

Digital Violence Against Children with Special Educational Needs and Cyber Due Diligence: Institutional and Educational Responses

Manayay-Mercedes Angela Giovanna ¹, Sendon-Alba, Jordan Joffre ²,
Muñoz-Ccuro, Felipa Elvira ³

¹ Doctoral Program in Law,
Graduate School, San Ignacio de Loyola University, Lima, Peru

Email : angela.manayay@epg.usil.pe

Orcid : <https://orcid.org/1730-1739-1730-1739>

² Public Ministry, Lima-Peru

Email : josendon@mpfn.gob.pe

Orcid : <https://orcid.org/1730-1739-1730-1739>

³ San Ignacio de Loyola University-Graduate School

Email : felipa.munoz@epg.usil.pe

Orcid : <https://orcid.org/1730-1739-1730-1739>

HOW TO CITE:

Manayay-Mercedes Angela
Giovanna ¹, Sendon-Alba, Jordan
Joffre ², Muñoz-Ccuro, Felipa
Elvira ³ (2026). Effectiveness of AI-
Based Lead Generation and
Market Segmentation in the
Bangalore Real Estate Industry.
International Journal of Special
Education, 41(22s), 1730-1739

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

This study analyzes the response of the State and educational institutions to digital violence against children and adolescents, with special attention to those with special educational needs, neurodiversity, or disabilities. Through a critical literature review, international research has been linked to the duty of protection applicable to digital media. Experiences of cybervictimization and the distress caused in specific groups are described; however, the differences identified in the studies make it difficult to apply their results to all students who need support. The analysis highlights the importance of accessible channels for reporting incidents and lawfully preserving digital evidence. Furthermore, the responsibility of digital platforms in the design of their services and the detection of alerts will also be considered. Finally, it will be concluded that digital due diligence must involve swift and appropriate actions according to each student's needs, and its effectiveness will be evaluated considering both harm reduction and opportunities for digital learning and participation.

Keywords: Cyberbullying, special educational needs, inclusive education, due diligence, school cybersecurity.

1. Introduction

The rapid digital transformation of daily life has changed how we interact socially and how learning environments take place; however, it has also created new avenues for violence against children and adolescents, facilitated by digital technologies. This problem is even more visible in the field of special and inclusive education,

where students with special educational needs (SEN), disabilities, or neurodiversity face greater vulnerability to cyberbullying, grooming, extortion, and digital manipulation. Unlike physical attacks, digital violence against victims with SEN is characterized by the difficulty in identifying socio-technical deception, the indefinite duration and amplification of the harm, which overwhelms the response capacity of

schools and child protection institutions, highlighting a gap between international due diligence standards and the operational capacity of the education system.

From a criminological and legal perspective, digital violence alters both the execution and the continuation of criminal acts. The capacity of information technologies to endlessly reproduce content and the permanence of digital footprints exponentially increase primary and secondary victimization. Digital violence presents a qualitative severity because it affects the psychological well-being of minors. As mentioned, unlike physical spaces where aggression can be stopped by leaving, in the digital environment, the persistence and universality of virtual content continuously exposes victims. All of this can generate anxiety, depression, isolation, and suicidal thoughts. Therefore, legal assessment must go beyond formal criminal classification to analyze the real impact on early childhood development.

The due diligence standard, in accordance with international human rights jurisprudence, imposes enhanced positive obligations on States with regard to children. Applied in the digital sphere, the “best efforts” principle has been established to prevent, investigate, punish, and redress harm. This model integrates State obligations with the corporate responsibility of platforms (*Child Rights Due Diligence* and “security by design”) based on five functional pillars: Prevention, Protection, Investigation/Prosecution, Sanction, and Redress.

