International Journal of Law, Crime and Justice

E-ISSN: 3047-1362
P-ISSN: 3047-1370

Review Article

Legal Implications of Cyber Bullying Crimes : A Comparative Study

Farizt Sultanul Husni[1], Taufiq[2], Fandi Rahmadi[3], Kautsar Ramadhan[4], Muhammad Arnif[5], Muhammad Hatta[6]

1 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
2 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
3 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
4 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
5 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
6 Magister Hukum, Fakultas Hukum, Universitas Malikussaleh, Indonesia
email: muhammad.hatta@unimal.ac.id

***** Corresponding Author : Farizt Sultanul Husni

Abstract: Cyber bullying or bullying carried out online or cyberspace has become a serious and worrying issue in today's digital era, with a wide impact on victims and perpetrators. This phenomenon not only causes psychological and social disturbances for victims, but also poses serious challenges in law enforcement. This study aims to analyze and compare the legal implications of cyber bullying in several jurisdictions, especially Indonesia, the United Kingdom, the United States, and South Korea. Through a normative juridical approach and comparative or comparative legal methods, this study analyzes the regulatory framework applicable in each country, including legal definitions, criminal sanctions, and legal protection for victims. The results of the study show that there are significant differences in the handling of cyber bullying laws between countries, both in terms of the formulation of legal norms and enforcement mechanisms. This study concludes that the harmonization of cyber law policies internationally is an urgent need to create more effective and comprehensive protection for victims of digital violence, especially among adolescents and children.

Keywords: cyber bullying, criminal law, legal comparison, cybercrime, victim protection

1. Introduction

The rapid development of information technology has brought significant changes in various aspects of human life, including in terms of communication, education, and social interaction. Where technology allows for cross-border activity relationships and provides ease in accessing and disseminating information instantly, but on the other hand this advancement also opens up space for various forms of social deviance and crime, including cyber-based crimes or cybercrime. One of the forms cybercrime that the world is concerned about is cyber bullying(Patchin & Hinduja, 2018), which is an act of bullying carried out through digital media such as social media or other online platforms.

Cyber bullying has become a serious issue in the digital age, which is exacerbated by the widespread use of technology and social media. This phenomenon is rife among children and adolescents and causes severe psychological and emotional impacts such as anxiety, depression, and even suicide in extreme cases. The legal aspects related to cyberbullying are quite complex and vary from country to country, so a comprehensive legal framework is needed to deal with this issue effectively.(Asam & Samara, 2016)

Cyber bullying differs from traditional forms of bullying because of its anonymous nature, can happen at any time, and has the potential to spread very quickly to the wider community. Cyber bullying is an extension of bullying in the form of bullying or bullying carried out in cyberspace. The perpetrator often feels protected by a hidden identity, while the victim does not have a safe space because these crimes can reach them even in private environments such as homes. Types of cyber bullying include insults, defamation, rumor

Received: 11 March 2025
Revised: 26 March 2025
Accepted: 19 April 2025
Online Available : 24 April 2025
Curr. Ver.: 24 April 2025

spread, digital sexual harassment, as well as visual manipulation using technologies such as deepfakes (Kowalski et al., 2014).

This type of crime not only impacts the psychological state of the victim, but can also lead to prolonged trauma and even the risk of suicide, especially among adolescents. According to a report from UNICEF (United Nation Children's Fund), one in three adolescents in more than 30 countries experience (UNICEF, 2021)cyber bullying. This phenomenon shows that Cyber bullying has become a global problem that transcends the boundaries of the State and culture. In Indonesia itself, the Ministry of Communication and Information Technology (Kominfo), which has now been renamed the Ministry of Communication and Digital (Komdigi), noted that there has been a significant increase in reports of cases of digital violence against children and adolescents in recent years. Although Indonesia already has legal instruments such as the Information and Technology Law (ITE Law), legal protection for victims Cyber bullying is still considered insufficiently effective and adequate, especially because there is no specific legal definition and comprehensive protection mechanism.(Kominfo, 2023)

