Master's in International Security Management

Final Thesis

Cyberbullying of Minors in the European Union: The Digital Services Act and the Challenge of Fragmented National Legal Frameworks

Montana Hill

2025-2026

Table of Contents

Research Question

To what extent do the European Union's Digital Services Act's platform accountability mechanisms, specifically risk assessment obligations and cross-border enforcement coordination, address the governance gap between EU-wide platform regulation and fragmented national cyberbullying frameworks, as evidenced through a comparative analysis of Spain and Germany, and platform compliance reports?

Introduction

The digitalisation of society has rapidly transformed the political, social, and security elements of the European Union. One of the most pressing problems that has arisen from this societal advancement has been the digitalisation of bullying, particularly when it comes to minors. Online harassment of minors, specifically in the form of cyberbullying, has become a substantial security issue within the European Union. The digitalisation of European societies and the extensive use of social media platforms in society itself have created spaces for children to become exposed to harmful online behaviour, making them easy targets for harassment and abuse.

Cyberbullying has been broadly defined by the European Commission as an act of bullying that takes place in online environments such as social media, messaging, and gaming platforms (European Commission, 2025a). This is a security issue that operates beyond borders and, as a result, it is much more difficult to control due to its fragmented nature across different online platforms. Its transnational element makes it both difficult to identify and to control due to the varying definitions across member states of the European Union.

The European Union’s Digital Services Act (DSA) serves as a way to mitigate any issues and discrepancies in the digital landscape by implementing a set of rules and guidelines for all European Union members to follow, with an end goal of creating a digital space that respects humans (European Commission, 2025b). The Digital Services Act represents a huge regulatory advancement in the digital sector, one that could potentially bring about its own set of unique challenges.

This research is relevant to the sector of international security for many reasons. First, cyberbullying towards children is a human security issue, focusing on the individualistic aspect of securitisation and adopting a people-first point of view, acknowledging how the nature of warfare is becoming increasingly more complex. Second, when it comes to security governance, states need to be able to enforce digital laws throughout the European Union that are both coherent with existing institutions and the current rule of law.

Third, the European Union's ability to control and enforce laws in the digital landscape through the Digital Service Act to such a high degree brings into question the sovereignty and

power of certain member states. Fourth and finally, according to Ladani, H. M., M Yogesh, Trivedi, N. S., Gandhi, R. B., & Dhruv Lakkad. (2025), smartphone use and addiction in minors have increased exponentially and are now a rising public health concern, with smartphone use being at 89% and addiction at a high of 64%. This, paired with the severity of cyberbullying, makes this a top securitisation issue in many fields.

This research examines whether the differences in legal frameworks towards cyberbullying across the nations of the European Union serve as a barrier to solving the issue.
and questions whether the European Digital Service Act properly addresses challenges. It defines the differing definitions of cyber-bullying across member states and analyses how these definitions of cyberbullying affect the European Union's ability to regulate said issues and protect minors. In order to examine this, the research is focused on comparing the EU member states Spain and Germany, which both operate under civil law practices, but have generated different responses to the protection of minors online, making the Digital Service Act a key variable of comparison.

The purpose of this research is to progress the academic understanding of the European Union's agenda and its role in digital securitisation. It will explain whether the Digital Services Act is positively useful when it comes to preventing cyberbullying towards minors or if it acts as a hindrance due to member states' ability to harmonise on its definition.

This research asks the following question: To what extent does the European Union’s Digital Services Act mitigate the challenges created by fragmented national legal frameworks in the cross-border enforcement of cyberbullying cases involving minors within the European Union?

Cyberbullying, in general, is an international and digital security issue. It functions transnationally, operating across borders, and is heavily reliant on digital platforms. It is a security issue that is a serious challenge to both the authority of the state and its capacity. The perpetrators of cyberbullying operate throughout the European Union, making any enforcement measures against it extremely difficult due to state jurisdiction and national laws. The Digital Services Act serves as a potential solution to this problem, tackling the fragmentation of national legal frameworks and trying to build a more secure digital space for minors.

This research focuses on this concrete and growing security issue in the European Union. Cyberbullying towards minors, specifically, is a growing and complex issue that is affecting Europe. According to Wright (2016), cyberbullying is an event that involves multiple factors. Meaning it is not only online, but it is a combination of the digital space along with various environments that include family, schools, and legal systems. Minors are accessing the internet at younger ages every year, exposing them to even higher risks of online bullying and victimisation (Wright, 2016).

This perspective is directly relevant to my research as it brings into question the legal systems, along with other factors, that allow cyberbullying towards minors to occur. Varying definitions of what constitutes cyberbullying, differing methods of law enforcement, and varied institutional authority all act as barriers to solving the issue at hand. This research examines whether the Digital Service Act reduces the barriers and examines the legal environment created by European Union rules toward online bullying of minors.

Literature Review

In order to differentiate cyberbullying from traditional bullying, bullying is defined as

> *"any unwanted aggressive behaviour (s) by another youth or group of youths, who are not siblings or current dating partners. It involves an observed or perceived power imbalance and is repeated multiple times or is highly likely to be repeated. Bullying may inflict harm or distress on the victim, including physical, psychological, social, or educational harm." (CDC, 2024)*

Cyberbullying is defined as

> *"bullying that takes place using digital devices such as cell/mobile phones, computers, and tablets. Cyberbullying can occur through SMS, e-mail, apps, social media, forums, or gaming when people view, participate in, or share content. Cyberbullying includes the deliberate sending, posting, or sharing of negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else, causing embarrassment or humiliation." (United Nations Office for Disaster Risk Reduction (UNDRR), & International Science Council (ISC), 2025)*

A more precise definition of cyberbullying is given by Smith et al. (2008, p. 376), pointing out that it is *"an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time, against a victim who cannot easily defend him or herself.*"

In comparison to normal bullying, cyberbullying differs because it has the ability to progress over longer periods of time. Normal bullying for a minor at school, for example, ends at the end of the day when they leave. Cyberbullying continues for as long as the perpetrator desires it to. This is because many children are constantly on their electronic devices and are continuously connected to the internet.

