

LA ACTUACIÓN DE LA INSPECCIÓN EDUCATIVA ANTE EL CIBERACOSO Y LOS RIESGOS DIGITALES: MARCO LEGAL, JURISPRUDENCIA Y RESPONSABILIDAD INSTITUCIONAL.

THE ROLE OF THE EDUCATIONAL INSPECTORATE IN ADDRESSING CYBERBULLYING AND DIGITAL RISKS AMONG STUDENTS: LEGAL FRAMEWORK, CASE LAW, AND INSTITUTIONAL RESPONSIBILITY

Olivia Vanesa García Rojas

Inspectora de educación, SIE de Málaga Andalucía

ORCID: 0009-0007-1959-6616

Resumen

El presente trabajo analiza el papel de la Inspección Educativa en la gestión de situaciones de ciberacoso y otros riesgos digitales que afectan a menores en el contexto escolar. A partir de un enfoque jurídico-educativo, se examina el marco normativo vigente en España, con especial atención a la legislación educativa, la normativa de protección de datos personales y la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI). Asimismo, se revisa

la jurisprudencia más relevante del Tribunal Supremo, del Tribunal Constitucional y de las Audiencias Provinciales en relación con la difusión no consentida de imágenes, la consideración jurídica del ciberacoso y la responsabilidad patrimonial de la Administración educativa.

El estudio pone de relieve la importancia de la denominada diligencia debida educativa como criterio para evaluar la actuación de los centros docentes ante conflictos digitales entre iguales. En este contexto, se analiza la función supervisora, asesora y mediadora de la Inspección Educativa, destacando su papel en la garantía del interés superior del menor y en la correcta aplicación de los protocolos de convivencia escolar. Finalmente, se proponen criterios técnicos de intervención orientados a reforzar la seguridad jurídica de las actuaciones de los centros educativos y a promover entornos escolares seguros también en el ámbito digital.

Palabras clave: *ciberacoso escolar, riesgos digitales, inspección educativa, protección de datos, convivencia escolar, responsabilidad patrimonial.*

Abstract

This article analyses the role of the Educational Inspectorate in managing situations of cyberbullying and other digital risks affecting minors within the school context. From a legal-educational perspective, it examines the current regulatory framework in Spain, with particular focus on educational legislation, data protection regulations, and Organic Law 8/2021, of June 4, on the comprehensive protection of children and adolescents against violence (LOPVI). Furthermore, it reviews the most relevant case law from the Supreme Court, the Constitutional Court, and Provincial Courts regarding the non-consensual dissemination of images, the legal status of cyberbullying, and the administrative liability of educational authorities.

The study highlights the importance of so-called "educational due diligence" as a criterion for evaluating the actions of schools in the face of digital conflicts between

peers. In this context, the supervisory, advisory, and mediating functions of the Educational Inspectorate are analysed, highlighting its role in guaranteeing the best interests of the child and the correct application of school coexistence protocols. Finally, technical intervention criteria are proposed, aimed at strengthening the legal certainty of school actions and promoting safe school environments also in the digital sphere.

Keywords: *cyberbullying, digital risks, educational inspectorate, data protection, school coexistence, administrative liability.*

1. INTRODUCTION

1.1. Contextual Background

The progressive digitalisation of society has profoundly transformed the ways in which children and adolescents socialise. Information and Communication Technologies (ICT) have expanded opportunities for learning, interaction and social participation; however, they have also created new risk scenarios that directly affect the well-being and fundamental rights of minors.

Digital environments have become spaces in which interpersonal conflicts traditionally confined to face-to-face settings are reproduced and, in some cases, intensified. Cyberbullying, the non-consensual dissemination of images, and social pressure exerted through social networking platforms and instant messaging applications constitute forms of violence that extend beyond the school environment while having a direct impact on school climate and the quality of educational coexistence.

A growing body of international research has highlighted the scale of this phenomenon. The EU Kids Online 2023 report indicates that a significant proportion of European children report having experienced harassment or intimidation through digital media, whether as victims, perpetrators or bystanders. Such experiences have emotional, psychological and educational consequences that adversely affect pupils' overall development and the school climate.

