

Cyberbullying under Criminal Law: A Comparative Analysis of Indonesian and Malaysian Legal Frameworks

Handina Sulastrina Bakhtiar¹, Ahmad Yusup²

¹Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta, E-mail: hbakhtiar@upnvj.ac.id

² Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta, E-mail: ahmadyusup@upnvj.ac.id

ARTICLE INFO	ABSTRACT
Keywords: Cyber Bullying; Criminal Law; Indonesia; Malaysia How to cite: Bakhtiar, Handina Sulastrina & Yusup, Ahmad. (2026). Cyberbullying under Criminal Law: A Comparative Analysis of Indonesian and Malaysian Legal Frameworks. <i>Veteran Law Review</i>. 9(1).114-126. Received:2026-06-03 Revised:2026-06-22 Accepted:2026-06-29	This study aims to analyse and compare the conception of cyberbullying under the criminal laws of Indonesia and Malaysia. This study employs a normative legal research method, also referred to as doctrinal legal research, with a prescriptive analytical approach. The approaches adopted in this study comprise a conceptual approach, a case approach, and a comparative approach. The findings indicate that Indonesia regulates cyberbullying indirectly through Law Number 11 of 2008 concerning Electronic Information and Transactions, including its subsequent amendments, as well as through the National Criminal Code. By contrast, Malaysia provides more specific provisions through the reform of its Penal Code. The main difference lies in the formulation of the elements of the offence and the applicable criminal sanctions. Malaysia tends to provide clearer and more specific regulation concerning cyberbullying, whereas in Indonesia the regulation remains relatively abstract, and law enforcement practices continue to rely primarily on the Electronic Information and Transactions Law, the Pornography Law, and the National Criminal Code.

1. Introduction

Bullying is, in principle, not a new phenomenon among children, adolescents, or adults. The fact that children, adolescents, and adults tend to “play around” and mock one another indicates that, historically, bullying has often been regarded as a *fait accompli*, or as a condition that must be accepted by children, adolescents, and adults, and has not always been taken seriously by them (Amy Dwyer & Patricia Easteal, 2013, hlm. 92). However, over time, bullying has increasingly been recognised as having adverse effects on health, affecting both physical and mental health (Windy Freska, 2023, hlm. 5). More broadly, bullying, often understood as “peer harassment”, constitutes a form of pressure that may produce serious consequences, particularly in relation to delinquency, and may further generate criminogenic effects (Hay dkk., 2010,

hlm. 131). Therefore, behaviour that was once perceived as normal has now been proven to constitute a serious problem (Choi dkk., 2016, hlm. 150).

Over the past few decades, issues of violence, gender discrimination, and harassment, committed both by and against young people, have become increasingly visible and widely voiced across the world (Anne Wagner, 2019, hlm. 303). This development has also been reinforced by the rapid advancement of technology, whereby violence and discrimination through bullying are no longer carried out only in traditional or direct forms, but also online through various instruments that utilise digital technology. The internet and online applications have become a fundamental part of society. Although they provide significant benefits, they also pose threats to children, adolescents, and adults (Adiarti & Fadhilah, 2025, hlm. 9).

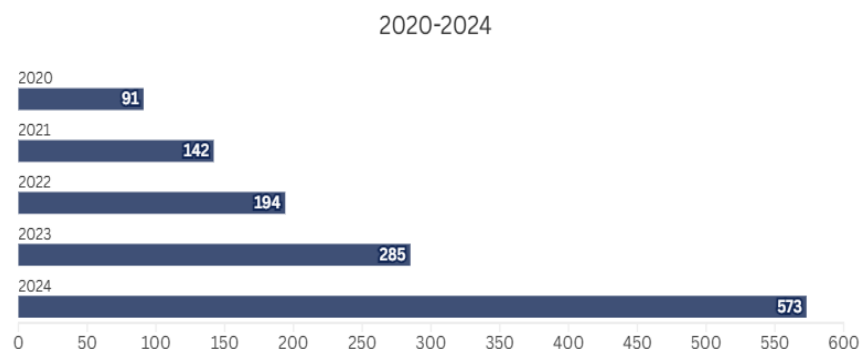
Cyberbullying is one such threat (Stevens dkk., 2021, hlm. 367). Cyberbullying has been defined as "the repeated use of various forms of technology, such as mobile phones, pagers, email, instant messaging, and websites, by individuals or groups to harm others" (Patchin & Hinduja, 2006, hlm. 148). The impact of cyberbullying may be more severe than that associated with traditional bullying, as cyberbullying causes harm to the mental and physical health of adolescents. In some cases, victims have even died by suicide, thereby prompting urgent action to prevent and address such behaviour (Mona O'Moore, 2012, hlm. 210). Several suicide cases involving victims of cyberbullying have drawn public attention to the seriousness of cyberbullying incidents (Ahmad Razali dkk., 2022, hlm. 124). One of the most shocking cases in the global context of cyberbullying was that of Amanda Michelle Todd, a 15-year-old student in Canada who tragically died by suicide after being unable to withstand the persistent bullying she experienced through social media (Muhammad Yasin & Norman Edwin Elnizar, 2019).

