high
Sweden	3.57	High

4. Discussion

4.1. Structural Patterns of Cyberbullying Regulation in the EU

The results not only highlight differences between data sources but also reveal the structural fragmentation of Member State regulatory approaches to cyberbullying. Although general, horizontal legal and policy instruments—most notably criminal law protection, preventive measures and reporting mechanisms—are present in the vast majority of EU Member States, child-specific and child-friendly solutions are integrated into national frameworks only to a limited and uneven extent. These differences do not necessarily indicate an absence of regulation, but rather reflect the coexistence of implicit, sectoral and often poorly coordinated normative responses, a pattern also identified in the literature [26,42].

To interpret the regulatory landscape, the study applies the CB level as a composite, structural indicator that enables an assessment of the extent to which Member States approach the regulation of cyberbullying within a coherent framework. As illustrated in Figure 1, the CB level reaches notably high values in a considerable number of Member States, suggesting that cyberbullying is formally covered from a regulatory perspective and that preventive approaches—particularly at the level of education and policy strategies—are widely present. As Neubauer and Gonzalez-Garcia demonstrate, European responses to bullying and cyberbullying are predominantly based on preventive and educational policy instruments, most often formulated as soft law measures [26].

At the same time, it is important to emphasize that, as a structural indicator, the CB level measures exclusively the formal existence of legal and policy frameworks based on the coded variables. The index does not provide information on the practical functioning, implementation or effectiveness of regulation, nor does it reflect the extent to which existing mechanisms are accessible or usable by children in everyday practice. This limitation is consistent with previous research highlighting that the existence of legal frameworks does not necessarily ensure effective protection, particularly in a context where cyberbullying regulation remains fragmented and unevenly developed across jurisdictions [43]. The distribution of CB level categories across Member States illustrates this pattern (Figure 1).

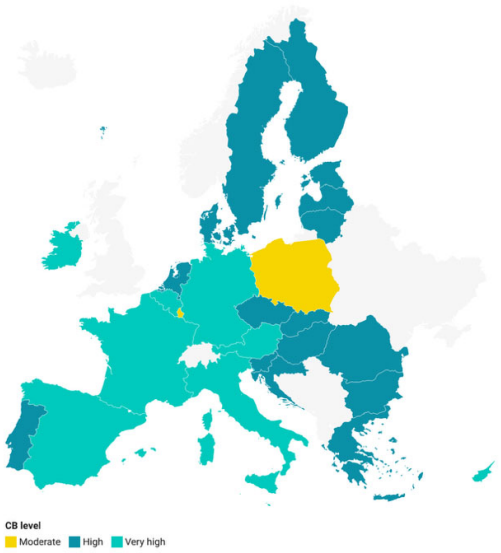


Figure 1. Structural CB Level Categories across EU Member States.

The disaggregated results (Table 5) reveal several structural shortcomings in national cyberbullying regulation. First, the existence of a stand-alone criminal offence specifically addressing cyberbullying (CRIM_SPEC) is extremely rare within the European Union, indicating that the legal treatment of the phenomenon relies predominantly on general criminal law categories. As Janković and Stošić highlight, many jurisdictions address cyberbullying through the application of existing offences such as insult, defamation or harassment rather than through specific legal provisions [44]. While this approach allows for the sanctioning of individual cases, it does not provide a uniform and targeted normative framework capable of addressing the specific characteristics of cyberbullying—namely its online nature, repetitive dynamics and frequent involvement of children.

In addition, the limited presence of child-specific legal protection (CHILD_SPEC) suggests that most Member States do not treat online harassment affecting children as an autonomous policy issue but rather subsume it under broader legal categories. This finding is consistent with previous research showing that cyberbullying is typically regulated through general legal provisions rather than through child-specific or digital-specific norms [44,45].

Similarly low levels of coverage can be observed regarding reporting and procedural mechanisms specifically designed for children (CHILD_FRIEND). By contrast, general institutionalized reporting channels (HOTLINE) are present in the majority of Member States, indicating that a basic reporting infrastructure for addressing cyberbullying is well established at the EU level. However, based on the EU-level sources examined, these channels only exceptionally appear as mechanisms structured in a genuinely child-friendly manner. The documents rarely refer to age-appropriate information, simplified procedures or communication that is understandable for children.