Within this context, schools cannot be regarded as institutions isolated from the social processes that unfold in the digital sphere. Although many of these conflicts originate outside school premises, their consequences are reflected in the everyday life of educational institutions, requiring schools to respond from preventive, educational and legal perspectives.

1.2. Relevance of the Topic

Managing the digital risks affecting pupils is not merely a matter of school coexistence; it also raises significant legal and administrative issues. The widespread use of mobile devices among children and adolescents has led to an increase in behaviours that may infringe fundamental rights, including the rights to honour, privacy and one's own image.

The complexity of these situations requires an institutional response grounded in sound legal principles and coordinated action among all relevant stakeholders. Schools, families, public authorities and minors themselves form part of a network of shared responsibilities that demands both legal certainty and a clear regulatory framework.

Against this background, the Educational Inspectorate assumes a particularly significant role as the body responsible for overseeing the functioning of the education system and ensuring compliance with the applicable legal framework. Its intervention is especially important in cases involving digital violence, as it must verify that schools have implemented the appropriate statutory protocols and that all measures adopted fully respect pupils' fundamental rights.

1.3. Aim of the Article

The aim of this article is to analyse the legislative and jurisprudential framework governing cases of cyberbullying and other digital risks affecting minors within the educational context. On the basis of this analysis, it seeks to examine the responsibilities that may arise for both educational institutions and the educational authorities, as well as the role of the Educational Inspectorate in supervising and providing guidance on the management of such situations.

Furthermore, the article aims to propose a set of technical criteria designed to strengthen legal certainty in inspection practice, promoting interventions that are consistent with the guiding principle of the best interests of the child and with the standards of due diligence expected of educational institutions.

2. CURRENT LEGAL FRAMEWORK

The management of digital incidents involving minors is governed by a complex legal framework that brings together provisions from several branches of law, most notably education law, data protection law and criminal law.

Within the field of education, Organic Law 2/2006 on Education, as amended by Organic Law 3/2020 (LOMLOE), establishes in Article 124 the obligation for all schools to adopt a *School Coexistence Plan* incorporating measures aimed at preventing, identifying and addressing incidents of bullying. This statutory requirement necessarily extends to bullying perpetrated through digital media, given the increasing prevalence of such conduct in pupils' everyday lives.

Educational legislation assigns the Educational Inspectorate responsibility for supervising the implementation of these measures, ensuring that schools adopt appropriate actions to provide a safe learning environment that respects pupils' fundamental rights.

The protection of personal data assumes particular importance in incidents involving the dissemination of digital content. Regulation (EU) 2016/679 of the European Parliament and of the Council, commonly known as the General Data Protection Regulation (GDPR), establishes a legal framework that affords enhanced protection to the personal data of minors in recognition of their particular vulnerability.

Within the Spanish legal system, these safeguards are further developed by Organic Law 3/2018 of 5 December on Personal Data Protection and the Guarantee of Digital Rights (LOPDGDD). This legislation contains specific provisions governing the use of technology within educational settings and establishes mechanisms to protect minors against the dissemination of digital content that may be harmful to them. Article 84 of the Act introduces an obligation to adopt measures safeguarding minors from inappropriate digital content, a provision that is particularly relevant in cases involving the unlawful dissemination of images or recordings.

A particularly significant legislative development was the enactment of Organic Law 8/2021 on the Comprehensive Protection of Children and Adolescents against Violence (LOPIVI). This legislation adopts a comprehensive approach to the prevention of and response to all forms of violence against children, expressly including violence perpetrated through digital technologies. It imposes specific obligations on schools, including the implementation of prevention, detection and intervention protocols, as well as the appointment of a *Well-being and Protection Coordinator*.

Finally, in the most serious cases, criminal law provides mechanisms for the prosecution of certain forms of unlawful conduct. The Spanish Criminal Code criminalises a range of offences relating to the non-consensual dissemination of images and the use of technological means to harass or intimidate minors. Among the most relevant provisions are those concerning the unlawful acquisition and disclosure of confidential information, set out in Article 197, together with the offences relating to the non-consensual dissemination of sexually explicit content.

2.1. Regulatory Framework in Andalusia

Within the Autonomous Community of Andalusia, policies on digital safety and school coexistence are governed by a set of specific legal provisions that develop and supplement the national regulatory framework, adapting it to the competences of the regional educational administration.