A similar case also occurred in Malaysia and involved a Malaysian influencer, Rajeswary Appahu, known as Esha. She was found dead at her home on Friday, 5 July 2024. The incident occurred one day after Esha had lodged a police report against two individuals, accusing them of harassing her online. She was allegedly driven to suicide after being subjected to continuous bullying for more than a month (Maheza Nurmiagita, 2024). In that case, the court imposed only a fine of RM100, equivalent to approximately IDR356,700. Such a decision raises the question of whether it may become a precedent for similar cases involving other women (Maheza Nurmiagita, 2024).

Following the Rajeswary Appahu case, the Malaysian Parliament, as the legislative authority, responded promptly by reformulating the legal framework concerning cyberbullying (Nazli bin Ismail, 2025). The Online Safety Bill was introduced in Parliament to close existing legal loopholes and to promote the creation of a safer digital environment. Under the Bill, social

media platform providers are required to ensure the safety of their platforms. These measures include protecting children under the age of 13 and restricting access to harmful content (Maheza Nurmiagita, 2024). According to Nazli bin Ismail, the Bill has been enacted into law, and cyberbullying cases in Malaysia are now subject to the new legislation, which provides for heavier criminal sanctions, including imprisonment of up to 30 years (Nazli bin Ismail, 2025).

In Indonesia, 48% of children who have accessed the internet reported having experienced cyberbullying. The phenomenon of digital bullying largely occurs in private spaces, such as personal chat rooms or friendship groups, thereby presenting particular challenges in terms of detection and response (Kiki Safitri & Dani Prabowo, 2025). Data from the Indonesian Child Protection Commission (Komisi Perlindungan Anak Indonesia, KPAI), the Indonesian Education Monitoring Network (Jaringan Pemantau Pendidikan Indonesia, JPPI), and digital monitoring reports by organisations such as SAFENet indicate a significant increase in bullying cases, both in schools and



in cyberspace (Emily Zakia, 2025). According to JPPI, as cited by GoodStats, there was a sharp increase in cases of violence within educational environments in 2024 (Emily Zakia, 2025).

Figure 1. Number of reported bullying cases in Indonesia from 2020 to 2024.
Source: Indonesian Child Protection Commission (KPAI) and Indonesian Education Monitoring Network (JPPI).

Nevertheless, despite the prevalence of cyberbullying cases in Indonesia, there is still no specific provision that explicitly regulates cyberbullying (Hadi, 2025, hlm. 138). When cyberbullying cases occur in Indonesia, the legal provisions applied generally refer to Article 45 paragraph (1) in conjunction with Article 27 paragraph (3) of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended twice, first by Law Number 19 of 2016 and most recently by Law Number 1 of 2024, hereinafter referred to as the Electronic Information and Transactions Law (UU ITE). This situation in Indonesia differs considerably from that in

Malaysia, which has responded more swiftly to cyberbullying. Therefore, this study seeks to compare the regulation of cyberbullying in Indonesia and Malaysia, particularly at the conceptual level. This is important because, in Indonesia, cyberbullying is still generally viewed as part of the offence of defamation, whereas closer examination reveals fundamental differences between the concept of defamation and that of cyberbullying.