This structural discrepancy reflects a broader pattern identified in the literature, namely that the formal existence of reporting mechanisms does not necessarily translate into their effective use by young people. As Hendry et al. emphasize, adolescents frequently refrain from reporting cyberbullying incidents or seeking help from formal channels, often due to lack of trust, perceived ineffectiveness, or the absence of supportive and accessible communication [46]. Similarly, Unaliya et al. point out that reporting practices remain limited and are often accompanied by weak institutional follow-up, which may further discourage engagement with existing mechanisms [47]. These findings suggest

that reporting infrastructures, while formally established, often fail to operate as genuinely accessible entry points to protection.

From a child rights perspective, this gap is particularly significant. Access to remedies depends not only on the existence of mechanisms but on their accessibility and usability for children. As Jackson et al. note, support systems must be adapted to young users' capacities, yet such child-sensitive elements remain only weakly integrated in national frameworks [48].

As a result, children's actual opportunities to seek redress remain limited in many Member States, even where reporting mechanisms formally exist. This finding is particularly problematic considering EU policy documents—most notably the BIK+ strategy and the Digital Services Act—which articulate as a normative expectation not merely the existence of reporting channels, but their accessibility and comprehensibility for children.

The absence of an explicit normative definition of cyberbullying (DEF_EXIST, DEF_SOURCE) also constitutes one of the weakest dimensions identified. Although implicit or soft law-based definitions appear in some Member States, the lack of clear, legally described conceptual frameworks contributes to regulatory fragmentation and complicates both legal application and EU-level comparability. This finding is consistent with previous research highlighting the lack of conceptual consensus in defining cyberbullying and its implications for understanding and addressing the phenomenon [49].

Concerning the implementation of the BIK+ strategy and the Digital Services Act (DSA), the findings indicate that further strengthening of the child rights dimension is required at the Member State level. While EU-level frameworks increasingly emphasize the primacy of the child's best interests and the necessity of child-friendly and accessible mechanisms, national regulatory practices tend to reflect this approach only partially. High CB level values indicate broad formal normative coverage; however, the limited integration of child-specific and access-to-remedy-oriented elements suggests that the child-centered principles embedded in the BIK+ strategy and the DSA require further reinforcement at the national level.

4.2. Cyberbullying Governance Through the Lens of the Cooperative Cyberfare State

Within the cyberfare state model, different regulatory approaches can be distinguished. One ideal type is the "smart total control" model, which presupposes strong state control and extensive surveillance. By contrast, the "cooperative cyberfare state" model emphasizes the role of the individual and regulates in a manner that ensures respect for human rights—and thus children's rights—as part of the material requirements of the rule of law [24]. Between these two models, a wide range of transitional forms can be identified, and even within democratic rule-of-law systems, an increasingly intensive level of state intervention can be observed. When designing age-based access restrictions, however, due regard must be given to the principle of evolving capacities, as well as to the normative and emancipatory dimensions of children's rights [50]. Interpreting these considerations within the framework of the tripartite legal relationship highlights that, alongside state reactions and preventive interventions, the respect for the rights of individuals (both parents and children) and prevention based on the development of digital competences are essential elements within rule-of-law constraints [25,51].

Alongside the role of the state, parental mediation can evidently play a significant role in addressing risks in the digital environment, including in cases of cyberbullying. However, these issues fall outside the detailed scope of the present study [52,53]. Empirical research conducted by Tao et al., involving primary school children, indicates that the effects of parental mediation are not uniform and that parental mediation alone cannot be considered a sufficiently effective protective mechanism. Moreover, under certain conditions, overly

restrictive parental attitudes may not reduce but rather increase children's exposure to cyberbullying. By contrast, digital media literacy emerges as an independent protective factor capable of mitigating risks associated with digital technology use, including the occurrence of cyberbullying [54].