When viewed from the side of law enforcement, Cyber bullying poses quite serious challenges due to the transnational nature of crime, the difficulty of tracking perpetrators, and the weak digital literacy of the community. Some countries have formulated specific regulations to deal with this form of crime more strictly, such as the United States integrating the issue of Cyber bullying (Slonje & Smith, 2008)in the criminal system and education. South Korea, which implements policies that focus on a punitive and educational approach, especially in schools and online environments or digital spaces. On the other hand, there are still many developing countries, including Indonesia, that do not yet have a structured legal approach to this crime. Where there are still weaknesses in the policies regulated in the ITE Law to reach Cyber bullying (Clara, Soponyono, & Astuti, 2016)

The absence of harmonization of international law related to cyber bullying also exacerbates the gap in handling cases involving perpetrators or victims from different jurisdictions. This has become one of the major challenges in the current international legal system. In addition, differences in legal culture and normative approaches in each country often hinder the process of cross-border law enforcement. Comparative studies are therefore important to understand how different countries respond to these challenges, and then how best practices can be adopted contextually.

To effectively address cyberbullying, a comprehensive approach is needed and not just relying on punishment. Prevention, education, and assistance and protection systems for victims are also very important. Given the nature of cyberbullying that can cross national borders, international collaboration and legal alignment between countries are strategic steps in tackling this problem globally.(Wijaya, Johardi, & Pratiwi, 2024)

The purpose of this study is to analyze and examine the legal implications of the crime of cyber bullying through a comparative legal study approach in four countries, namely, Indonesia, the United Kingdom, the United States and South Korea. The selection of these countries is based on the diversity of legal systems and policy approaches used in dealing with cyber bullying, so that it can provide a broad and in-depth picture. By understanding the differences and similarities in legal approaches between countries, it is hoped that this research can make a theoretical and practical contribution to the development of legal policies that are more adaptive and responsive to the challenges of cybercrime, especially cyber bullying.

2. Literature Review

Technological Developments and the Emergence of Cybercrime

The increasingly advanced and rapid development of technology has created an increasingly complex digital ecosystem. The cyberspace, which was originally created to facilitate and accelerate the exchange of information and strengthen social connections, is now also a new forum for crime. Cybercrime (cybercrime) covers various forms of violations of the law committed through electronic media, including online fraud, malware distribution, personal data theft, and digital verbal violence. One form of cybercrime that is the main concern is cyber bullying, namely bullying that occurs through digital channels such as social

media, email, forums, or other communication platforms. The existence of technology expands the reach of perpetrators and aggravates the psychological impact on victims.(Wall, 2007)

Definition of Cyber Bullying

Crimes born as a negative impact of the development of internet technology are often referred to as cyber crime. According to the British police, cyber crime is all kinds of use of computer networks for criminal purposes or high-tech criminals by abusing the convenience of digital technology. (Wahid & Labib, 2004)Cyber bullying itself is one of the types of cyber crime. Cyber bullying is a negative impact of the growing use of information technology.

Cyber bullying is a form of bullying. Bullying is a form of violence and intimidation carried out by a person or group of people continuously with the aim of oppressing the victim into being injured, losing confidence or even killing his character. Bullying It has three basic elements, namely aggressive or offensive behavior, carried out repeatedly, and the imbalance of power between the parties involved. It can be said that (Clara, Soponyono, & Astuti, 2016)cyber bullying is an aggressive act carried out deliberately and repeatedly by individuals or groups against victims who are unable to defend themselves, by utilizing electronic means. cyber bullying This is a form of bullying that has distinctive characteristics, namely it occurs in cyberspace, is carried out anonymously, and is able to spread very quickly to a wide audience. Main characteristics of (Hinduja & Patchin, 2015)cyber bullying These include the anonymity of the perpetrator, the ability of the message to spread quickly, and to take place continuously in time. This makes the victim feel that they do not have a safe place, because bullying can happen anytime and anywhere and the impact cyber bullying often more severe than conventional bullying