2. Method

This study is normative legal research, also referred to as doctrinal legal research, and employs a prescriptive analytical method. It examines cyberbullying as a legal concept within criminal law by analysing statutory provisions, legal doctrines, relevant cases, and comparative legal developments. Three approaches are employed. First, the conceptual approach is used to clarify the meaning, elements, and legal characteristics of cyberbullying, including its distinction from defamation, harassment, and other technology-facilitated offences. Secondly, the case approach is adopted to examine cyberbullying cases that have occurred in Indonesia and Malaysia, particularly in relation to victim protection, evidentiary issues, and criminal liability. Thirdly, the comparative approach is used to compare the legal construction of cyberbullying in Malaysia and Indonesia, and, where relevant, with other jurisdictions that provide similar criminal law concepts.

3. Results

There is no universally agreed definition of cyberbullying (Ahmad Razali dkk., 2022). The term cyberbullying is a combination of the words “cyber” and “bullying” (B dkk., 2018, hlm. 2). Bullying refers to a form of aggressive behaviour manifested through disrespectful treatment and the use of violence or coercion to influence others, carried out intentionally and repeatedly, or with the potential to be repeated, and involving an imbalance of strength and/or power (Elpemi & Isro’i, 2020, hlm. 1–5). Such behaviour may include verbal harassment, physical violence, or coercion, and may be repeatedly directed at a particular victim, possibly on the basis of race, religion, gender, sexuality, or ability (Muhammad Dani Ihkam & I Gusti Ngurah Parwata, 2016, hlm. 4). When associated with the cyber context, cyberbullying may be understood as a form of aggressive behaviour manifested through disrespectful treatment and the use of violence or coercion to influence others, carried out intentionally and repeatedly, or with the potential to be repeated, and involving an imbalance of strength and/or power through the use of information technology or internet-based media. In brief, cyberbullying refers to bullying conducted through communication technologies (Sidauruk dkk., 2024, hlm. 157).

Cyberbullying uses electronic technologies, such as computers, tablets, and mobile phones, to access social media, websites, text messaging services, and chat rooms through which perpetrators may attack victims (Anne Wagner, 2019, hlm. 309). These attacks involve meaningful relationships, persistent aggression, and a tendency to blame the victim. Therefore, the determining factors in legally identifying whether an act constitutes cyberbullying are “intent” and “repetition”, which support the understanding of cyberbullying as “intentional, repeated, and hostile behaviour by an individual or group intended to harm others” (Anne Wagner, 2019, hlm. 310). The question that then arises is: what forms of conduct indicate that a person has experienced cyberbullying?

In response to this question, Nancy E. Willard classifies cyberbullying into eight forms (Nancy E. Willard, 2007, hlm. 5-13). The first is flaming. Flaming refers to heated and brief arguments that occur between two or more people. It generally involves offensive, abusive, and vulgar language, insults, and, in some cases, threats. Flaming commonly occurs in public communication environments, such as discussion forums, chat rooms, or online games. A series of private angry messages sent through email or instant messaging may also be considered flaming (Nancy E. Willard, 2007, hlm. 5). The second form is online harassment, commonly referred to as cyber harassment. This usually relates to threatening or harassing emails, instant messages, or website comments. Such conduct is often carried out repeatedly to target a particular person, either by contacting the victim directly or indirectly by using or disseminating the victim’s personal information, thereby causing the victim to feel distressed, frightened, or angry. Perpetrators of cyber harassment may send angry messages containing offensive, abusive, and vulgar language to the victim (Nancy E. Willard, 2007, hlm. 6-7).