About the role of parents, the study by Perić-Prkosovački et al. indicates the existence of perceptual asymmetry between parents and children concerning the occurrence, nature and handling of digital violence—particularly cyberbullying. Children consistently report significantly higher levels of exposure than those perceived or acknowledged by their parents. One reason for this discrepancy is that children often do not share their negative experiences, while parents tend to underestimate the intensity of children's digital presence. At the same time, there is clear agreement between parents and children that safe, child-friendly reporting and support systems are needed [55], as well as targeted anti-bullying campaigns [56].

Emphasizing the importance of rule-of-law frameworks is consistent with the arguments advanced by Milosevic et al., who stress that cyberbullying is not merely an online safety issue and that preventive practices grounded in a dignity-based framework are essential [57]. According to El Asam, cyberbullying behavior can be understood as an umbrella concept, which necessitates legal regulation addressing both prevention and the remediation of rights violations caused by cyberbullying. In this context, legal awareness among members of society plays a decisive role [42]. In some countries, initiatives based on horizontal knowledge transfer and peer mentoring have emerged, aiming to involve young people rather than relying exclusively on traditional, adult-centered prevention strategies. Concrete examples include the NETMENTOR programme in Hungary [58] and the Cyberscout programme in Bulgaria [59].

In states approximating the cooperative model, the protection of children in the digital environment entails a dual state responsibility: (1) the provision of preventive tools, such as educational programmes and awareness-raising campaigns, and (2) the establishment of effective intervention mechanisms in cases where risks or harms materialize. These include, for example, reporting systems, notice-and-action procedures, content moderation measures, and access to support services for child victims. Such mechanisms are increasingly emphasized in EU policy frameworks, including the BIK+ policy monitor, which highlights the importance of complaint mechanisms and support infrastructures for children, as well as in the EU Action Plan against Cyberbullying, which calls for improved reporting tools, child-friendly procedures and effective support services across Member States [33,37]. In the present study, the analysis focuses explicitly on the formal presence of these expectations. Within the cooperative model, market actors also play an important role in the effective enforcement of children's rights; however, this aspect falls outside the scope of the paper [60].

4.3. Child-Specific Gaps Within Formally Strong Regulatory Frameworks

The empirical findings presented in this study can be interpreted within this cooperative regulatory framework, particularly in relation to the observed child-specific gaps. The cooperative type of the cyberfare state model is particularly evident in the legal order of the European Union and in Member State regulatory frameworks. Within this approach, the governance of the digital environment is shaped not by all-encompassing state control, but by the substantive and material requirements of the rule of law. These requirements include respect for human rights—including children's rights—and the assurance of their effective protection in the digital sphere as well. This perspective is reflected within the human rights framework by UNCRC General Comment No. 25, which elaborates children's rights in the digital environment [61]. Both within the EU regulatory framework and in the

practice of EU institutions, there is a growing tendency to interpret the management of online risks increasingly through a child rights-based lens.

This regulatory logic—grounded in respect for children's rights, the primacy of the fundamental rights framework, and cooperation with Member States—clearly reflects the core characteristics of the cooperative type of the cyberfare state. According to this model, online safety and the protection of children in the digital environment can only be conceived within a child rights-based framework. The role of the state is to establish a system of prevention, education, awareness-raising and post-harm intervention that is guided by the child's best interests.

This approach is also supported by the child rights literature, which emphasizes the need for a complex and integrated response to risks and harms arising in the digital environment, and highlights that rule-of-law obligations cannot be fulfilled solely through preventive or informational measures but must also be underpinned by effective remedial structures [62,63]. Findings from empirical research examining the effectiveness of preventive programmes indicate that solutions which are relevant to children, participation-based and age-appropriate play a key role in addressing cyberbullying [64]. Longitudinal evidence further suggests that cyberbullying often follows a dynamic pattern of escalation, in which inadequate or inaccessible protective mechanisms may contribute to sustained victimization and cumulative harm [65,66]. This is consistent with the findings of the present study, which demonstrate that the formal existence of regulatory and policy frameworks alone is insufficient, and further justify the need to strengthen the child rights-based approach within Member State responses.