Studies on cyberbullying help us understand this new form of aggression and its consequences. To safeguard students with special educational needs and neurodivergent identities, it is necessary to examine what happens when the incident comes to light: the school's response, the support they receive, and how the justice system intervenes. Coordination must be carried out as quickly as possible, considering that digital information or evidence may be lost. All these issues lead us to the following research question: *What does international scientific evidence on digital violence against*

children and adolescents with special educational needs and neurodivergent identities contribute to guiding the application of cyber due diligence in educational and justice institutions? The objective of this study is to critically review the available information and examine its relationship with legal protection frameworks, in order to propose criteria for an accessible, timely, and coordinated response within the context of special and inclusive education.

2. Methodology

Design : A qualitative systematic review was conducted in accordance with PRISMA 2020, focusing on methodological rigor and reproducibility. The descriptive and interpretive approach encompassed international scientific literature, legal doctrine, and regulatory frameworks published between 2016 and 2026.

Sample: The review comprised 20 specialized documents, including empirical articles, dogmatic analyses, and normative reports. These documents address child protection, special education, digital violence against vulnerable groups, and state due diligence.

Instruments: Searches in Scopus, Web of Science and international academic repositories were performed using the following Boolean equation: ("digital violence" OR "cyberbullying" OR "grooming") AND ("child protection" OR "special educational needs" OR "disability" OR "neurodiversity") AND ("due diligence" OR "institutional response" OR "school response").

Procedure: 285 records were identified and 53 duplicates were removed. Of the 232 abstracts reviewed, 142 were excluded for lack of direct thematic relevance. Subsequently, 90 full texts were examined and 70 were discarded for not specifically addressing digital child protection or criminal due diligence. The final selection comprised 20 documents.

Data analysis: A qualitative thematic synthesis was carried out using structured matrices of documentary extraction to categorize the findings in victimology, procedural law, state obligations and algorithmic governance.

This research was conducted in strict adherence to the standards of integrity and academic ethics inherent in systematic reviews. Due to its qualitative and indirect methodological design, focused exclusively on the critical examination of documents, legislation, and public domain scientific publications, the work was carried out without tests, surveys, or direct interaction with human participants. Consequently, intellectual

property and copyright were protected through the faithful and objective attribution of each source consulted, in accordance with APA citation guidelines (7th edition).

3. Results

The systematic synthesis of the 20 documentary units analyzed is presented in Table 1:

Table 1. Documentary Analysis Matrix of Included Studies on Digital Violence and Due Diligence

ID	Author(s) and Year	Country/ Scope	Methodology	Sample Corpus	/	Key Findings (Due Diligence / Digital Violence)
01	Stringhi (2024)	European Union	Qualitative (doctrinal and legislative analysis)	EU regulatory framework (DSA and Directives)		The DSA leaves gaps by excluding encrypted private messaging and ignoring the intersectional approach to digital violence.
02	Perić-Prkosovački et al. (2025)	Serbia	Quantitative (descriptive and inferential)	N = 450 students from 5th to 8th grade and their parents		Intergenerational gap: parents systematically underestimate the online harassment their children experience.
03	Cronin et al. (2017)	United Kingdom	Qualitative (systematic review)	Review of 35 studies and interventions		Technology facilitates prevention, but rigorous evaluation of its real impact on harm reduction is lacking.
04	Baldry et al. (2024)	Australia and the United Kingdom	Qualitative, with literature review, co-design, thematic analysis, and speculative fiction	6 XR and technology professionals; specialized literature; 15 speculative fictions		XR platforms and generative AI can amplify psychological, social, and physiological attacks and damage; the article proposes the Inter-

						Reality Threat Model to identify these risks and guide their mitigation.
05	Ahmad & Smith (2024)	Indonesia, Philippines, Thailand	Systematic (dogmatic-legal)	Review	Normative documents and reports (UNICEF, ECPAT, INTERPOL)	Increased online violence and child exploitation; procedural gaps and lack of state forensic technical capacity.
06	Pane et al. (2025)	Indonesia	Qualitative-explanatory (functionalist/ecological)		Children who are victims of digital violence and their guardians	Family dysfunction and lack of supervision increase vulnerability to grooming, cyberbullying, and extortion.
07	Abu Okeal et al. (2026)	Australia/France	Qualitative, descriptive-analytical and comparative legal		Digital security and childhood laws in Australia, France, and Egypt.	Australia and France have adopted preventative models against online child abuse, imposing requirements on platforms such as age verification and content moderation. Egypt maintains a primarily reactive approach.
08	Cosgun Demirdag and Kucuk (2026)	Türkiye	Quantitative, serial mediation (PROCESS Model 6).		n = 438 parents (69% women; M = 40.5 years) with children from preschool to high school.	Technological literacy among parents increases their awareness of cyberbullying prevention, acting both directly and indirectly through the development of healthy digital practices (digital parenting) and the