Thirdly, denigration refers to defamatory conduct. Denigration consists of harmful, false, or cruel statements. Such harmful statements may be posted online or sent to others in relation to the intended victim (Nancy E. Willard, 2007, hlm. 7). Denigration is one of the most frequently used forms of cyberbullying. It is usually committed consciously and intentionally. In general, perpetrators of denigration disseminate false information or expose another person’s negative aspects through the internet (Info Psikologi, 2024). Fourthly, impersonation refers to identity imitation. Impersonation occurs when a cyberbullying perpetrator obtains the ability to imitate the target and post content that adversely affects the victim or disrupts the victim’s friendships (Nancy E. Willard, 2007, hlm. 8). Singkatnya, peniruan identitas ini merupakan kejahatan peniruan dengan mempergunakan identitas korban guna memperoleh akses informasi yang bersifat privasi dengan tujuan mempermalukan ataupun melecehkan korban In brief, impersonation is an offence involving the misuse of a victim’s identity to gain access to private

information, with the aim of embarrassing or harassing the victim (Agustina & Purwanto, 2024, hlm. 316). Fifthly, outing and trickery constitute forms of cyberbullying in which the perpetrator disseminates another person's secrets or personal information without consent, known as outing, and/or deceives the victim into revealing secrets or personal information, known as trickery (Nancy E. Willard, 2007, hlm. 8-9).

Sixthly, exclusion refers to deliberate social exclusion. Cyberbullying through exclusion concerns the determination of who is included in a group and who is excluded (Nancy E. Willard, 2007, hlm. 9). In short, exclusion is a form of cyberbullying carried out by intentionally excluding a person from an online group (Titania Nurrahim, 2019). Seventhly, cyberstalking refers to the repeated stalking or harassment of a person through digital or electronic means. This conduct is intended to intimidate, threaten, or make the victim feel unsafe, and may be carried out through various platforms, including social media, email, instant messaging, or internet forums (Nancy E. Willard, 2007, hlm. 10-11). Cyberstalking is one form of indirect cyberbullying (Langos, 2015, hlm. 107). Eighthly, cyber threats refer to threats or cybersecurity attacks carried out by irresponsible parties through internet or computer networks (Phintraco Group, 2023). Cyber threats may be broadly classified into several categories: (Nancy E. Willard, 2007, hlm. 11) First, direct threats are statements expressing an intention to harm another person or to commit suicide. Direct threats generally contain information concerning an actual planned event. Flaming, as a form of cyberbullying, may also illustrate what is considered a direct threat. Secondly, distressing material refers to online content indicating that a person is emotionally distressed and may be considering harming another person, self-harm, or suicide. At times, the boundary between these two types of cyber threats may be unclear. Thirdly, indirect threats are forms of cyberbullying associated with cyberstalking, as they refer to online communications that threaten to cause physical harm (Langos, 2015).

In addition to the eight forms of cyberbullying identified by Nancy E. Willard, a more recent form of cyberbullying has emerged, known as happy slapping. Happy slapping refers to a form of cyberbullying in which the perpetrator deliberately slaps the victim, records the assault, and uploads it online or to the internet (Marija Draganic dkk., 2024, hlm. 3). Based on these various forms of cyberbullying, this study examines the conceptions adopted in Indonesia and Malaysia regarding cyberbullying. According to Cyber Security Malaysia, as cited by Nurulhuda Ahmad Razali, there are various forms of cyberbullying (Ahmad Razali dkk., 2022, hlm. 127). Among the commonly reported forms are: (Ahmad Razali dkk., 2022) (a) rude or cruel messages intended to intimidate through text messages, email, or other online platforms; (b) uploading or forwarding embarrassing content, including videos or photographs; (c) uploading or forwarding another person's private

or confidential information without consent; (d) harassing others by repeatedly sending messages or texts; (e) spreading rumours or falsehoods about another person; (f) using fake profiles on social networking sites to trick or mock someone; (g) happy slapping, where bullying or physical assault is recorded and disseminated; (h) flaming; (i) outing and trickery; (j) exclusion, or deliberate removal from an online group; and (k) impersonation.

Malaysia has revised its Penal Code, as reflected in the Laws of Malaysia Act A1750, Penal Code (Amendment) Act 2025. Under this amendment, cyberbullying is regulated through Sections 507b, 507c, 507d, 507e, 507f, and 507g (Laws of Malaysia Act A1750 Penal Code (Amendment) Act 2025). The purpose of this revision is to provide specific regulation for bullying committed by any means, including through online media. Accordingly, the Act regulates offences relating to bullying, including acts that cause harassment, distress, fear, or alarm, as well as acts involving the publication of identifying information that causes harassment, distress, fear, or alarm to another person (Laws of Malaysia Act A1750 Penal Code (Amendment) Act 2025). With these provisions, Malaysia now possesses a stronger legal basis for prosecuting perpetrators of cyberbullying.