The principal legal instrument remains the Order of 20 June 2011, which regulates measures to promote school coexistence in publicly funded educational institutions in Andalusia. This Order provides the legal basis for the development of School Coexistence Plans in Andalusian schools, defining behaviours that undermine school coexistence and establishing procedures for addressing conflicts between pupils.

Nevertheless, given the rapid evolution of Information and Communication Technologies (ICT) and the emergence of new forms of digital violence, this regulatory framework is continuously supplemented and updated through the current Instructions

issued by the Directorate-General responsible for School Coexistence within the Regional Ministry of Educational Development and Vocational Training. These mandatory Instructions provide detailed guidance on the implementation of the Protocol for Action in Cases of Suspected Bullying.

In the specific context addressed in this study, Andalusian legislation clearly establishes the obligation to initiate investigative procedures *ex officio* and to implement provisional safeguarding measures as soon as there are reasonable grounds to suspect harassment or cyberbullying. A particularly significant technical aspect for both schools and the Educational Inspectorate is that this obligation applies irrespective of whether the harmful conduct or dissemination of digital content originated on or off school premises, or outside school hours.

This approach reflects the well-established administrative and educational doctrine that latent or overt conflicts arising in virtual environments—such as instant messaging groups or social networking platforms—have a direct and disruptive impact on school coexistence, undermining the emotional well-being of the pupils concerned and interfering with the normal educational process. Consequently, when assessing schools' compliance with the principle of educational due diligence, the Educational Inspectorate in Andalusia is concerned not merely with verifying formal or procedural compliance, but with ensuring that schools respond proactively, promptly and effectively to incidents occurring in the digital environment, thereby guaranteeing that the Andalusian protocol operates as a genuine instrument for safeguarding the best interests of the child.

3. CASE LAW AND PUBLIC AUTHORITY LIABILITY

Recent developments in Spanish case law have significantly contributed to defining the

scope of the legal responsibilities arising from cyberbullying and other digital risks affecting minors within the educational context. The courts have progressively developed a body of interpretative principles that provides valuable guidance for both educational institutions and the educational authorities.

One of the central issues concerns the legal classification of images and digital content as particularly protected categories of personal data. In this regard, the Criminal Chamber of the Spanish Supreme Court has consistently held that the dissemination of images of minors without the consent of their legal representatives constitutes a serious infringement of the fundamental rights to one's own image and to personal privacy, as protected under Article 18 of the Spanish Constitution. Supreme Court Judgment No. 949/2021 of 25 November (Appeal No. 3064/2019), reaffirmed by Supreme Court Judgment No. 210/2022 of 9 March, confirms this principle by holding that the non-consensual dissemination of intimate content through social networking platforms or messaging applications—criminalised under Article 197.7 of the Spanish Criminal Code—directly infringes these fundamental rights, even where the original image was voluntarily created or shared by the minor concerned. This judgment is particularly relevant within the educational context, where images may circulate rapidly among pupils with limited initial supervision by families.

Another key issue concerns the liability of the educational authorities for failures in the provision of public educational services where bullying or violence occurs between pupils. Supreme Court Judgment No. 3639/2020 of 4 November (Administrative Chamber, Appeal No. 6511/2018), together with the subsequent Supreme Court Judgment No. 4291/2021 of 23 November (Appeal No. 1629/2020), establishes that the educational administration may incur liability where an abnormal functioning of the public service results from omissions or negligence in the management of the conflict. The Supreme Court emphasises that liability does not arise merely from the existence of interpersonal conflict, but from the absence of a prompt and effective institutional response. In particular, liability may arise where a school, despite having reasonable grounds for concern, fails to activate the appropriate anti-bullying protocols or neglects

to adopt suitable interim safeguarding measures to protect the victim. These judgments consolidate the doctrine of educational due diligence, understood as the proactive standard of care expected of educational institutions in preventing, identifying and comprehensively addressing school violence while minimising the psychological and emotional harm suffered by the child.

Likewise, the case law of the Provincial Courts has further clarified the legal criteria for identifying cyberbullying and its intrinsic connection with the educational environment. Several judicial decisions have held that hostile conduct occurring exclusively through digital media should nevertheless be regarded and addressed as school bullying where a causal link exists with the educational setting and where its harmful effects directly affect school coexistence or the well-being of the pupils involved. The courts have consistently emphasised that the fact that messages or online posts are generated outside school premises or outside school hours does not exclude either the school's competence or its duty to intervene.