When interpreting high CB level values, it is particularly important to consider longitudinal evidence indicating that peer victimization—including cyberbullying—may result in persistent mental health and psychosocial consequences if formally existing protective mechanisms are not accessible to or effective for children [67].

4.4. Limitations

This study is subject to certain methodological limitations that should be considered when interpreting the findings.

First, the composite CB level indicator applies equal weighting across all variables. This approach simplifies comparison but does not differentiate between the relative importance of individual dimensions. As a result, the indicator may not fully capture the varying significance of specific regulatory elements. As highlighted in the OECD Handbook on Composite Indicators, weighting choices can influence results and may obscure meaningful differences between dimensions if not grounded in a clear theoretical framework [68].

Second, the CB level captures only the formal existence of legal and policy measures. It does not reflect their practical functioning or their accessibility for children. Consequently, high scores should not be interpreted as evidence of effective protection, but rather as an indication of the breadth of formal regulatory coverage.

5. Conclusions

This study provides a structural mapping of legal and policy responses to cyberbullying across EU Member States. The findings show that, while general legal and preventive instruments are widely established, child-specific and child-friendly elements remain unevenly developed. High CB level scores therefore reflect the breadth of formal regulatory coverage rather than the effectiveness or accessibility of protection mechanisms.

These results highlight a key gap between the formal existence of regulatory frameworks and their child-centered implementation. In this context, the findings support the need to strengthen access-to-remedy mechanisms and the integration of child rights princi-

ples within national frameworks, in line with EU initiatives such as the BIK+ strategy and the Digital Services Act. The recent EU Action Plan against cyberbullying further reinforces the importance of coordinated child-centered approaches.

Future research should build on this structural analysis by examining the practical functioning, accessibility, and child-friendliness of existing mechanisms, including through approaches that incorporate children's perspectives.

Author Contributions: Conceptualization, E.K.-S. and B.M.; methodology, E.K.-S.; software, E.K.-S. and B.M.; validation, E.K.-S., B.M. and B.S.; formal analysis, E.K.-S., B.M. and B.S.; investigation, E.K.-S., B.M. and B.S.; resources, E.K.-S. and B.M.; data curation, E.K.-S., B.M. and B.S.; writing—original draft preparation, E.K.-S., B.M. and B.S.; writing—review and editing, E.K.-S. and B.M.; visualization, E.K.-S.; supervision, E.K.-S.; project administration, E.K.-S.; funding acquisition, E.K.-S. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Széchenyi István University. Author E.K.-S. was supported by the STARTING_25 funding scheme of the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study were derived from publicly available sources in the public domain, including the Joint Research Centre (https://publications.jrc.ec.europa.eu/repository/handle/JRC144335 accessed on 10 December 2025) and Better Internet for Kids (BIK+) policy reports and country profiles (https://better-internet-for-kids.europa.eu/en/knowledge-hub/policy-monitor accessed on 30 October 2025). The analytical dataset generated through the coding process is described within the article. Further details can be provided by the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Moral-García, J.; Rusillo-Magdaleno, A.; Patiño-Villada, F.; Martínez-López, E. Bullying and Cyberbullying Are Associated with Inappropriate Use of the Internet, Cell Phones, and Video Games in Children and Adolescents. *Eur. J. Investig. Health Psychol. Educ.* **2025**, *15*, 82. [CrossRef] [PubMed]
2. Livingstone, S.; Stoilova, M. *The 4Cs: Classifying Online Risk to Children. CO:RE Short Report Series on Key Topics*; Leibniz-Institut für Medienforschung Hans-Bredow-Institut (HBI): Hamburg, Germany, 2021; p. 14. [CrossRef]
3. European Commission. *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; Communication C/2025/5519*; European Union: Brussels, Belgium, 2025.
4. Murphy, C. *Cyberbullying Among Young People: Laws and Policies in Selected Member States*; European Parliamentary Research Service: Brussels, Belgium, 2024; Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI(2024)762331_EN.pdf (accessed on 30 October 2025).
5. Cosma, A.; Molcho, M.; Pickett, W. *A Focus on Adolescent Peer Violence and Bullying in Europe, Central Asia and Canada: Health Behaviour in School-Aged Children (HBSC) International Report from the 2021/2022 Survey*; WHO Regional Office for Europe: Copenhagen, Denmark, 2024; Volume 2.
6. Knauf, R.-K.; Eschenbeck, H. School Bullying and Cyberbullying—Associations of Student's Roles with Social-Cognitive and Affective Reactions. *Soc. Psychol. Educ.* **2025**, *28*, 51. [CrossRef]
7. Alkhallouf, A. Parental Cyberbullying through a Global Lens: Children's Digital Rights and Social Media Policies. *J. Child. Media* **2021**, *15*, 448–453. [CrossRef]
8. Suler, J. The Online Disinhibition Effect. *CyberPsychol. Behav.* **2004**, *7*, 321–326. [CrossRef]
9. Slonje, R.; Smith, P.K. Cyberbullying: Another Main Type of Bullying? *Scand. J. Psychol.* **2008**, *49*, 147–154. [CrossRef]