When it comes to the power imbalance in cyberbullying, it is just as present, if not more, in comparison to traditional bullying. A key concept here is recognising the anonymity factor, which creates an even larger power balance because the victim isn't even aware of who is bullying them (Vandebosch, H., & Van Cleemput, K., 2008). This can take an even greater psychological toll on a minor, completely removing their ability to defend themselves.

The World Health Organisation reported that 1 in 6 children/adolescents in the European Union have been bullied online, with 1 in 8 admitting to participation in online bullying (Better Internet for Kids, 2026). Cyberbullying has been the top reason for people calling the European “Safer Internet Centre” helplines, roughly around 15% of the total calls received by the helpline (Better Internet for Kids, 2026). It is worth noting that cyberbullying is increasingly becoming a human security issue, demonstrating a change towards a security dimension focused more on the people, acknowledging the change in security in the digital age (NATO, 2024).

Victims of cyberbullying don’t tend to report the abuse, and as a result, feel completely isolated and powerless (Murphy, 2024). In extreme cases, many victims use substances, self-harm, and suicidal ideation to cope with the bullying, many instances resulting in suicide (Murphy, 2024). Knowing this information, we can recognize the possibility that cyberbullying is a much more extreme and exhausting form of bullying due to the fact that victims cannot escape it.

In the European Union, only thirteen member states have a legal definition for cyberbullying, and these definitions tend to be heavily reliant on general laws involving harassment, hate speech, and defamation (Joint Research Centre (JRC), & European Commission, 2024).
The difference between regulations in Spain and Germany easily demonstrates how differently countries approach this issue. Spain has relied on its Penal Code and a law passed in 2021, the Ley Organica 8/2021. This established general protections for children, but never put into place any regulations to hold online platforms accountable and/or regulate them (Jefatura del Estado, 2021; Mind the Challenge, 2022). The Spanish approach has been heavily criticised by legal experts, stating that it is extremely vague. Specifically, by Rodolfo Tesone, lawyer who specialises in digital transformation issues, worries that because Spain doesnt hold these private companies accountable, and that by not doing so, it “opens up the debate on freedom of expression versus filtering/censorship, although it is not up to these platforms – private companies – to defend or limit citizens’ liberties” (Mind the Challenge, 2022).

Spain has started working towards resolving these issues, and in June of 2024, a draft of Organic Law for the Protection of Minors in Digital Environments was approved by the Council of Ministers (Osborne Clarke, 2025; European Audiovisual Observatory, 2024). This proposal would raise the age of consent for processing online data from 14 to 16 years old, and it would also include age verification and even sanctions that would prevent convicted criminals from accessing digital spaces where they committed any offence (Osborne Clarke, 2025;European Audiovisual Observatory, 2024). In March of 2025, this draft was approved in a second round by the Council of Ministers, demonstrating strong improvements in legislation compared to the 2021 framework (Osborne Clarke, 2025).

Germany has a different regulatory route compared to Spain, placing more of the burden on the platforms. Germany’s Network Enforcement Act (NetzDG) was enacted in 2017, and

forced social media platforms to monitor and take down illegal content within a certain amount of time (Bundesministerium der Justiz, 2017). When the European Union's Digital Service Act became applicable in 2024, the Network Enforcement Act was repealed due to the European Union replacing it under its country-of-origin principle (Hogan Lovells, 2023). As a result of this action, Germany proposed two new pieces of legislation; one is a law on digital violence, which would allow victims to have stronger legal rights, and it would also require digital platforms to have a German representative (Hogan Lovells, 2023). However, it is not clear yet how this will work alongside the Digital Service Act and European Union rules. The other piece of legislation, which is an amendment to the Interstate Treaty on the Protection of Minors in the Media (JMStV), would change and/or adjust a current set of rules between Germany and regional states when it comes to the protection of children from harmful media (Hogan Lovells, 2023). These changes were finalised in December of 2025 and placed new responsibilities on the operating system providers. The European Commission questions whether they conflict with existing EU law, and some even challenge in courts in Germany (Freshfields, 2025). Germany's political parties have also proposed social media bans on children under 14 years old. Legal experts said that national measures of this kind are blocked by the Digital Service Act's harmonisation framework (Health Policy Watch, 2026).

The difference between Germany and Spain when it comes to this issue is that Germany is more focused on the regulation of online platforms, whereas Spain is more focused on its actual criminal law, putting its focus above the responsibility of the platforms. This reveals a fundamental structural difference between the two states. Although it seems like both Spain and Germany are on the right track, there are still significant gaps when it comes to cyberbullying targeting children, with both countries being pressured to meet the European Union's rules and regulations.

Spain and Germany do have different laws; however, what needs to be pointed out here is that the problem is not simply due to this fact, but also serves as an example of what happens when member states have to fill the gap created by the European Union on their own. Yes, the Digital Services Act does regulate online platforms; however, it fails to define the act and to take action to actually solve the problem of cyberbullying. Each country chose its own method of dealing with the problem at hand. Spain had its criminal law, and Germany turned to regulating the platforms. Neither approach taken by these states fully fits the gap left by the Digital Services Act, and under the country-of-origin principle, neither state can go further on their own.