Legal Framework of Cyber bullying in Different Countries

Legal handling of cyber bullying varies greatly globally. Developed countries tend to have designed more specific legal frameworks. In the UK, for example, there are Malicious Communications Act 1988 and Communications Act 2003 that regulates electronic communications that are threatening, harassing, or insulting. The United States, although it does not have a specific federal law, gives states the authority to regulate issues (Citron, 2014)cyber bullying, especially in the educational environment. South Korea has taken a progressive step by implementing harsh laws following suicide cases among artists due to online bullying. In Indonesia, namely Law Number 1 of 2024 The second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

3. Methods

Research Approach

This study uses the descriptive qualitative with normative juridical methods and comparative law (comparative legal study). The normative juridical approach is used to examine applicable laws and regulations and legal norms related to crime cyber bullying in each country. The descriptive approach aims to provide a comprehensive picture of social phenomena, especially government measures in tackling cyber threats. Meanwhile, the comparative approach of law allows researchers to analyze the similarities and differences of the legal system in dealing with (Sugiyono, 2017)cyber bullying comprehensively (Zweigert & Kötz, 1998). The focus of the research is not only on the content of formal law, but also on the context of the implementation and effectiveness of legal application in the field.

Data Type

The data used in this study are primary and secondary data:

1) Data Primer

Laws and regulations such as the ITE Act in Indonesia, the Malicious Communications Act in the United Kingdom, state regulations in the United States, and the Network Act in South Korea.

2) Data Seconds

Secondary data was obtained from various sources such as scientific journals, books, legal documents (Laws and Regulations and ITE Law), scientific journals, research results, and UNICEF reports.

3) Tertiary Legal Materials

In the form of a legal dictionary, and other complementary documents that help explain the basic concepts of cyber bullying.

Data Collection Techniques

Data collection is carried out using documentation study techniques, namely by searching and collecting legal materials and academic literature from various trusted sources such as university digital libraries, international journal databases and official government websites or legal institutions. In addition, credible legal news sources are also used to enrich understanding of the dynamics of law application that occur in actuality. According to Creswell (2014), documentation studies are an appropriate method in normative legal research because they allow researchers to trace the legal footprint and compare regulatory developments in a global context.

Data Analysis Techniques

Data analysis was carried out through qualitative-descriptive and comparative analysis. The first stage is legal content analysis of each relevant regulation. Then an identification of the substance of the law, the structure of law enforcement, and the legal culture (Friedman, 2001) in each country was carried out. Furthermore, a comparison between legal systems is made based on three main aspects:

1) Normative (legal substance): for example, how each country defines cyber bullying and establishes its sanctions.

2) Institutional (law enforcement): actors involved, such as regulatory agencies, police, schools, and social media platforms.

3) Preventive and educational: non-penal policies such as digital education, awareness campaigns, and victim rehabilitation.

The comparative legal technique used refers to the systematic approach by Zweigert & Kötz (1998), which emphasizes principles such as functional equivalence and contextual analysis, i.e. comparing legal institutions that have similar functions in different social and cultural contexts.

Data Validity Test

To ensure the validity of the data, source triangulation was carried out, which is comparing various sources of legal data and scientific literature from various jurisdictions. In addition, validity is also maintained through peer review and cross-checking between legal references to avoid bias and ensure that legal interpretation is carried out accurately and objectively.

4. Results

Definition of Cyber bullying as Part of Cyber Crime

Cyber bullying is a form of cyber crime that develops along with the advancement of information and communication technology. According to Willard (2007), cyber bullying is defined as aggressive behavior that is carried out repeatedly by individuals or groups through electronic media, with the aim of hurting, threatening, or humiliating the victim. The form can be in the form of offensive text messages, unauthorized photo distribution, hate speech, and social manipulation through cyberspace.

In the context of criminal law, cyber bullying is classified as a crime against a person's personal dignity and psychological security, which in the digital realm can have a wide impact and is difficult to control due to its viral and anonymous nature (UNODC, 2022). In some countries, cyber bullying has been specifically codified in the legal system, while in other countries it is still handled through the general norms of cybercrime.