10. Zhu, Y.; Li, W.; O'Brien, J.E.; Liu, T. Parent–Child Attachment Moderates the Associations Between Cyberbullying Victimization and Adolescents' Health/Mental Health Problems: An Exploration of Cyberbullying Victimization Among Chinese Adolescents. *J. Interpers. Violence* **2021**, *36*, NP9272–NP9298. [CrossRef]
11. Armitage, R. Bullying in Children: Impact on Child Health. *BMJ Paediatr. Open* **2021**, *5*, e000939. [CrossRef]
12. Chen, Q.; Chan, K.L.; Guo, S.; Chen, M.; Lo, C.K.; Ip, P. Effectiveness of Digital Health Interventions in Reducing Bullying and Cyberbullying: A Meta-Analysis. *Trauma Violence Abus.* **2023**, *24*, 1986–2002. [CrossRef]
13. Antoniadou, N.; Kokkinos, C.M. Cyber and School Bullying: Same or Different Phenomena? *Aggress. Violent Behav.* **2015**, *25*, 363–372. [CrossRef]
14. Fulantelli, G.; Taibi, D.; Scifo, L.; Schwarze, V.; Eimler, S.C. Cyberbullying and Cyberhate as Two Interlinked Instances of Cyber-Aggression in Adolescence: A Systematic Review. *Front. Psychol.* **2022**, *13*, 909299. [CrossRef]
15. Rong, K.; Chu, X.; Zhao, Y. Qualitative Analyses on the Classification Model of Bystander Behavior in Cyberbullying. *Front. Psychol.* **2023**, *14*, 1152331. [CrossRef] [PubMed]
16. Zych, I.; Farrington, D.P. Defining Bullying and Cyberbullying According to the Scientific Community: A Mixed Method Study. *Int. J. Bullying Prev.* **2026**. [CrossRef]
17. Liang, Z. Legal Regulation on Cyberbullying of Children. *Asian Res. J. Arts Soc. Sci.* **2022**, *17*, 21–26. [CrossRef]
18. Rodionov, A.E. The Modern International Legal Framework of Cyberbullying in Relation to the Protection of Children's Rights. *Int. Law* **2025**, *14*, 13–35. [CrossRef]
19. McVay, S.S.; Santo, J.; Lydiatt, H. The Impact of Cyberbullying Victimization on Adolescents' School-Related Distress Across Nine Countries: Examining the Mitigating Role of Teacher Support. *Soc. Sci.* **2025**, *14*, 559. [CrossRef]
20. Espino, E.; Veiga-Simão, A.M.; Ferreira, P.C.; Sánchez-Jiménez, V.; Rey, R.D. Adolescents Suffering from Long-Term Cyberbullying Victimisation: Peer Pressure and Anger Dysregulation as Risk Factors. *Res. Child Adolesc. Psychopathol.* **2025**, *53*, 1339–1351. [CrossRef]
21. United Nations. *Convention on the Rights of the Child*; United Nations: New York, NY, USA, 1989; Available online: https://www.ohchr.org/sites/default/files/crc.pdf (accessed on 10 January 2025).
22. Whalen, C. Article 19: The Right to Protection from All Forms of Violence. In *Monitoring State Compliance with the UN Convention on the Rights of the Child*; Vaghri, Z., Zermatten, J., Lansdown, G., Ruggiero, R., Eds.; Children's Well-Being: Indicators and Research; Springer International Publishing: Cham, Germany, 2022; Volume 25, pp. 293–302.
23. Sutherland, E.E. The Enigma of Article 5 of the United Nations Convention on the Rights of The Child: Central or Peripheral? *Int. J. Child. Rights* **2020**, *28*, 447–470. [CrossRef]
24. Kelemen, R. The Cyberfare State: Divergent Models of Digital Governance and Control. *Front. Polit. Sci.* **2026**, *8*, 1748562. [CrossRef]
25. Kovács-Szépvölgyi, E.; Kiss, Z.C. Mind the Net: Parental Awareness and State Responsibilities in the Age of Grooming. *Soc. Sci.* **2025**, *14*, 506. [CrossRef]
26. Neubauer, A.; Gonzalez-Garcia, A. The European Union's Response to Bullying and Cyberbullying: An Educational Policy Analysis. *Soc. Sci.* **2025**, *14*, 505. [CrossRef]
27. Lievens, E. Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights. *Nord. J. Hum. Rights* **2021**, *39*, 128–145. [CrossRef]
28. Henares-Montiel, J.; Benítez-Hidalgo, V.; Ruiz-Pérez, I.; Pastor-Moreno, G.; Rodríguez-Barranco, M. Cyberbullying and Associated Factors in Member Countries of the European Union: A Systematic Review and Meta-Analysis of Studies with Representative Population Samples. *Int. J. Environ. Res. Public Health* **2022**, *19*, 7364. [CrossRef] [PubMed]
29. Zweigert, K.; Kötz, H. *Introduction to Comparative Law*, 3rd ed.; Clarendon Press, Oxford University Press: Oxford, UK, 1998; ISBN 978-0-19-826860-4.
30. European Commission, Joint Research Centre; Villar Onrubia, D.; Barreda Ángeles, M.; Cachia, R.; Economou, A.; López Cobo, M. *Cyberbullying*; EUR 40535; Publications Office of the European Union: Luxembourg, 2025.
31. O'Neill, B.; Dopona, V. *The Better Internet for Kids Policy Monitor Report 2025*; European Schoolnet, Prepared for the European Commission: Brussels, Belgium, 2025. Available online: https://better-internet-for-kids.europa.eu/en/knowledge-hub/policy-monitor (accessed on 1 December 2025).
32. von der Leyen, U. *Europe's Choice: Political Guidelines for the Next European Commission 2024–2029*; European Commission: Brussels, Belgium, 2024; Available online: https://commission.europa.eu (accessed on 1 December 2025).
33. European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Action Plan Against Cyberbullying "Safer Online, Stronger Together"; COM(2026) 71 Final*; European Commission: Strasbourg, France, 2026.
34. European Parliament, Directorate-General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs. *Cyberbullying Among Young People*; Study for the LIBE Committee; European Union: Brussels, Belgium, 2016; Available online: http://www.europarl.europa.eu/supporting-analyses (accessed on 1 December 2025).