Germany's Network Enforcement Act previously was the top enforcement measure towards online platforms within the European Union, and it was repealed when the Digital Services Act came into effect (Hogan Lovells, 2023). Spain's Ley Organica 8/2021 places no accountability on online platforms. These two facts demonstrate how there is no harmonisation and how the Digital Services Act creates a hole where a shared definition of cyberbullying is needed.

The lack of harmonisation can also be seen when states act alone when faced with challenges in this area. When Germany tried to adapt their Interstate Treaty on the Protection of Minors in the Media (JMStV) by proposing banning social media for those under 14 years of age, and Spain also tried to restrict access to those under 16, the European Commission questioned these actions (Freshfields, 2025; Health Policy Watch, 2026; NicFac, 2025). Actions like these, which are simply member states trying to regain control that the Digital Services Act gave to the European Union Level. The European Commission's questioning demonstrates how tense it is on the level of national sovereignty and the practice of state coordination. Another key point is also reflected here; the European Union is not a single organised unit, and its digital rules are crafted and applied based on the legal/political context of each state (Orland-Salling, 2025).

Another example of differing measuring in EU member states includes France and Poland. In France, cyberbullying is specifically defined in the Criminal Code as:

> *The fact of harassing a person by repeated comments or behavior with the purpose or effect of degrading his or her living conditions resulting in an alteration of his or her physical or mental health is punishable by one year's imprisonment and a fine of €15,000 when these acts have resulted in a total work incapacity of less than or equivalent to eight days or have not led to any work incapacity. (Criminal Code, Article 222-33-2-2, as cited in Xu, Y., & Trzaskawka, P., 2021).*

Whereas Poland's laws are more vague and are related to the state's general stalking laws, with no specifications toward minors (Xu, Y., & Trzaskawka, P., 2021). Cyberbullying is a rising issue, as in 2024, 14 per cent of the 54,000 phone calls that the Safer Internet Centre helplines located across Europe received involved online bullying cases (Joint Research Centre (JRC), & European Commission, 2024).

In the European Union, all 27 member states have set legislation that fights against cyberbullying (Joint Research Centre (JRC), & European Commission, 2024). However, only 8 states have an official definition for what constitutes cyberbullying, and these definitions mainly take into account adult experiences, not minors. These states include Denmark, France, Greece, Italy, Lithuania, Malta, Romania, and Spain (Joint Research Centre (JRC), & European Commission, 2024). According to the Joint Research Centre of the European Commission (2024), in states that don't have an official definition, cyberbullying is addressed in conjunction with criminal and civil law. This obligates cyberbullying to only be serious when it is related to instances of crime, such as threats, defamation, hate speech, and/or harassment.

Although this may seem like progress, most member states do not have any data collection practices when it comes to cyberbullying. Meaning, cyberbullying is difficult to measure, compare, and regulate across the EU, with results being incomparable also due to the fact that there is no shared definition (Joint Research Centre (JRC), & European Commission, 2024). In Europe alone, half of the population of children report having experienced cyberbullying

(UNESCO,2021). Experts within the EU are in support of setting a definition for cyberbullying in order to tackle it at an efficient level.

The Digital Services Act, as defined by the European Union (2024), *"introduces rules for online services used by European citizens in their everyday life. These services include marketplaces, social media networks, app stores, and online travel and accommodation platforms."* It aims to have one unified framework replace 27 regulations in the European Union (European Union, 2024). The Digital Services Act pushes for more protection for minors, requiring them to verify their age and also requiring platforms to implement protection measures, putting forward a "best interest of the child" principle (European Commission, 2024, February 6). This principle originated in international law. Article 3 of the United Nations Convention on the Rights of the Child (1989) states that:

> *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." (United Nations, 1989, Article 3)*.

Meaning that platforms need to ensure that minors are safe from online harassment, bullying, false information, and illegal content when using these platforms (European Commission, 2024, February 6)

The European Union's Digital Services Act has been its strongest attempt at creating a single set of rules/laws for online platforms to follow that goes across all member states. Instead of having 27 different systems, the Digital Services Act establishes one singular framework for all online platforms to follow across all 27 states, no matter whether the company is based inside of Europe (European Union, 2024). For the purpose of this research, I take into account Articles 14, 16, 26, 28, 34 and 38. Both articles 14 and 16 focus on how online platforms are required to handle and report harmful online content. Article 26 has to do with banning advertising content that is geared towards children. Article 28 determines specific protections for minors. Article 34 requires the largest of the online platforms to assess the risk that they pose. Finally, Article 38 would require them to ask about any said risk that they pose. The Digital Services Act prevents online platforms from using the data they've acquired from children to create targeted ads, it also requires online platforms to include terms and conditions that are appropriate for children, and it especially requires platforms with more than 45 million monthly users in the European Union to conduct formal assessments of the risk that their digital platforms pose to children (European Parliamentary Research Service, 2021).

The European Commission wrote and published guidance on how Article 28, specifically, should be practised. These guidelines are built upon 5 specific categories of risk: content, contact, conduct, consumer, and cross-cutting risks. This guidance also lists a number of measures recommended by the European Commission. measures such as age verification, tools that would allow children to prohibit users from contacting them, prevent them from

being added to online groups, and better online reporting systems. It also includes disabling addictive features of these online platforms, such as the infinite scroll, autoplay, and streaks (European Commission, 2025c; Hogan Lovells, 2025). Online platforms should routinely review how children use their online platforms and also check whether their safety features are working (NicFab, 2025). The European Commission has made it explicitly clear that these guidelines will be the standard when it comes to these online platforms providing their services to children, and will especially be taken into account when the European Commission assesses these online Platforms in order to decide whether they are meeting their obligations under Article 28. This has already been taken into effect, and since 2025, 19 legal proceedings have been launched, and most of them involved failures to protect minors (Centre for Future Generations, 2025).