This principle has been reflected in several judicial decisions. Thus, Judgment No. 144/2021 of the Madrid Provincial Court (23 March) recognised the existence of cyberbullying in a case involving instant messaging exchanges between pupils attending the same school, holding that such interactions formed part of the social relationships established within the educational environment. Similarly, Judgment No. 658/2020 of the Barcelona Provincial Court (16 December) concluded that systematic harassment carried out through social networking platforms seriously disrupted the overall school climate and adversely affected the victim's personal situation within the school, thereby requiring the activation of the school's protective and corrective mechanisms.

From a constitutional perspective, the Spanish Constitutional Court has likewise established important principles concerning the protection of fundamental rights in educational settings. Constitutional Court Judgments Nos. 290/2000 (30 November)

and 14/2003 (28 January) recognise the right to personal data protection as an autonomous fundamental right, guaranteeing individuals control over the use of their personal image and information. The Court further requires that any processing of personal data or institutional intervention within the educational context must strictly comply with the principles of proportionality, necessity and the primacy of the best interests of the child. These constitutional principles remain fully applicable to contemporary incidents arising from pupils' use of digital technologies, particularly where schools are required to conduct investigations or manage digital evidence.

Taken together, this body of case law demonstrates that educational institutions are not expected to exercise absolute or unrealistic supervision over every virtual interaction between pupils. They are, however, required to act with reasonable and diligent care whenever credible indications or reports of bullying or digital violence arise. Accordingly, the prompt activation of the appropriate protocols, the adoption of interim safeguarding measures to protect the victim, and the thorough documentation of all actions taken constitute essential requirements for ensuring legal certainty in administrative decision-making and for reducing the risk of public authority liability.

3.1. Educational Due Diligence in Schools' Response

The concept of educational due diligence has progressively become established as a key interpretative criterion for assessing the response of educational institutions to incidents of peer violence, particularly in the context of cyberbullying and the digital risks associated with pupils' use of technology.

Although Spanish law does not expressly define this concept within the educational sphere, its legal foundations derive from a combined interpretation of educational legislation, child protection law and the case law governing the liability of public authorities. Broadly speaking, educational due diligence may be understood as the set of reasonable measures that educational institutions are expected to implement in order to prevent, identify and address situations capable of affecting pupils' physical, psychological or moral integrity.

From this perspective, the obligation imposed on schools is not to guarantee the complete absence of conflict between pupils, but rather to adopt proportionate and effective measures whenever there are indications of bullying or other forms of violence. The Spanish Supreme Court has consistently held that the educational authorities incur liability where negligence or a failure to fulfil their duties of supervision and pupil protection can be established.

In this regard, Supreme Court Judgment No. 3639/2020, reaffirmed by Supreme Court Judgment No. 4291/2021, makes clear that the failure to activate the established protocols or to adopt appropriate immediate intervention measures in response to a known risk falls below the standard of care required of educational institutions, resulting in an unlawful failure in the provision of the public education service.

The enactment of Organic Law 8/2021 on the Comprehensive Protection of Children and Adolescents against Violence (LOPVI) has further reinforced this institutional obligation by establishing a comprehensive safeguarding framework requiring public authorities and educational institutions to implement preventive measures, early detection mechanisms and intervention procedures for all forms of violence against minors. This legislative approach broadens the scope of institutional responsibility and requires a proactive response focused on the effective protection of pupils.

Within this framework, educational due diligence is reflected in a range of institutional measures, including the existence of regularly updated School Coexistence Plans, the effective implementation of anti-bullying protocols, staff training in digital citizenship and online coexistence, and the adoption of appropriate safeguarding measures whenever risks are identified. Thorough documentation of these actions is equally essential, as it enables schools to demonstrate compliance with the required standard of due diligence.

The Educational Inspectorate plays a central role in monitoring compliance with this standard by verifying that schools correctly implement the established protocols, that

the measures adopted are proportionate, and that all actions taken are guided by the principle of the best interests of the child. In doing so, the Inspectorate strengthens legal certainty in administrative decision-making while helping to ensure an appropriate institutional response to risks arising within the digital environment.