Cyber bullying is included in the subcategory of interpersonal cyber crime, which is cybercrime that targets individuals personally through digital media. It is different from economic Cyber Crime such as online fraud or data theft, because it has more impact on the mental health and social integrity of the victim (Wall, 2007). Therefore, the legal framework governing cyber bullying must consider psychological and social aspects, not just digital technical aspects.

Legal Implications of Cyber Bullying Crime

Implications of criminal law cyber bullying is a criminal threat, which is in the form of imprisonment and fines. In Indonesia cyber bullying regulated in Law Number 1 of 2024 The second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions and can also be handled based on the Criminal Code, especially Article 310, Article 311, and Article 315. cyber bullying It can be classified as an unlawful act because it contains elements of insult, defamation, threats, and incitement to commit certain actions. In many jurisdictions, the cyber bullying that are recurrent and cause significant psychological distress can be classified as cyberstalking or harassment(Citron, 2014), which has the threat of criminal penalties. For example, if the perpetrator systematically disseminates false or embarrassing information about the victim, then the act can qualify as a criminal act of defamation or electronic harassment.

Comparison of Cyber Bullying Regulations in Indonesia, UK, United States and South Korea

1. Indonesia

In Indonesia, cyber bullying is regulated in Law Number 1 of 2024, the second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. cyber bullying can also be charged with the Criminal Code, here are several articles that regulate cyber bullying.

a. Article 27 of the ITE Law regulates cyber bullying in the form of insults and threats Article 27A of Law No. 1 of 2024 regulates bullying on social media in the form of insults, attacking someone's honor or good name.

b. Article 27B paragraph (2) of Law No. 1 of 2024 regulates prohibited acts, especially related to the threat of pollution.

c. Article 310, Article 311, and Article 315 of the Criminal Code regulate insults through cyberspace (cyber bullying).

However, the use of the ITE Law in the case of cyber bullying (Kominfo, 2023)often causes polemics, because these articles are often considered multi-interpreted and have the potential to be abused. In Indonesia, cyberbullying is categorized as a cybercrime that requires special handling because of its significant impact on victims and challenges in enforcing the law against perpetrators. Through the Electronic Information and Transaction Law (ITE Law), acts such as insults, threats, and defamation in the digital space have been regulated as violations of criminal law. Even so, protection for victims, especially children, is still not

optimal, because the legal approach is more focused on punishing perpetrators than providing support and recovery for victims.(Aradhana & Pangaribuan, 2022)(Laena & Riswadi, 2022).

2. **English**

The UK has a relatively comprehensive approach to regulating cyber bullying. Under the Malicious Communications Act 1988 and the Communications Act 2003, any form of communication that is intimidating, threatening, or psychologically harmful is punishable. In the latest development, the UK government passed the Online Safety Act 2023 which gives the regulator (Ofcom) the power to crack down on digital platforms that allow the spread of violent or bullying content online (UK Parliament, 2023). The UK has also developed education and protection programmes in schools through cooperation between education departments, police and civil society organisations. Strict law enforcement combined with a preventive approach makes the system in the UK one of the models worth looking at.

3. **United States**

Regulation cyber bullying in the United States is decentralized. There is no federal law that specifically governs cyber bullying, however most states have local regulations that include definitions, sanctions, and mechanisms for handling them, especially in educational settings. Some states like New Jersey and California implement policies (Hinduja & Patchin, 2015)zero tolerance against cyber bullying in schools, and requiring reporting and intervention. However, the legal approach in the United States focuses more on education and prevention than criminalization, because the principle of freedom of expression in the constitution is highly guarded (First Amendment). This creates its own challenge in formulating the boundaries between hate speech and freedom of opinion.