Without a proper consensus among member states, the right strategies and measurements cannot be developed to tackle online abuse towards minors (Joint Research Centre (JRC), & European Commission, 2024). Due to the fact that the Digital Services Act wants to create a single set of rules across the European Union, this creates a problem for the European Union member states that may want to do more when it comes to protecting children on online platforms. The European Union operates under a country of origin principle, this would mean that online platforms would be regulated according to the country where they are based, not according to every single country where their services are being used.

This means that Germany, Spain or any of the 27 other member states cannot add extra rules on the usage of these online platforms due to the fact that they are headquartered in another European Union country. This would only be allowed if specific conditions under European Union law are met (Health Policy Watch, 2026; Freshfield, 2025). Stefan Dreyer, who is a media law expert, states that the Digital Services Act takes all issues into account and that there is no space for individual states with their own national laws to achieve similar goals that are already addressed, using different means. Due to this fact, it is difficult to have children banned from using social media without strong action from a European Union level (Health Policy Watch, 2026).

This issue is clearly demonstrated between the countries that are examined in this research, Germany and Spain. As mentioned previously, Germany's changes in December of 2025 to its Treaty on the Protection of Minors in the Media were heavily criticised by the European Commission over whether it was compatible with both the European Union law. Germany's proposed ban on social media for children under 14 years old is also questioned as it's seen as unenforceable under the current European Union framework (Freshfields,2025; Health Policy Watch, 2026). Spain, also trying to restrict social media for children under 16 years old, faces similar legal difficulties, even being one of the five countries leading the European Commission's age verification plan, demonstrating how the European Union prefers coordinated efforts over states standing and acting alone (NicFab,2025). This fact is important to this research. The Digital Services Act may stop member states from acting on the gaps it fails to address, especially when it comes to cyberbullying of minors, since the

Digital Services Act mainly addresses online platform behaviour rather than legally defining cyberbullying.

There are several gaps within the Digital Services Act. When it comes to handling cross-border cases of cyberbullying towards minors, the current level of the framework is weak. The Digital Services Act, for example, puts the responsibility of enforcement for the largest online platforms at the level of the European Union, and it puts the responsibility of enforcement for the smallest online platforms at each country's Digital Services Coordinator. This was set up to tackle systemic risks; it did not take into account cyberbullying involving children in different member states (European Parliamentary Research Service, 2021). A system for shared reporting, tackling and coordination between European Union member states does not exist. Due to this, jurisdiction is more often than not unclear and complicated. For example, a cyberbullying incident involving a child in Spain being bullied by someone in Germany on an online platform in Ireland could potentially fall under three different legal systems at the same time. Making it extremely complicated since none of them has a clear shared definition of what constitutes cyberbullying to begin with.

In response to similar issues, the European Commission created a European Union Action Plan against Cyberbullying in 2025 after quite a few public discussions (European Commission, 2025a). This action plan would involve the application of laws that already exist in a more effective manner and focus more on cyberbullying (European Commission, 2025a). It also involved encouraging other member states to enforce policies on a national level that were based on a shared understanding of the issue (European Commission, 2025a). Finally, advocating responsible behaviour on these digital platforms from a young age (European Commission, 2025a). Although this may seem like a step in the right direction, it also involves the European Union being heavily reliant on the agreement of its member states to enforce these common definitions, highlighting the limited framework and how much work needs to be done. The Joint Research Centre has commented that without a shared definition of what constitutes cyberbullying, it cannot be addressed and/or regulated throughout the European Union (JRC & European Commission, 2024).

Theoretical and Analytical Framework

This research is dependent on multi-level governance. It provides a certain viewpoint and correct method of analysing a problem that occurs throughout the member states of the European Union and the private platforms discussed above, where the bullying occurs. Multi-level governance involves a system that spreads authority throughout different levels instead of the sovereign state (Hooghe and Marks, 2003). The concept of multi-level governance was initially used to describe the European Union's levels of operation, since it operates on a level that involves both the European Union itself and its member states (Hooghe and Marks, 2001). This research brings a third level to the idea of multi-level governance, that level being the online platforms such as Meta, TikTok, and YouTube. These

platforms operate on their own levels of power. Since they themselves decide how their content is managed and the process of age verification, along with how each individual risk is measured and dealt with. The Digital Services Act operates similarly and allows the European Union to have control of these online platforms at the same operational level. Although it seems functional, the laws that actually protect minors remain dependent on the state. This research argues that the issues that come with the cyberbullying of minors fall within the gaps that the Digital Services Act fails to address, and these gaps cannot be closed with the Digital Services Act alone.

This research paper touches on four central concepts that each play a part within the framework.

The first concept is securitisation, one that easily explains how cyberbullying turned into a problem that is treated as a security issue by states (Wæver,1995). The fact that the European Commission states that cyberbullying poses a large risk and then went on to create an Action plan against it in 2025 demonstrates that it is a serious security issue, so serious that the European Union as a whole needs to take action.

The second concept is human security, which analyses human safety above the safety of the state (UNDP, 1994; NATO, 2024). Human security explains why cyberbullying is a security issue since it is focused on the human aspect: protecting the child, explaining the reasoning behind why it matters. Multi-level governance, on the other hand, demonstrates/explains how the system that is meant to deal with the issue actually works. The United Nations Development Programme (1994, p. 23) describes it as *"safety from such chronic threats as hunger, disease and repression … protection from sudden and hurtful disruptions in the patterns of daily life — whether in homes, in jobs or in communities."* (UNDP, 1994, p. 23)

Sovereignty is the third concept, which is where the majority of tension lies. The Digital Services Act uses the country-of-origin principle, taking a large sum of power away from the individual states of the European Union, creating issues between member states when a state tackles an issue that oversteps shared rules. The European Commission questioned Germany’s changes to the States Treaty on the Protection of Minors in the Media, and Spain and Germany's desire to limit social media for minors, demonstrating the tensions between the European Union and its individual member states when it comes to harmonisation when tackling these issues.