4. THE RESPONSIBILITIES OF EDUCATIONAL INSTITUTIONS

Educational institutions play a fundamental role in preventing and managing cyberbullying and other digital risks affecting pupils. Although schools cannot reasonably be expected to exercise absolute supervision over every interaction between pupils, they are nevertheless required to comply with a standard of reasonable care appropriate to the circumstances.

Schools may incur liability where there is evidence of inadequate preventive measures, insufficient oversight of school coexistence, or an inadequate response to indications of bullying. In this respect, case law has consistently established that schools are not required to guarantee the complete absence of conflict, but rather to respond promptly, proportionately and effectively whenever such situations arise.

All actions taken by the school should be properly documented in order to demonstrate that the necessary measures have been implemented to safeguard the victim and restore a safe and positive school environment. These actions include activating the relevant protocols, communicating with families, adopting interim safeguarding measures and, where appropriate, referring the matter to the competent authorities whenever there are indications that a criminal offence may have been committed.

Within this context, the Educational Inspectorate performs an essential supervisory and advisory function. Its intervention enables the appropriateness of the school's response to be assessed while providing technical guidance that strengthens the legal certainty of the decisions adopted.

5. DIGITAL EDUCATION, PREVENTION AND AN INSTITUTIONAL CULTURE OF SAFEGUARDING

Preventing digital risks within educational settings cannot be limited to reacting to individual incidents; rather, it requires the development of an institutional culture of safeguarding that integrates digital education, school coexistence and the effective protection of pupils' rights. Numerous studies have shown that cyberbullying displays characteristics that distinguish it from traditional bullying, including the potential for the rapid and widespread dissemination of harmful content, the permanence of information in the digital environment, and the increasingly blurred boundaries between school and personal spheres of interaction.

Kowalski, Limber and Agatston (2012) argue that cyberbullying may have particularly severe psychological consequences owing to victims' sense of public exposure and the difficulty of escaping abuse in digital environments. At the European level, Livingstone and Smith (2014) have emphasised the need for education systems to develop comprehensive preventive strategies that combine digital literacy, values education and early institutional intervention.

Within the Spanish educational context, educational legislation and school coexistence policies have progressively incorporated this preventive perspective. The LOMLOE reinforces the educational dimension of school coexistence and highlights the importance of promoting the responsible use of digital technologies throughout the teaching and learning process. Similarly, LOPIVI adopts a comprehensive safeguarding approach that requires schools to establish mechanisms for the early identification of situations involving violence, including those occurring through digital media.

Within this framework, the role of the Well-being and Protection Coordinator assumes particular importance as a key link between the school's preventive actions, the safeguarding of pupils and coordination with other specialised support services. The

Educational Inspectorate likewise plays a significant role in overseeing the effective operation of this position and in evaluating the measures adopted by schools to ensure safe environments in both physical and digital settings.

6. THE ROLE OF THE EDUCATIONAL INSPECTORATE

The Educational Inspectorate plays a pivotal role in safeguarding pupils' right to develop within a safe and respectful educational environment. Its involvement in cases of cyberbullying and other digital risks encompasses two complementary dimensions: first, monitoring compliance with the applicable legal framework, and secondly, providing technical guidance to school leadership teams and the wider educational community.

In exercising its supervisory function, the Educational Inspectorate must examine the sequence of actions undertaken by the school from the moment a potential incident comes to its attention. This assessment includes reviewing whether the appropriate protocol has been activated, evaluating the measures adopted to safeguard the victim, and verifying that the decisions taken comply with the principles of proportionality and legality.

Its advisory function is particularly significant in relation to digital risks, owing to the legal complexity that characterises many of these cases. School leadership teams are frequently required to interpret legislation concerning data protection, the use of mobile devices and the management of digital evidence. In such circumstances, the technical guidance provided by the Educational Inspectorate helps to prevent actions that could inadvertently infringe fundamental rights.

Another important aspect of the Inspectorate's work is institutional mediation. In cases of cyberbullying, relationships between the families involved and the school may deteriorate rapidly, creating tensions that hinder the effective resolution of the conflict.