						reduction of parental stress.
09	O'Reilly et al. (2024)	United Kingdom	Qualitative (participatory action research)		18 boys and girls aged 10 to 11 years old from Primary Education	Digital disinhibition due to a lack of physical cues leads to cruelty; the DEC ethical framework helps manage harassment.
10	Rohde-Abuba (2025)	Germany	Qualitative Analysis (Discourse and Netnography)		8 documentaries about <i>kidfluencers</i> and social media profiles	Digital hatred towards hyper-visible minors is monetized by algorithms; symbolic violence turns into real threats.
11	Urbano, R. (2024)	Italy / Spain	Qualitative (hermeneutic and content-based)		European laws, UNICEF/IEEE reports and literature	AI generates risks of impersonation, synthetic violence, and cognitive manipulation in minors, requiring algorithmic ethics.
12	Nadhiroh et al. (2023)	Indonesia	Quantitative (cross-sectional survey)		480 adolescents (12 to 25 years old)	High prevalence of cyber gender violence (64%), with a predominantly psychological impact (55%: anxiety, depression and fear).
13	Morolong & Batani (2025)	Lesotho	Qualitative (Stakeholder Analysis)		Key actors and child protection institutions	Legislative gaps, inter-ministerial fragmentation, and poor digital literacy among parents and police forces.
14	Yun et al. (2023)	South Korea / USA	Systematic Review	Scoping	Global (34 studies of digital interventions)	Digital interventions predominate in child mental health; ethical and

						technology access challenges are identified.
15	Rodríguez et al. (2021)	Spain	Systematic Review	Literature	Global (articles on computing and security)	Computer tools (AI/NLP, computer vision, IoT) allow the detection of online and offline violence.
16	Coco & de Souza Dias (2021)	United Kingdom	Qualitative legal analysis	dogmatic-	ICJ case law, UN GGE reports and Tallinn Manual 2.0	Cyber due diligence is a flexible duty of conduct ("best efforts") to prevent and remedy harm.
17	Baroni and Padovani (2025)	European Union	Critical analysis of public policies		EU AI Act , AI Code of Practice and UN/UNESCO frameworks	The AI Act limits its requirements to "high-risk" systems, omitting mandatory safeguards and <i>gender mainstreaming</i> for generative digital violence.
18	Lendvai et al. (2025)	Union	Critical normative and qualitative analysis		Digital Services Act (<i>DSA</i>), E-Commerce Directive and codes of conduct	The DSA requires due diligence from platforms through "notice and takedown," but explicitly omits digital gender violence as a mandatory systemic risk.
19	Sam et al. (2026)	Sierra Leone	Mixed (qualitative and quantitative with co-design)		70 survey participants and 7 key informants	Interactive digital prototypes improve inter-institutional coordination for effective prevention and response.

20	Morales et al. (2026)	Netherlands, Israel, Sweden/digital	Conceptual interdisciplinary and development of a theoretical framework	article; review of a framework	Interdisciplinary Literature and 10 Contributions from the Special Issue	Digital violence on platforms arises from the interaction between technologies, algorithms, platform policies, cultural contexts, and power relations, and can be amplified and normalized.
----	-----------------------	-------------------------------------	---	--------------------------------	--	---

4. Discussion

Upon examining the information available in the corpus under analysis, it can be seen that the specialized literature primarily addresses the topic of cyberbullying and due diligence from a general population perspective. Thus, the analysis of the results mapped in Table 1 is projected from a dogmatic-legal and intersectional perspective, deriving from the analyzed information the theoretical, procedural, and educational criteria necessary to establish cyber due diligence and implement protocols adapted to the specific needs of children with special educational needs and neurodivergent identities.