4. **South Korea**

South Korea is one of the countries that is very proactive in dealing with cyber bullying. Following an increase in suicides among artists attributed to online harassment, the country tightened laws through Act on Promotion of Information and Communications Network Utilization and Information Protection. The regulation regulates the prohibition of anonymous comments and gives authorities the authority to remove offensive content quickly. In addition, South Korea developed an integrated online reporting system as well as online counseling services handled by government agencies. Strong law enforcement coupled with strict control over social media makes South Korea a model of regulation based on victim protection.(Chung, 2021)

Each country has a different approach to tackling cyber bullying, depending on its legal system, culture, and technology policies. Indonesia does not yet have special regulations regarding cyber bullying. Handling generally uses the ITE Law Article 27 paragraph (3) and Article 29, which regulates defamation and threats of violence. However, this regulation is considered not yet able to reach the complexity of modern forms of cyber bullying, such as doxing or the dissemination of personal content (Kominfo, 2023).

The UK regulates cyber bullying through the Malicious Communications Act 1988, the Communications Act 2003, and the Online Safety Act 2023. The country has a progressive approach, which not only punishes the perpetrators, but also requires digital platforms to be responsible for user content. Regulator Ofcom has the authority to impose sanctions on platforms that neglect (UK Parliament, 2023). The United States does not yet have a specific federal law, but almost all states have adopted anti-cyber bullying policies, especially in the education sector. The law is drafted so as not to violate the First Amendment, so that the approach is preventive through education and school policies (Patchin & Hinduja, 2018). South Korea has designated Cyber bullying as a violation of the law under the Network Act. The country has a rapid reporting system and user identity obligations to prevent abuse. The government also provides psychological and legal support services for victims (Chung, 2021).

Broadly speaking, the UK and Korea have a strong and holistic legal approach, while the US and Indonesia are more limited to certain aspects. Britain emphasizes the responsibility of the platform, Korea emphasizes the protection of victims, the US maintains a balance with the right to freedom of expression, and Indonesia is still struggling to establish more specific regulations.

Legal Implications of Cyber Bullying

The legal implications of cyber bullying can be seen in three main areas:

1. Criminal

Cyber bullying perpetrators can be charged with criminal law, either through special laws (such as in the UK and South Korea), or general articles (such as in Indonesia). The sanctions include fines and imprisonment (confinement).

2. Digital Platform Liability (intermediary liability),

In the UK and Korea, digital service providers are required to follow up on cyber bullying reports and provide a complaint feature. The UK through the Online Safety Act even gives Ofcom the authority to impose fines on platforms such as TikTok or Instagram if it does not respond quickly to harmful content (UK Government, 2023).

3. Victim Protection and Prevention, In Korea and the United Kingdom, victims of cyber bullying can access legal aid, psychologists, and social recovery services online. In contrast, in Indonesia and the US, victim protection systems are still limited and have not been consistently regulated at the national level. In Indonesia, this protection is still weak because there is no integrated system.

Obstacles in Law Enforcement

Law enforcement of cases cyber bullying face a number of major challenges. First, the difficulty of identifying the perpetrator due to anonymity in cyberspace. Second, the limitations of the apparatus in understanding digital technology, as well as the uneven digital literacy among the public and law enforcement agencies. Third, there are limitations in jurisdiction, especially in cross-border cases. This makes it difficult for law enforcement officials to handle cases where the perpetrators are abroad or using foreign servers. In addition, differences in legal norms and cultures between countries complicate international cooperation in terms of extradition and digital proof.(Wall & Williams, 2007)

Protection of Victims and the Role of Education

Protection for victims of cyber bullying must not only be in the form of repressive laws against the perpetrators, but also needs to include aspects of psychological rehabilitation, counseling services, and safe and accessible reporting mechanisms. Livingstone and Smith (2014) emphasize the importance of collaboration between schools, families, governments, and digital platforms in preventing and dealing with digital bullying. Many countries have developed education-based approaches, such as digital literacy curricula and intervention programs in schools. Building awareness of social media etiquette and digital empathy is an important part of a long-term prevention strategy.