The intervention of the Educational Inspectorate can facilitate dialogue between the parties and encourage solutions that prioritise the protection and well-being of the child.

Throughout all these activities, the Educational Inspectorate must act in accordance with the principle of the best interests of the child, as recognised both in Spanish legislation and in international child protection instruments. This principle requires that every decision should primarily seek to safeguard pupils' well-being and holistic development, giving preference, wherever possible, to educational and restorative approaches.

6.1. A Proposed Model for Educational Inspectorate Intervention in Cases of Cyberbullying

The Educational Inspectorate's response to incidents of cyberbullying should be guided by the principles of proportionality, child protection and compliance with administrative law. Although each case presents its own particular circumstances, professional experience and the current legal framework make it possible to identify a structured intervention model that supports inspection practice and enhances legal certainty for educational institutions.

The intervention typically begins following notification by the school, a complaint submitted by a family, or information received through other institutional channels. At this initial stage, it is essential to verify whether the school has activated the appropriate intervention protocol and whether immediate safeguarding measures have been implemented to protect the potential victim. The Inspectorate must also ensure that all actions have been properly documented and that the information rights of the families concerned have been respected.

The second stage involves an assessment of the school's response. This includes reviewing the sequence of actions undertaken by the school leadership team,

evaluating the appropriateness of the measures adopted and verifying that the procedures established in the School Coexistence Plan have been correctly implemented. At this stage, particular importance is attached to the assessment of the available evidence, especially digital evidence such as messages, screenshots and content disseminated through social networking platforms.

The intervention subsequently incorporates a technical advisory dimension aimed at both the school leadership team and the teaching staff involved. Such guidance may address issues relating to the interpretation of the applicable legal framework, the protection of personal data, the adoption of interim safeguarding measures, or coordination with other public bodies, including the Spanish Data Protection Agency or the law enforcement authorities where there are indications that a criminal offence may have been committed.

Where the conflict gives rise to significant tensions between families and the school, the Educational Inspectorate may also undertake an institutional mediation role, facilitating dialogue between the parties and helping to steer the dispute towards solutions that place the best interests of the child at the forefront.

Finally, the intervention concludes with an overall assessment of the case and, where appropriate, the formulation of guidance or recommendations designed to improve the management of similar situations in the future. This stage may include proposals for improving the School Coexistence Plan, recommendations regarding staff training, or guidance on updating the school's intervention protocols.

For ease of reference, this intervention process may be summarised in the following stages:

Stage 1. Receipt of Information and Initial Assessment

Verification that the bullying or cyberbullying protocol has been activated and that immediate safeguarding measures have been implemented to protect the pupil concerned.

Stage 2. Review of the School's Response

Assessment of the measures adopted, review of the documentation produced, and evaluation of the appropriateness of the intervention undertaken by the school leadership team.

Stage 3. Technical Guidance for the School

When advising schools on the management of digital evidence, the Educational Inspectorate should emphasise that access to the contents of pupils' personal mobile devices must remain exceptional, properly justified and strictly limited to what is necessary to protect a higher legal interest—namely, the integrity and safety of the victim—while avoiding any disproportionate interference with the child's right to privacy.

Stage 4. Institutional Mediation and Inter-agency Coordination

Facilitating dialogue between the parties involved and coordinating with other competent bodies whenever necessary.

Stage 5. Final Evaluation and Recommendations

Overall assessment of the intervention undertaken and formulation of recommendations aimed at strengthening the school's preventive strategies and intervention protocols.

This proposed intervention model is not intended to replace the procedures established under regional legislation. Rather, it provides a practical framework to support the technical work of the Educational Inspectorate in an area characterised by considerable legal and educational complexity.

6.2. Digital Risks and Educational Inspectorate Response

The following table summarises the most common digital risks encountered in educational settings, the relevant legal framework and the recommended responses for both schools and the Educational Inspectorate. Its purpose is to provide a practical technical reference that facilitates the identification of digital risks and the implementation of safeguarding measures consistent with the principle of the best interests of the child.

The information presented is based on the current legislative framework (LOMLOE, LOPIVI, LOPDGDD and the GDPR), the case law of the Spanish Supreme Court and the Provincial Courts (Supreme Court Judgments Nos. 3639/2020 and 949/2021, and Barcelona Provincial Court Judgment No. 658/2020), together with recommendations issued by specialised bodies such as the Spanish Data Protection Agency (AEPD, 2022) and the scientific literature on cyberbullying and school-based prevention (Del Rey et al., 2019; Kowalski et al., 2012; Livingstone & Smith, 2014).