Dynamics of Victimization, Grooming and Perception Gaps:

Digital violence against children manifests in various ways, including cyberbullying, grooming, extortion, and the production or dissemination of child sexual abuse material (CSA). In these cases, family support is crucial for the early detection of such aggression. Pane et al. (2025) emphasize the importance of psychological support and guidance within the student experience. Perić-Prkosovački et al. (2025), on the other hand, acknowledge differences in the perceptions of students and families. The analyzed results will allow for an examination of the difficulties in recognizing and communicating the phenomenon of violence, although they do not demonstrate that the gap is greater among students with cognitive or sensory disabilities.

In terms of prevention, Cosgun Demirdag and Kucuk (2026) examine the relationship between technological literacy, parental stress, digital parenting practices, and preventative awareness of cyberbullying. Their research suggests that families should be provided with support that includes technological guidance and emotional support, without equating these measures with a proven reduction in aggression. On the other hand, the psychological dimension also requires attention: Nadhiroh et al. (2023) indicate that digital violence against adolescents and young adults has repercussions. Their results provide contextual information but do not allow us to attribute specific effects on the educational continuity of students with special educational needs. In special and inclusive education, this contribution adds to the proposal to develop and evaluate psychoeducational resources that adapt to different communication and comprehension needs. The participatory experience of O'Reilly et al. (2024) highlights the value of incorporating children's perspectives into the design of educational resources. Based on this, it is proposed that schools, families, and students participate in developing easily accessible protocols to identify risks, report instances of aggression, and receive support. Training can address self-regulation, self-determination, and understanding digital interactions, according to each student's specific support needs. These resources should be coordinated with those responsible for student care and include referral channels that allow for timely responses and

follow-up on well-being and educational continuity.

Procedural Bottlenecks, Chain of Custody and Digital Evidence:

Technical limitations and a lack of forensic expertise hinder the judicial response to digital violence in Indonesia, the Philippines, and Thailand (Ahmad & Smith, 2024). Preserving digital evidence, such as IP addresses, server files, and metadata, requires immediate action to ensure its integrity and chain of custody. In cross-border investigations, delays and insufficient coordination impede progress and can exacerbate revictimization. Therefore, each case must be assessed to determine whether the deficiencies violate the duty of due diligence, which requires examining applicable obligations and reasonable measures.

Cyber Due Diligence, Encryption and Regulatory Gaps:

Dogmatically, cyber due diligence is conceptualized as a conduct obligation of the State, which must make better efforts in preventing, neutralizing, and redressing damages caused by technology (Coco & de Souza Dias, 2021). However, critical regulatory gaps remain in both national and international frameworks. Comparative jurisprudence adopts preventive models and requires moderation of platforms (Abu Okeal et al., 2026), while regulatory frameworks such as the EU Digital Services Act (DSA) exclude end-to-end encrypted messaging (E2EE), through which a substantial volume of technology-related harm (TRF) is transmitted, and ignore digital gender-based violence as a mandatory systemic risk (Lendvai et al., 2025; Stringhi, 2024). Furthermore, global moderation policies implement criteria that are universal and do not take into account local environments, which produces governance failures and epistemic violence (Esteban Morales et al., 2026).

Algorithmic Governance and Responsible Technological Innovation:

Technologies have a dual dimension, as immersive and emergent environments, with XR platforms combined with generative AI,

significantly amplify the risk of harassment, AI-generated violence (deepfakes), cognitive manipulation, and physiological or omnidirectional harm through sociotechnical attacks (Baldry et al., 2024; Urbano, 2024). Added to this is the monetization of hate directed at kidfluencers through algorithms (Rohde-Abuba, 2025) and the limitations of instruments such as the EU AI Act, which restricts its safeguards to “high-risk” systems without a cross-cutting and intersectional approach focused on children (Baroni & Padovani, 2025). On the other hand, computer architecture provides us with mitigation tools such as Natural Language Processing (NLP) and computer vision for detecting inappropriate content (Rodríguez et al., 2021). However, for these tools to be effective in special education, they must be integrated with interactive and inclusive digital prototypes that enable communication among teachers, mental health professionals, families, and judicial authorities (Sam et al., 2026), thus ensuring that digital environments are safe and adapted to functional diversity.