35. European Union. Charter of Fundamental Rights of the European Union (2000/C 364/01). *Off. J. Eur. Communities* **2000**, *364*, 1–22.
36. European Commission. *2025 Annual Report on the Application of the EU Charter of Fundamental Rights: Taking Stock of the Implementation of the Strategy to Strengthen the Application of the Charter of Fundamental Rights in the EU.COM(2025) 751 Final*; European Commission: Brussels, Belgium, 2025.
37. European Commission. *A Digital Decade for Children and Youth: The New European Strategy for a Better Internet for Kids (BIK+). COM(2022) 212 Final*; European Commission: Brussels, Belgium, 2022.
38. Cheng, L.; Hu, X.; Matulewska, A.; Wagner, A. Exploring Cyberbullying: A Socio-Semiotic Perspective. *Int. J. Leg. Discourse* **2020**, *5*, 359–378. [CrossRef]
39. Xu, Y.; Trzaskawka, P. Towards Descriptive Adequacy of Cyberbullying: Interdisciplinary Studies on Features, Cases and Legislative Concerns of Cyberbullying. *Int. J. Semiot. Law* **2021**, *34*, 929–943. [CrossRef]
40. European Union. 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). *Off. J. Eur. Union* **2022**, *L 277*, 1–102.
41. European Union. Directorate-General for Communications Networks, Content and Technology. The Better Internet for Kids (BIK) Policy Monitor. Available online: https://better-internet-for-kids.europa.eu/en/knowledge-hub/policy-monitor (accessed on 1 December 2025).
42. El Asam, A.; Samara, M. Cyberbullying and the Law: A Review of Psychological and Legal Challenges. *Comput. Hum. Behav.* **2016**, *65*, 127–141. [CrossRef]
43. Paunovic, N. Cyberbullying of Children: Challenges of Victim Support. *Temida* **2018**, *21*, 249–268. [CrossRef]
44. Janković, A.; Stošić, L. Cyberbullying Legislation: The Role of Cyberbullying Law. *Pravo Teor. Praksa* **2022**, *39*, 97–108. [CrossRef]
45. Sekar, A.Y.; Setiono, J.; Sutrisno, S. Legal Vacuum Analysis and the Need for Criminal Policy Reformulation in Handling Cyberbullying Cases in Indonesia Based on the Perspective of Child Protection and the Law on Electronic Information and Transactions. *J. Greenation Sos. Polit.* **2025**, *3*, 558–567. [CrossRef]
46. Hendry, B.P.; Hellsten, L.M.; McIntyre, L.J.; Smith, B.R.R. Recommendations for Cyberbullying Prevention and Intervention: A Western Canadian Perspective from Key Stakeholders. *Front. Psychol.* **2023**, *14*, 1067484. [CrossRef] [PubMed]
47. Unaliya, M.; Kataria, Y.; Bhutra, Y.; Chauhan, R.; Maseleno, A.; Isnanto, R. Exploring Cyberbullying: Reporting Practices, Institutional Responses, and Perceptions of Effectiveness. *Siber Int. J. Adv. Law SIJAL* **2024**, *1*, 70–82. [CrossRef]