The final concept is fragmentation, which explains what is going wrong at a national level. Fragmentation itself is not a separate issue; it is the byproduct of laws not being successfully merged. We can see it in the differing national definitions of cyberbullying throughout the member states, the lack of shared data, and the large absence of a shared system put in place to handle cross-border cases of cyberbullying. We see how limited the power of the European Union is when we recognise how fragmentation continues to be an issue, even though the Digital Services Act has been put into place.

The four central concepts come together to create the main idea that this research challenges: Although the Digital Services Act creates a controlled centre for the online platforms at the European Union level, the core definition and the protection of minors are dependent at the state level, leaving cyberbullying to fall between the gaps. The question the empirical analysis aims at is whether the Digital Services Act risk assessment and cross-border measures are enough to close the gap, or whether an agreed-upon shared definition, a working system for cross-border cases of cyberbullying and cyberbullying itself being its own category is what is needed.

Methodology

Analytical Framework

This research questions whether the European Union's Digital Services Act addresses and solves cyberbullying issues as a result of fragmented national frameworks towards minors. To be able to answer this question in my research, I will define key concepts and my observations. This section outlines concepts, variables, and indicators suitable for the analysis of the research question.

Concept 1: Cyberbullying involving Minors

The first concept is cyberbullying involving minors. In this study, and as previously mentioned, cyberbullying is defined as *"bullying that takes place using digital devices such as cell/mobile phones, computers, and tablets…It can include sharing personal or private information about someone else, causing embarrassment or humiliation." (United Nations Office for Disaster Risk Reduction (UNDRR), & International Science Council (ISC), 2025)*. Cyberbullying is the core security issue in this study. The variable connected to this concept is its legal definition, which differs and/or is nonexistent throughout member states. This research will assess the following variables: whether the legal definitions of cyberbullying within the national criminal codes of Spain and Germany cater towards minors; whether that definition includes online conduct; and whether online platforms are legally obliged to act on cases of cyberbullying towards minors. The results will demonstrate whether the state's legal constructs are effective in bridging the gap between current regulations and the EU Digital Services Act. This research will also account for recent legislative advancements in Spain and Germany. This includes Spain's Organic Law on Digital Environments from 2025 and Germany's amendments on the Interstate Treaty on the Protection of Minors in the Media

(JMStV) from December of 2025, both representing European Union states attempting to address and fix gaps in the Digital Services Act.

Concept 2: Fragmentation of National Legal Frameworks

The second concept in this research is the fragmentation of national legal frameworks. Fragmentation in this sense refers to differing definitions, rules, and institutional regulations of cyberbullying throughout the member states of the European Union. Ultimately, fragmentation in this sense acts as an impediment to legal systems. Disrupting their functions and the success of their operations. A variable connected to this concept is the scale of legal divergence between Spain and Germany. This research will assess this variable by determining whether each state has a legal definition of cyberbullying, how each state classifies cyberbullying, how each state addresses cyberbullying and how recent reforms in the legislature in each state interfere with the Digital Services Act.

Concept 3: Cross-border Enforcement

The third concept in this research is cross-border enforcement. This will address whether and how cases involving cyberbullying towards minors are handled when different European Union states are involved. A variable connected to this concept is state coordination. This research will assess this variable by examining the security measures taken by states in these situations. It will also take into account how states work together and the clarity of jurisdiction in cross-border situations. The results will indicate whether enforcement measures and the current systems put into place are functional when dealing with cross-border issues. This research will also examine whether the European Commission's 2025 Action Plan against Cyberbullying is a potential method for coordination, and whether its dependence on member states is enough to close gaps.

Concept 4: Digital Services Act Regulation and Cyberbullying of Minors

The fourth and final concept is the European Union's regulation of cyberbullying towards minors through the Digital Services Act. The variable connected to this concept is aligned governance of cyberbullying towards minors throughout the European Union. This research will assess how this variable correlates to digital regulations under the Digital Services Act and whether they are effective through their coordinators, requirements, and cooperation measures taken between states. It will assess whether the Digital Services Act uniformisation, which includes the country-of-origin principle, acts as a limitation on member states' ability to address cyberbullying at an independent level.

These concepts, variables, and indicators will create a clear picture of how to assess whether the European Union's Digital Service Act addresses fragmented national frameworks relating to cyberbullying of minors. It will also determine whether it improves cross-border enforcement of cyberbullying of minors throughout the European Union while preventing tension between member states. This research will directly determine whether it is possible for the Digital Services Act to serve as an improvement to cross-border enforcement between member states and whether coordination between these states can be achieved without eroding the significance of state sovereignty.

Research Design

This research uses a qualitative research approach to determine to what extent the European Union's Digital Services Act mitigates the challenges created by fragmented national legal frameworks in the cross-border enforcement of cyberbullying cases involving minors within the European Union. Fragmentation of this nature results in delayed legal action and weak protection for minors, as states have to deal with differing concepts and regulations. In this research, the focus is on the European Union's regulations and enforcement practices along with its institutional operations, and not on numerical data. A qualitative research approach allows me to dissect legal works, policy, and enforcement forms in a detailed manner.