Table 1. Digital Risks, Applicable Legal Framework and Educational Inspectorate Response

Digital Risk	Legal Basis / Applicable Legislation	Recommended Response by Schools and the Educational Inspectorate
Cyberbullying	Organic Law 8/2021 (LOPIVI); Article 124 LOMLOE	Immediate activation of the relevant protocol; prompt safeguarding of the victim; supervision of the measures adopted; comprehensive documentation of all actions taken.
Non- consensual dissemination of images (Sexting)	Article 84 LOPDGDD; Article 197.7 of the	Notification through the Spanish Data Protection Agency's Priority Channel; preservation of digital evidence; guidance to the school on privacy and proportionality;

	Spanish Criminal Code	notification of families and, where appropriate, the competent authorities.
Online Grooming	Article 183 ter of the Spanish Criminal Code	Immediate referral to the Public Prosecutor's Office and law enforcement authorities; coordination with the relevant authorities and the school; supervision of safeguarding measures and ongoing monitoring of the victim.
Identity Theft or Online Threats	Organic Law 8/2021; Article 124 LOMLOE	Recording and preservation of evidence; assessment of the impact on school coexistence; educational and corrective intervention; technical guidance provided by the Educational Inspectorate.
Exposure to Harmful Content or Online Radicalisation	Organic Law 8/2021; Article 124 LOMLOE; GDPR	Awareness-raising and digital education for pupils; review of digital safeguarding protocols; coordination with families and external authorities where necessary; ongoing monitoring by the Educational Inspectorate.

Source: Author's own elaboration.

The table provides a concise overview of the relationship between each digital risk, its legal basis and the corresponding intervention measures, thereby reinforcing the coherence between prevention, educational response and inspection oversight. Its systematic use contributes to ensuring that educational institutions comply with the required standard of educational due diligence while enabling the Educational Inspectorate to assess the adequacy of institutional interventions, always prioritising the comprehensive protection of pupils.

7. TECHNICAL CRITERIA FOR INTERVENTION IN CASES OF DIGITAL RISK

Institutional responses to incidents of cyberbullying or the unlawful dissemination of digital content require prompt, coordinated and legally sound action. Experience gained from managing such cases demonstrates that the foremost priority must always be to ensure the immediate protection of the victim.

Among the priority measures is the adoption of interim safeguarding arrangements designed to prevent the continuation of abusive behaviour or the further public exposure of the child concerned. Such measures may include temporary changes to class organisation, restrictions on the use of digital devices within the school, or the implementation of educational strategies aimed at restoring a safe and positive school environment.

Another essential aspect is the proper management of digital evidence. Screenshots, messages and shared digital files may constitute important evidence for establishing the facts and should therefore be preserved without altering their content or infringing the fundamental rights of those involved. In handling such evidence, schools must comply with the principle of proportionality, as established by the case law of the Spanish Constitutional Court (Judgment No. 14/2003). Access to the contents of pupils' personal mobile devices should remain an exceptional measure, justified only where strictly necessary to establish the occurrence of the abusive conduct, while avoiding any disproportionate interference with the child's right to privacy that cannot be justified by the protection of a higher legal interest, namely the integrity and safety of the victim.

Communication with families should be conducted transparently and with full respect for their statutory rights to information as the child's legal representatives. Where there are indications that a criminal offence may have been committed, the school should consider referring the matter to the competent authorities in coordination with the Educational Inspectorate.

Institutional intervention may also include cooperation with specialised bodies such as the Spanish Data Protection Agency, particularly where it becomes necessary to request the urgent removal of digital content that infringes the rights of a child.

8. CONCLUSIONS

The expansion of the digital environment has created new challenges for education systems in relation to school coexistence and the protection of pupils. Cyberbullying and the unlawful dissemination of digital content represent forms of violence that require an institutional response founded upon robust legal principles and coordinated action by all relevant stakeholders.