48. Jackson, E.; Boyes, M.; Blundell, B.; Hirn, J.; Leitão, S. Managing Cyberbullying among Adolescents with Neurodevelopmental Disorders: A Scoping Review. *Int. J. Speech-Lang. Pathol.* **2025**, *27*, 341–356. [CrossRef] [PubMed]
49. Dennehy, R.; Meaney, S.; Walsh, K.A.; Sinnott, C.; Cronin, M.; Arensman, E. Young People's Conceptualizations of the Nature of Cyberbullying: A Systematic Review and Synthesis of Qualitative Research. *Aggress. Violent Behav.* **2020**, *51*, 101379. [CrossRef]
50. Livingstone, S.; Sylwander, K.R. There Is No Right Age! The Search for Age-Appropriate Ways to Support Children's Digital Lives and Rights. *J. Child. Media* **2025**, *19*, 6–12. [CrossRef]
51. Zhu, C.; Huang, S.; Evans, R.; Zhang, W. Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Front. Public Health* **2021**, *9*, 634909. [CrossRef]
52. Buçaj, E.; Haziri, F. Cyberbullying and Cyberstalking: Parents' Role to Protect Their Children. *Multidiscip. Rev.* **2024**, *7*, 2024079. [CrossRef]
53. Rega, V.; Gioia, F.; Boursier, V. Parental Mediation and Cyberbullying: A Narrative Literature Review. *Marriage Fam. Rev.* **2022**, *58*, 495–530. [CrossRef]
54. Tao, S.; Reichert, F.; Law, N.; Rao, N. Digital Technology Use and Cyberbullying Among Primary School Children: Digital Literacy and Parental Mediation as Moderators. *Cyberpsychol. Behav. Soc. Netw.* **2022**, *25*, 571–579. [CrossRef]
55. Perić-Prkosovački, B.; Brkić Jovanović, N.; Runčeva, J. Perceptual Differences Between Parents and Children Regarding Digital Violence. *Societies* **2025**, *15*, 327. [CrossRef]
56. Vlaanderen, A.; Bevelander, K.E.; Kleemans, M. Empowering Digital Citizenship: An Anti-Cyberbullying Intervention to Increase Children's Intentions to Intervene on Behalf of the Victim. *Comput. Hum. Behav.* **2020**, *112*, 106459. [CrossRef]
57. Milosevic, T.; Collier, A.; Norman, J.O. Leveraging Dignity Theory to Understand Bullying, Cyberbullying, and Children's Rights. *Int. J. Bullying Prev.* **2023**, *5*, 108–120. [CrossRef]
58. Better Internet for Kids. Hungary—Policy Monitor Country Profile. Available online: https://better-internet-for-kids.europa.eu/en/knowledge-hub/hungary-policy-monitor-country-profile (accessed on 10 December 2025).
59. Better Internet for Kids. Bulgaria—Policy Monitor Country Profile. Available online: https://better-internet-for-kids.europa.eu/en/knowledge-hub/bulgaria-policy-monitor-country-profile (accessed on 10 December 2025).
60. Milosevic, T. *Protecting Children Online?: Cyberbullying Policies of Social Media Companies*; The MIT Press: Cambridge, MA, USA, 2018.