The documents inspected in this research include three levels of governance. At the level of the European Union, the Digital Services Act, this research focuses on Articles 14, 16, 26, 34, and 38, along with their supporting documents. At a national level, this research focuses on Germany's NetzDG 2017 and Spain's Ley Orgánica 8/2021 and the Spanish Penal Code. At a digital level, this research also analyses the Digital Services Act's transparency reports and the Article 34 risk assessments that are submitted by Meta, TikTok, and YouTube.

This research compares the definitions and approaches of the regulation of cyberbullying of minors taken by member states to strengthen the analysis. A qualitative approach helps in the identification of similarities and disparities in policy between member states, allowing me to determine whether the Digital Services Act would be a benefit to European society by solving potential gaps in its legal application.

A comparative approach is necessary due to the fact that cyberbullying of minors can often cross borders and involve more than one state. Since every state handles these situations differently, it is important that I am able to recognise gaps in the law. This research examines whether there are underlying gaps and inconsistencies and shines a light on how the Digital Services Act can improve enforcement. With a qualitative study, I am able to read and interpret legal texts while also being able to interpret nuances in the texts, which a quantitative analysis will not allow for. This method allows me to have a clear view of the situation at hand and to understand any intricacies that are present.

Empirical Analysis

Spain

As mentioned previously, Spain relies on its Ley Organica 8/2021 as an approach to cyberbullying of minors instead of the regulation of online platforms. The Ley Organica 8/2021 broadly defines what constitutes violence under Article 1, including acts that were carried out through information/communication technologies (Ministerio de Juventud e Infancia, 2021). Title III Chapter VIII of the Ley Organica 8/2021 supports the collaboration of public and private bodies when it comes to collaborating to ensure minors are safe on the internet, even recommending systems that rate by age under Article 46; nothing is imposed (Mind the Challenge, 2022).

When the four analytical concepts listed above are applied to this research, gaps are revealed. Spain does not have one strong and singular definition of what constitutes cyberbullying; it is simply assumed under a broad definition, and action can only be taken when a specific threshold is met, such as defamation and/or harassment. The online platforms themselves face no legal duty to monitor, enforce, or even act on cases of cyberbullying. Also, Spain's Ley Organica 8/2021 does not apply to cross-border situations of cyberbullying of minors.

Germany

Germany's 2017 Network Enforcement Act (NetzDG) obligated online platforms that had above two million German users to remove illegal content within a 24-hour timeframe after a complaint was made, and to also publish transparency reports every 6 months (Bundesministerium der Justiz, 2017). On a European Union Level, the NetzDG was the most active enforcement measure towards online platforms. By mid 2023, X received over 1.1 million complaints from NetzDG, TikTok received 202,747 complaints, and YouTube received 193,131 complaints (Jackson School of International Studies, 2024). However, NetzDG only designated illegal content based on what was already determined illegal by German law. NetzDG did not include anything specific to cyberbullying, nor did it include any cross-border enforcement measures (Bundesministerium der Justiz, 2017). It was determined by the BIK Policy Monitor (2025) that Germany has made no advancements towards addressing cyberbullying. An HBSC study done in 2022 of 6,475 German students found an increase in cyberbullying from the year 2017 up until 2022, a timeframe that includes the enforcement of the NetzDG (Robert Koch Institute, 2024).

A 2025 Digital Services Act assessment on TikTok and Meta under Article 34 determined minor protection measures to include parental controls, notification limits and screen-time tools (Knight-Georgetown Institute, 2026). Unfortunately, the reports do not include proof that these preventative measures work. Internal documents from a United States legal proceeding determined that more than 90% of TikTok users ignored their reminders to take a break from the app (Knight-Georgetown Institute, 2026), suggesting a massive gap between compliance and effectiveness. None of the platforms identifies cyberbullying as its own category. The Digital Services Act does not provide a core definition of cyberbullying, a reporting system, or a process for handling cross-border situations.

Conclusion

This research explored to what extent do the European Union's Digital Services Act's platform accountability mechanisms, specifically risk assessment obligations and cross-border enforcement coordination, address the governance gap between EU-wide platform regulation and fragmented national cyberbullying frameworks, as evidenced through a comparative analysis of Spain and Germany, and platform compliance reports. The findings of this research suggest that while the Digital Services Act improves some aspects of online platform regulation, it does not solve the governance issues that are at the centre of the issue.

The multi-level governance lens allows us to point out the gaps easily. The Digital Services Act gives more authority to the European Union over online platforms. The Digital Services Act determines what rules TikTok, Meta and YouTube need to follow; however, the definition of what constitutes cyberbullying and core protection of minors still remains at a national level. Cyberbullying of minors, specifically, falls between these two factors, which is why regulating the platforms alone will not suffice.

The research compared European Union member states Spain and Germany, which demonstrated that the issue at hand is not that different countries have different laws, but that they take different approaches to the regulation. Spain has chosen to rely on criminal law to charge, while Germany has relied on regulating private companies. Neither country has a shared definition of what constitutes cyberbullying towards minors; effectively, neither of them has a proactive system set into place to manage this issue. Even though both countries are taking measures to bridge any gaps, it is limited due to the Digital Services Act’s coordination framework.

The risk assessment rules in Article 34 of the Digital Services Act and the 2025 Guidelines on the Protection of Minors are steps in the right direction. It is proof that the European Union recognises the gaps in the Digital Services Act and is taking measures to close said gaps, and that it is taking online harm more seriously. However, as mentioned above, the

compliance reports from Meta, TikTok, and YouTube show that these measures still do not fully solve the problem at hand. Cyberbullying is more often a personal and targeted attack, and the Digital Services Act was created to regulate online platforms at a broad level. In direct answer to the research question, the Digital Services Act's platform only addresses the gap at a partial level. This includes its risk assessment procedures and cross-border enforcement measures. They serve to coordinate how online platforms operate, but they do not address the core issue, which is the fragmented national definitions and having no shared system when it comes to cross-border coordination, where cyberbullying of minors is actually concerned.