The Urgency of Legal Comparative Studies

In the face of the phenomenon cyber bullying cross-border, comparative legal studies are important to identify the best handling model that can be adapted according to the national context. Comparative studies allow analysis of regulatory effectiveness, appropriateness of sanctions approaches, and protection of victims in different jurisdictions (Zweigert & Kötz, 1998). This study emphasizes the importance of looking at how countries such as the UK, South Korea, and the United States respond to the issue cyber bullying through legal instruments, and compare it with the legal framework in Indonesia that is still developing. The results are expected to provide more contextual and implementable policy recommendations.

Discussion

The findings of the comparative study show that cyber bullying is a form of cybercrime that has not been fully accommodated equally within the legal framework in each country. In Indonesia, regulations still rely on general articles in the ITE Law, such as articles on insults or threats. Unfortunately, these rules have not been able to cover the complexity of anonymous, repetitive, and multidimensional digital bullying behaviors (Kominfo, 2023).

Meanwhile, countries such as the United Kingdom and South Korea have developed more comprehensive legal instruments. Their approach involves the active role of digital platforms in moderating content, efficient reporting systems, and psychological protection for victims. This shows that they acknowledge cyber bullying It is not just a problem between individuals, but a structural issue that requires the intervention of the state and third parties such as technology companies. But in the UK, some laws such as Protection from Harassment Act and Communications Act used to tackle online bullying. However, obstacles remain, mainly due to unclear legal definitions and difficulties in proving the element of intent .(Asam & Samara, 2016)

The United States faces a different challenge: maintaining a balance between individual protection from cyberbullying and the freedom of speech guaranteed by the constitution. Therefore, regulations related to cyber bullying in America tend to be localized at the state level and are mostly associated with school policies, rather than national laws (Patchin & Hinduja, 2018). Indonesia itself still has a lot of homework. The absence of special rules causes victims to often not get maximum protection. The lack of knowledge of law enforcement about digital crimes, limited victim assistance services, and the lack of synergy between legal and social institutions are major obstacles in handling cases (UNICEF Indonesia, 2022).

The legal system, both at the national and international levels, still faces various limitations, such as the lack of a uniform definition of cyberbullying and barriers in terms of proof and jurisdiction between countries. In addition, the difficulty in identifying the element of intentionality to hurt and the low public understanding of this issue are significant additional challenges.(Cheng, Hu, Matulewska, & Wagner, 2020)

The U.K., has positioned an independent regulator (Ofcom) to ensure the accountability of online service providers, while South Korea has implemented a rapid reporting system and identity authentication obligations to reduce potential abuse. These practices can be used as a reference in the formulation of national policies that are more responsive to technological developments. Furthermore, the approach to countering cyber bullying should not only rely on criminal punishment. Preventive strategies are also needed, such as digital literacy education, the formation of a healthy internet culture, and the inculcation of online ethical values from an early age. As stated by Livingstone and Smith (2014), preventing online crime should start with a deep understanding of the online behavior of children and adolescents, not just by taking action against the perpetrators after the incident.

Thus, this discussion emphasized that the legal approach to Cyber bullying must touch on three main aspects, legal clarity, the participation of digital platforms, and a sustainable victim protection system. A reactive approach alone is not enough, a combination of regulation, education, and cross-sector collaboration is needed to address these challenges comprehensively.

5. Conclusion

Cyber bullying is a complex form of digital crime and has a serious impact, but not all countries have an adequate legal approach to deal with it. This study shows that the United Kingdom and South Korea have implemented progressive legal policies, while the United States focuses on freedom of expression, and Indonesia still lacks specific regulations, where although the regulation of cyber bullying has been recognized through the ITE Law and the Criminal Code, there is no law that specifically and comprehensively regulates the issue of cyber bullying in Indonesia. This difference in approach emphasizes the importance of the presence of laws that are not only repressive, but also preventive and protective. Indonesia needs to urgently design specific regulations that respond to various forms of cyberbullying, while strengthening victim protection and digital platform responsibility. Overall, the challenge of cyber bullying requires cross-sectoral strategies, ranging from law, technology, to digital education, to create a safer and fairer online space for all users.