61. Committee on the Rights of the Child. General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. 2021. Available online: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=H7gSiTrGnN8Kz89nitiHmFJww2AnfdyTopg7NaqMK3cP9VzxbcxmYirTrM+ToYhGEltLAW33x5DgMRr3Lim7Tg== (accessed on 10 December 2025).
62. Lievens, E.; Livingstone, S.; McLaughlin, S.; O'Neill, B.; Verdoodt, V. Children's Rights and Digital Technologies. In *International Human Rights of Children; International Human Rights*; Kilkelly, U., Liefaard, T., Eds.; Springer: Singapore, 2018. [CrossRef]
63. Livingstone, S.; Third, A.; Burton, P.; Witting, S.; Lievens, E.; Steinberg, S.; Gilutz, S.; Souter, D. The UN Committee on the Rights of the Child's General Comment on the Digital Environment. *AoIR Sel. Pap. Internet Res.* **2023**. [CrossRef]
64. Hajnal, Á. Cyberbullying Prevention: Which Design Features Foster the Effectiveness of School-Based Programs?: A Meta-Analytic Approach. *Intersections* **2021**, *7*, 40–58. [CrossRef]
65. Lozano-Blasco, R.; Cortés-Pascual, A.; Latorre-Martínez, M.P. Being a Cybervictim and a Cyberbully—The Duality of Cyberbullying: A Meta-Analysis. *Comput. Hum. Behav.* **2020**, *111*, 106444. [CrossRef]
66. Giuliani, A.; Petruccelli, I.; D'Urso, G. Longitudinal Evidence on Peer Victimisation and Persistent Mental Health Outcomes in Youth: A Systematic Review. *Behav. Sci.* **2025**, *15*, 1734. [CrossRef]
67. Antivilo-Bruna, A.; Patino-Alonso, C. Categorical Data in the Evaluation of School-Based Cyberbullying Prevention Programs: A Review of the Literature. *Behav. Sci.* **2026**, *16*, 93. [CrossRef]
68. OECD; European Union; European Commission; Joint Research Centre. *Handbook on Constructing Composite Indicators: Methodology and User Guide*; European Commission, Organisation for Economic Co-Operation and Development, SourceOECD (Online Service), Eds.; OECD: Paris, France, 2008.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.