In order to close these gaps, the European Union needs to do three things. First, the European Union needs to agree on one singular definition of what constitutes cyberbullying and have it include minors. Second, cyberbullying should have its own category of harm in the Digital Services Act. Third and final, coordinators of the Digital Services Act should have a system set in place for dealing with cross-border cases of cyberbullying involving minors.

By using the multi-governance lens to look at the issue of cyberbullying, this research adds to our knowledge of how the European Union tackles the problem of online bullying. This research shows that although there are rules implemented towards these online platforms across the European Union, this does not solve the problem at hand. There are limits to this research. This research is a qualitative study that solely compares Spain and Germany, meaning that the findings of this research cannot speak for every member state of the European Union.

Protecting minors from cyberbullying can only work if the European Union closes the gaps created by the Digital Services Act. This would involve agreeing on one core definition of what constitutes as cyberbullying throughout all member states, creating a category for this issue alone, and establishing a system to deal with cases of cyberbullying that involves multiple states. Until these things happen, the Digital Services Act, while remaining a strong tool for regulating online platforms, will fall short when it comes to protecting minors from cyberbullying.

References

Bauman, S., Cross, D., & Walker, J. L. (2013). *Principles of cyberbullying research: Definitions, measures, and methodology*. Routledge.

Better Internet for Kids. (2026). *Cyberbullying in the EU member states*. https://better-internet-for-kids.europa.eu/en/news/cyberbullying-eu-member-states

BIK Policy Monitor. (2025). *Germany country profile*. https://better-internet-for-kids.europa.eu/en/knowledge-hub/germany-policy-monitor-country-profile

Bundesministerium der Justiz. (2017). *Netzwerkdurchsetzungsgesetz (NetzDG) — Act to improve enforcement of the law in social networks (Network Enforcement Act)*. BGBl. I S. 3352. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

Cachia, R., Villar Onrubia, D., Barreda Angeles, M., Economou, A., & Lopez Cobo, M. (2025). *Cyberbullying: Considerations towards a common definition*. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC143340

Centers for Disease Control and Prevention. (2024). *About bullying*. https://www.cdc.gov/youth-violence/about/about-bullying.html

Centre for Future Generations. (2025). *Enforcement spotlight — Autumn 2025*. https://cfg.eu/enforcement-spotlight-autumn-2025/

European Commission. (2024, February 6). *The Digital Services Act (DSA) explained: Measures to protect children and young people online*. https://digital-strategy.ec.europa.eu/en/library/digital-services-act-dsa-explained-measures-protect-children-and-young-people-online

European Commission. (2025a). *Cyberbullying – protecting children online*. https://digital-strategy.ec.europa.eu/en/policies/cyberbullying

European Commission. (2025b). *The Digital Services Act*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

European Commission. (2025c). *Guidelines on the protection of minors under the DSA*. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors

European Parliamentary Research Service. (2021). *Digital Services Act* [Briefing]. European Parliament.

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf

European Union. (2024). *The Digital Services Act*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

Fair Patterns. (2025). *TikTok's algorithm crisis, EU's minor protection push*. https://www.fairpatterns.com/post/tiktoks-algorithm-crisis-eus-minor-protection-push

Freshfields. (2025). *Germany adopts new youth protection obligations for operating system providers*. Technology Quotient. https://technologyquotient.freshfields.com/post/102lwz8/

Health Policy Watch. (2026). *German parties back social media ban for minors, legal hurdles loom*. https://healthpolicy-watch.news/german-parties-align-on-social-media-ban/

Hogan Lovells. (2023). *Online regulation: Germany's plans to tackle "digital violence."* https://www.hoganlovells.com/en/publications/online-regulation-germanys-plans-to-tackle-digital-violence-and-likely-other-issues-too

Hogan Lovells. (2025). *The long-awaited EU guidelines on Article 28(1) DSA: What online platforms must know*. https://www.hoganlovells.com/en/publications/the-longawaited-eu-guidelines-on-article-281-dsa-what-online-platforms-must-know

Hooghe, L., & Marks, G. (2001). Types of multi-level governance. *European Integration online Papers (EIoP), 5*(11). https://eiop.or.at/eiop/pdf/2001-011.pdf

Hooghe, L., & Marks, G. (2003). Unravelling the central state, but how? Types of multi-level governance. *American Political Science Review, 97*(2), 233–243. https://garymarks.web.unc.edu/wp-content/uploads/sites/13018/2016/09/hooghe.marks_.unravelingcentralstate.apsr_.2003.pdf

Jackson School of International Studies. (2024). *German content moderation and platform liability policies*. University of Washington. https://jsis.washington.edu/news/german-content-moderation-and-platform-liability-policies/

Jefatura del Estado. (2021). *Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia*. Boletín Oficial del Estado, núm. 134. https://www.boe.es/eli/es/lo/2021/06/04/8

Joint Research Centre & European Commission. (2024). *Cyberbullying on the rise: The benefits of a common definition*. https://better-internet-for-kids.europa.eu/en/news/cyberbullying-common-definition-jrc

Knight-Georgetown Institute. (2026). *What US lawsuits reveal about platform design that DSA reports don't*.

https://kgi.georgetown.edu/research-and-commentary/what-us-lawsuits-reveal-about-platform-design-that-dsa-reports-dont/