6. Limitation

This research has several limitations. First, the legal analysis is only focused on four countries so that it does not reflect global conditions as a whole. Second, the discussion is normative and does not include empirical data such as case studies or interviews with victims and law enforcement. Third, comparisons are carried out at the level of formal regulations, without in-depth review of the implementation or effectiveness of the law in the field. These limitations open up opportunities for more comprehensive follow-up research with a multidisciplinary approach and wider regional coverage.

References

[1] Aiman El, A., & Samara, M. (2016). Cyberbullying and the Law: A Review of Psychological and Legal Challenges. Computer in Human Behaviour, Vol. 65. 127-141. https://doi.org/10.1016/j.chb.2016.08.012

Aradhana, A. A. A., & Pangaribuan, C. S. (2022). Cyberbullying in Media Social: A Mainstreaming the Victim Protection Principles in Indonesian Criminal Justice System. Indonesia Media Law Review, 1(2). 2829-7628.

[2] Clara, F., Soponyono, E., & Astuti, AM, E, S., (2016). Criminal Law Policy in an Effort to Overcome Cyberbullying in an Effort to Reform the Criminal Law. Diponegoro Law Journal, Vol. 5 No. 3.

[3] Cheng, L., Hu, X., Matulewska, A. E., & Wagner, A. (2020). Exploring Cyberbullying: a Socio-Semiotic Perspective. International Journal of Legal Discourse, 5(2).

[4] Chung, Y. (2021). Cyberbullying Regulation and Social Media Control in South Korea. Asian Journal of Comparative Law, 16(2), 321–340.

[5] Citron, D. K. (2014). Hate Crimes in Cyberspace. Harvard University Press.

[6] Citron, D. K., & Franks, M. A. (2019). The Internet as a Speech Machine and a Weapon. Fordham Law Review, 87(1), 231–260.

[7] Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

[8] Friedman, L. M. (2001). The Legal System: A Social Science Perspective. Russell Sage Foundation.

[9] Hinduja, S., & Patchin, J. W. (2015). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (2nd ed.). Corwin Press.

[10] Kominfo. (2023). National Cybersecurity Annual Report 2023. Ministry of Communication and Information of the Republic of Indonesia.

[11] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137.

[12] Laena, M., & Riswadi. (2022). Legal Protection for Child Victims of Cyber Bullying, Proceeding of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE, DOI 10.4108/eai.16-4-2022.2319752

[13] 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.

[14] Wijaya, J. N., Johardi A., & Pratiwi. S. (2024). Criminal Liability Perpetrator Bullying Through Social Media. Journal Of Indonesia Law & Policy Review, 6(1), 2715-498X

[15] Patchin, J. W., & Hinduja, S. (2018). Cyberbullying: Review of an old problem gone viral. Journal of Adolescent Health, 63(4), 1–6.

[16] Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. Scandinavian Journal of Psychology, 49(2), 147–154.

[17] Sugiyono. (2017). Quantitative, Qualitative, and R&D Research Methods. Bandung: Alfabeta.

[18] UK Parliament. (2023). Online Safety Act 2023. Retrieved from https://www.parliament.uk

[19[Law Number 1 of 2024 The second amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

[20] UNICEF. (2021). Cyberbullying: What is it and how to stop it. Retrieved from https://www.unicef.org/end-violence/how-to-stop-cyberbullying

[21] UNODC. (2022). The Global Threat of Cybercrime: A Report on Current Challenges. United Nations Office on Drugs and Crime.

[22] Wahid, A., & Labib, M., (2004). Cyber Crime. Bandung: Refika Aditama.

[23] Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.

[24] Wall, D. S., & Williams, M. L. (2007). Policing cybercrime: Networked and social control. Policing and Society, 17(3), 305–323.
[25] Willard, N. (2007). Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress. Research Press.
[26] Zweigert, K., & Kötz, H. (1998). An Introduction to Comparative Law (3rd ed.). Oxford University Press.