The current legal framework provides adequate instruments for addressing these phenomena. Nevertheless, their effective implementation requires a high level of legal expertise together with a strong awareness of the educational dimensions of these issues. Educational institutions must develop effective preventive strategies and respond diligently whenever situations of risk are identified, ensuring that every measure adopted is appropriately documented.

Within this context, the Educational Inspectorate performs an essential function as both a guarantor of legal compliance and a source of technical support for educational institutions. Its intervention strengthens the legal certainty of institutional decision-making while ensuring that the principle of the best interests of the child remains at the centre of every decision.

The consolidation of an institutional culture committed to safeguarding children within the digital environment represents one of the most significant challenges facing contemporary education systems. Continuous professional development for teachers, the regular revision of school coexistence protocols and effective coordination with specialised agencies constitute essential components in creating safer educational environments that uphold the rights of every member of the school community.

REFERENCES

- Agencia Española de Protección de Datos. (2022). Guía para centros educativos sobre protección de datos personales. AEPD. <https://www.aepd.es>
- Del Rey, R., Ortega-Ruiz, R., & Casas, J. A. (2019). Asegurando la convivencia escolar en la era digital: el ciberacoso como reto educativo. *Revista de Educación*, 385, 59–83. <https://www.educacionyfp.gob.es/revista-de-educacion/numeros-revista-educacion/numeros-anteriores/2019/385/385-3.html>
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley-Blackwell.
- Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://doi.org/10.1111/jcpp.12197>
- Ortega-Ruiz, R., Casas, J. A., & Del Rey, R. (2014). Cyberbullying: The overlap between cyberbullying and traditional bullying. *Psicothema*, 26(4), 417–424. <https://www.psicothema.com/pdf/4213.pdf>
- Sánchez-Valverde, M. (2022). Ciberacoso y educación: Retos para la convivencia escolar en la era digital. Narcea.
- Smith, P. K., del Barrio, C., & Tokunaga, R. (2013). Definitions of bullying and cyberbullying: How useful are the terms? *Educational Psychology Review*, 25, 1–14.
- <https://link.springer.com/article/10.1007/s10648-023-09723-7>

• LEGISLATIVE AND CASE LAW REFERENCES

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation GDPR).
- Organic Law 2/2006 of 3 May on Education (LOE), as amended by Organic Law 3/2020 of 29 December (LOMLOE).
- Organic Law 1/1982 of 5 May on Civil Protection of the Rights to Honour, Personal and Family Privacy, and One's Own Image.

- Organic Law 10/1995 of 23 November approving the Spanish Criminal Code.
- Organic Law 3/2018 of 5 December on Personal Data Protection and the Guarantee of Digital Rights (LOPDGDD).
- Organic Law 8/2021 of 4 June on the Comprehensive Protection of Children and Adolescents against Violence (LOPVI).
- Order of 20 June 2011 regulating measures to promote school coexistence in publicly funded educational institutions in Andalusia and establishing the right of families to participate in the educational process.
- Current Instructions issued by the Directorate-General responsible for School Coexistence within the Regional Ministry of Educational Development and Vocational Training of the Government of Andalusia, establishing the Protocol for Action in Cases of Suspected Bullying and Cyberbullying in Andalusian Educational Institutions. Spanish Constitutional Court Judgment No. 290/2000 of 30 November (recognising the autonomous nature of the fundamental right to personal data protection in relation to the right to one's own image).
- Spanish Constitutional Court Judgment No. 14/2003 of 28 January (establishing the principles of proportionality and necessity in the processing of minors' personal data).
- Spanish Supreme Court Judgment No. 3639/2020 (Administrative Chamber, Fourth Section), 4 November (Appeal No. 6511/2018).
- Spanish Supreme Court Judgment No. 949/2021 (Criminal Chamber), 25 November (Appeal No. 3064/2019).
- Spanish Supreme Court Judgment No. 210/2022 (Criminal Chamber), 9 March (extending criminal protection to the non-consensual dissemination of intimate content through social networking platforms).
- Spanish Supreme Court Judgment No. 4291/2021 (Administrative Chamber), 23 November (Appeal No. 1629/2020).
- Madrid Provincial Court Judgment No. 144/2021 (Fourth Section), 23 March.

- Barcelona Provincial Court Judgment No. 658/2020 (Twelfth Section), 16 December.