Ladani, H. M., Yogesh, M., Trivedi, N. S., Gandhi, R. B., & Lakkad, D. (2025). Exploring smartphone utilisation patterns, addiction, and associated factors in school-going adolescents: A mixed-method study. *Journal of Family Medicine and Primary Care, 14*(1), 334–340. https://doi.org/10.4103/jfmpc.jfmpc_1308_24

Mind the Challenge. (2022). *Legislation on minors in the digital sphere*. https://mindthechallenge.com/en/legislation-on-minors-in-the-digital-sphere/

Ministerio de Juventud e Infancia. (2021). *Violence against children and adolescents*. https://www.juventudeinfancia.gob.es/en/childhood/violencia-contra-la-infancia-y-la-adolescencia

Murphy, C. (2024). *Cyberbullying among young people: Laws and policies in selected Member States*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI%282024%29762331_EN.pdf

NicFab. (2025). *Safer Internet Forum 2025 and the comprehensive EU framework for child online protection*. https://www.nicfab.eu/en/posts/eu-child-online-protection/

North Atlantic Treaty Organization. (2024). *Human security*. https://www.nato.int/en/what-we-do/wider-activities/human-security

Orlando-Salling, J. (2025). The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation. *European Law Open*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5020805

Osborne Clarke. (2025). *Spain seeks to protect minors in the digital environment*. https://www.osborneclarke.com/insights/spain-seeks-protect-minors-digital-environment-key-points-new-version-draft-law

Pozza, V. D., Di Pietro, A., Morel, S., & Psaila, E. (2016). *Cyberbullying among young people*. European Parliament Think Tank. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU%282016%29571367

République Française. (2024). *Article 222-33-2-2 - Code pénal*. Légifrance. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037289658/

Robert Koch Institute. (2024). Traditional bullying and cyberbullying at schools in Germany: Results of the HBSC study 2022. *Journal of Health Monitoring*. https://www.rki.de/EN/News/Publications/Journal-of-Health-Monitoring/GBEDownloadsJ/Focus_en/JHealthMonit_2024_01_Bullying.html

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

Tech Policy Press. (2026). *EU intensifies child safety enforcement, flags gaps in Meta age checks*. https://www.techpolicy.press/eu-intensifies-child-safety-enforcement-flags-gaps-in-meta-age-checks/

TechCrunch. (2025). *EC finds Meta and TikTok breached transparency rules under DSA*. https://techcrunch.com/2025/10/24/ec-finds-meta-and-tiktok-breached-transparency-rules-under-dsa/

UNESCO. (2021). *Tackling cyberbullying and other forms of online violence involving children and young people: Fact sheet*. https://unesdoc.unesco.org/ark:/48223/pf0000379486

United Nations. (1989). *Convention on the Rights of the Child*. United Nations Treaty Series, vol. 1577. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press. https://hdr.undp.org/system/files/documents/hdr1994encompletenostats.pdf

United Nations Office for Disaster Risk Reduction & International Science Council. (2025). *Cyberbullying: Definition and facts*. https://indonesia.un.org/en/305496-cyberbullying-definition-and-facts

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior, 11*(4), 499–503. https://doi.org/10.1089/cpb.2007.0042

Wæver, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On security* (pp. 46–86). Columbia University Press. https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf

Waller, A. P., Lokhande, A. P., Ekambaram, V., Deshpande, S. N., & Ostermeyer, B. (2018). Cyberbullying: An unceasing threat in today's digitalized world. *Psychiatric Annals, 48*(9), 408–415. https://doi.org/10.3928/00485713-20180821-01

Wright, M. F. (2016). *A social-ecological approach to cyberbullying*. Nova Science Publishers. https://gala.gre.ac.uk/id/eprint/35463/1/35263_GORZIG_Cyberbullying_in_Europe.pdf

Xu, Y., & Trzaskawka, P. (2021). Towards descriptive adequacy of cyberbullying: Interdisciplinary studies on features, cases and legislative concerns of cyberbullying. *EPJ Techniques and Instrumentation, 34*(4). https://doi.org/10.1007/s11196-021-09856-4

Yoti. (2026). *Understanding age assurance in Spain's new online safety law*. https://www.yoti.com/blog/age-assurance-spain-online-safety-organic-law/

European Audiovisual Observatory. (2024). *[ES] Approval of draft Organic Law on the Protection of Minors in Digital Environments*. IRIS Merlin. https://merlin.obs.coe.int/article/10093

ANNEX: Declaration of Use of Generative AI Tools

Academic Year: _2025-2026_____
Master's Programme: Master in International Security Management (MISM)
Student Name: ____Montana Hill_____

I declare that generative artificial intelligence tools have been used as support tools in the preparation of this Master's Final Thesis.

X YES □ NO

1. Ethical and Academic Use

Have you included sensitive or personal data when using AI tools? If yes, specify:
_No_____
_____

Have you used AI tools to replace your own work without critically reviewing the generated content? If yes, specify:

_No_____
_____

Have you followed the academic recommendations and guidelines regarding the use of AI tools?

_Yes_____
_____

2. Technical Use of AI Tools

Please indicate the AI tools used (e.g., ChatGPT, Copilot, Claude, Gemini):

Claude

Please mark the applicable uses:

- ☐ Text generation
- ☐ Reformulation / editing
- ☐ Translation / proofreading
- ☐ ~~Structure suggestions~~
- ☐ ~~Methodological support~~
- ☐ ~~Bibliographic search or citation support~~
- ☐ Audiovisual content generation

- ☐ Other uses (please specify)

I confirm that the final content of this thesis has been fully reviewed, corrected, and validated by me as the author. The use of AI has not replaced my own critical analysis, personal reflection, or intellectual work.

Signature: _____Montana Hill_____