5. Conclusion

First, digital violence against children and adolescents in special and inclusive education settings demands a coordinated response that includes prevention, protection, and access to justice mechanisms. The analysis must consider the mechanisms for disseminating and recommending content, as well as the difficulties that prevent individuals from recognizing abuse and seeking support. Experiences and support needs can vary among students, so neurodivergence or disability do not allow us to assume uniform vulnerability in all cases. In this context, the punitive response must be accompanied by educational measures and support that promote safer digital participation. Secondly, digital due diligence must be implemented through timely, accessible, and appropriate state actions in accordance with the identified risk. In terms of evidence, it is necessary to lawfully obtain and preserve digital evidence, document its handling, and ensure that justice system personnel are able to examine its integrity, authenticity, and context. Unjustified

delays can lead to the loss of digital evidence and prolong the harmful effects; its legal relevance must be assessed considering the risk and the measures that each authority can apply. Immediate protection of the victim must be coordinated within an investigation that respects due process and the right to a defense. Third, to protect children, digital technology companies must include risk assessments for children's rights and ensure the security of their products' design, offering accessible ways to report and receive a response. These functions should be defined according to the characteristics of each service and the applicable regulatory framework. Encrypted messaging and digital reality environments present challenges that require a comprehensive examination of protection, privacy, and research. Similarly, moderation policies must address the cultural and linguistic diversity of user groups and the communication

needs of those requiring specific support. Fourth, it is proposed to strengthen coordination between schools, child protection services, and the justice system through inclusive protocols that define responsible parties, referral channels, and expedited response times according to the urgency of each case. This action should include training for educational staff, accessible digital literacy for students and families, and comprehensive communication support during the intervention and investigation. The effectiveness of these measures should be evaluated considering the timeliness of the response, educational continuity, the persistence of the harm, and the student's experience. Reparation and support should be integral to the follow-up process, ensuring that the intervention does not end solely with the removal of the content or the imposition of a criminal penalty.

References

- Abu, A., et al. (2026). Preventive legislative approaches to child protection in the digital environment: A comparative study of Australia, France, and Egypt. *Nusantara: Journal of Law Studies* , 5 (1), 205–228. <https://doi.org/10.66325/nusantaralaw.v5i1.222>
- Ahmad, D.N.F., & Smith, N.N. (2024). Digital safety for women and children: Legal and policy challenges in Indonesia, Philippines, and Thailand. *Journal of Law and Legal Reform* , 5(4), 1673–1696. <https://doi.org/10.15294/jllr.v5i4.16539>
- Baldry, E., et al. (2024). From embodied abuse to mass disruption: Generative, inter-reality threats in social, mixed-reality platforms. *Digital Threats: Research and Practice* , 5 (4), Article 38, 1–36. <https://doi.org/10.1145/3696015>
- Baroni, A., & Padovani, C. (2025). AI, democracy and gender equality: EU regulatory frameworks and the wager of gender mainstreaming. *European Journal of Communication* , 40 (4), 411–432. <https://doi.org/10.1177/02673231251349323>
- Coco, A., & de Souza Dias, T. (2021). 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law. *The European Journal of International Law* , 32(3), 771–805. <https://doi.org/10.1093/ejil/chab056>
- Cosgun Demirdag, P., & Kucuk, S. (2026). The impact of parental behavior in the digital age on awareness of cyberbullying prevention: the role of technological literacy and parental stress. *BMC Psychology* , 14 , article 456. <https://doi.org/10.1186/s41730-1739-01730-1739>
- Cronin, C., Sood, S., & Thomas, D. (2017). From innovation to transcreation: Adapting digital technologies to address violence against children. *Child Abuse Review* , 26(3), 215–229. <https://doi.org/10.1002/car.2447>
- Lendvai, G.F., Papp, J.T., & Gosztonyi, G. (2025). Mitigating harmful content on social media via platform regulation: The Digital Services Act and content assessment. *Információs Társadalom* , 25 (2), 59–72. <https://dx.doi.org/10.22503/inftars.XXV.2025.2.4>

- Morales, E., Divon, T., & Lundqvist, M. (2026). Context matters: Understanding the platformization of violence. *New Media & Society* , 28 (4), 1395–1411. <https://doi.org/10.1177/14614448261420823>
- Morolong, M., & Batani, J. (2025). Stakeholders' perspectives on child online safety in Lesotho: Insights, challenges and opportunities. In *DATA '25: Proceedings of the Sixth International Conference on Digital Age & Technological Advances for Sustainable Development*, 28–35. ACM. <https://doi.org/10.1145/3747897.3747902>
- Nadhiroh, AM ., Winarti, E. ., Rozifa, AW ., & Saudah, N. . (2023). Multi-Dimensional Impact of Cyber Gender-Based Violence: Examining Physical, Mental, Social, Cultural, and Economic Consequences. *Caracas Medical Gazette* , 131 (Supl 4), S591–S598. https://saber.ucv.ve/ojs/index.php/rev_gmc/article/view/27115
- O'Reilly, M., Levine, D., Batchelor, R., & Adams, S. (2024). Digital ethics of care and digital citizenship in UK primary schools: Children as interviewers. *Journal of Children and Media* , 18 (4), 585–604. <https://doi.org/10.1080/17482798.2024.2394932>
- Pane, E., Mukri, Alamsyah, & Yanis, A.M. (2025). Family dysfunction: The reproduction of online violence against children. *El-USrah: Jurnal Hukum Keluarga* , 8(2), 1080–1101. <https://doi.org/10.22373/ujhk.v8i2.30041>
- Perić-Prkosovački, B., Brkić Jovanović, N., & Runčeva, J. (2025). Perceptual differences between parents and children regarding digital violence. *Societies* , 15(12), Article 327. <https://doi.org/10.3390/soc15120327>
- Rodríguez, DA, et al. (2021). A systematic review of computing solutions to address violence against women and children. *IEEE Access* , 9, 114622–114639. <https://doi.org/10.1109/ACCESS.2021.3103459>
- Rohde-Abuba, C. (2025). “I know where you live, let's be friends”: Digital violence in the context of kidfluencing. *Kriminologie – Das Online-Journal* , 7 (4), 476–490. <https://doi.org/10.18716/ojs/krimoj/2025.4.3>
- Sam, S., et al. (2026). Socially aware design of interactive systems to combat gender violence. *International Journal of Human-Computer Studies* , 215, Article 103876. <https://doi.org/10.1016/j.ijhcs.2026.103876>
- Stringhi, E. (2024). Due diligence obligations in the Digital Services Act: Addressing cyber violence in the EU. *International Review of Law, Computers & Technology* , 38(2), 215–229. <https://doi.org/10.1080/13600869.2023.2295101>
- Urbano, R. (2024). Strategies to protect children from violence in artificial intelligence. *Rotura - Journal of Communication, Culture and Arts* , 4(1), 40–49. <https://doi.org/10.34623/8jry-ws91>
- Yun, J., et al. (2023). Characteristics and potential challenges of digital-based interventions for children and young people: Scoping review. *Journal of Medical Internet Research* , 25 , e45465. <https://doi.org/10.2196/45465>

Acknowledgments (Optional)

This study was developed within the framework of the Doctoral Program in Law of the San Ignacio de Loyola University (Lima, Peru).

Author Declaration

Originality: The authors confirm that the submitted manuscript constitutes original research.

Conflict of interest: The authors declare no conflict of interest with respect to the publication of this article.