From these six additional provisions, at least five forms of cyberbullying may be identified under Malaysian legislation (Laws of Malaysia Act A1750 Penal Code (Amendment) Act 2025). First, acts that cause harassment, distress, fear, or alarm are regulated under Section 507B. Secondly, acts that cause harassment, distress, fear, or alarm to a person who is likely to feel harassed, distressed, fearful, or alarmed are regulated under Section 507C. Thirdly, acts that cause a person to believe that harm will be inflicted are regulated under Section 507D. Fourthly, acts involving the publication of any identifying information that causes harassment, distress, fear, or alarm are regulated under Section 507E. Fifthly, acts involving the publication of any identifying information with the intention of causing a person to believe that harm will be inflicted are regulated under Section 507F. Section 507G, meanwhile, provides definitions of "harm", "identifying information", and "related person".

The introduction of these provisions in the amendment to Malaysia's Penal Code was prompted by the death of a Malaysian influencer who was alleged to have died by suicide after being unable to withstand the bullying she had experienced through social media. In that case, the perpetrator was only sentenced to a fine of RM100, equivalent to approximately IDR356,700 (Maheza Nurmiagita, 2024). This differs from Indonesia, where no similarly progressive measures have been adopted, as Malaysia has done, in response to cyberbullying cases that have resulted in victims dying by suicide. This can be seen in the tragic case that occurred in 2022 involving a man in Ciledug,

Tangerang City, who died by suicide as a result of cyberbullying. The case attracted public attention, particularly on Twitter, and was associated with allegations of harassment involving the victim (Muhammad Egi Tri Setia, 2024). Bagong Suyanto, a sociologist from Universitas Airlangga, commented that the increasing prevalence of cyberbullying constitutes a problem of the postmodern era. He also highlighted that many victims of harassment prefer to seek justice through social media rather than through legal channels because of trauma and fear of being stigmatised (Muhammad Egi Tri Setia, 2024). In the context of victimology, this phenomenon is referred to as secondary victimisation. This means that victims experience continuing burdens after the initial victimisation, with the criminal justice system often being characterised as a source of secondary victimisation for crime victims (Paripurna, 2021, hlm. 27).

In Indonesia, cyberbullying cases are generally prosecuted on the basis of the Electronic Information and Transactions Law. An examination of Article 45 paragraph (1) in conjunction with Article 27 paragraph (3) of the Electronic Information and Transactions Law indicates that there are at least two forms of insult. The first is defamation or insult (*smaad*), and the second is calumny (*laster*) (Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik). In addition, other provisions may also be applied to cyberbullying, namely Article 45 paragraph (1) in conjunction with Article 27 paragraph (1), where the form of cyberbullying contains content that violates decency and is intended to be publicly accessible (Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik). Furthermore, following the second amendment to the Electronic Information and Transactions Law, two additional forms of conduct may also be applied in cyberbullying cases. The first is attacking another person's honour or reputation, which refers to conduct that degrades or damages another person's reputation or dignity and causes harm to that person, including insult and/or calumny, as regulated under Article 27A of the second amendment to the Electronic Information and Transactions Law (Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik). In principle, there is no fundamental difference between Article 27A and Article 27 paragraph (3) of the Electronic Information and Transactions Law. The second is conduct involving threats of defamation, namely threatening to attack another person's honour or reputation by accusing that person of a particular matter with the intention that it be publicly known (Article 27B (2) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik), as regulated under

Article 27B paragraph (2) of the second amendment to the Electronic Information and Transactions Law.

One of the weaknesses of Indonesia's Electronic Information and Transactions Law is that it does not accommodate all forms of insult as recognised under the Criminal Code. Under Indonesian criminal law, both the former Criminal Code and the National Criminal Code recognise five forms of insult (Hiariej, 2024, hlm. 137-138). First, defamation, which consists of two forms: oral defamation or insult (*smaad*), regulated under Article 310 of the former Criminal Code or Article 433 paragraph (1) of the National Criminal Code; and written defamation or libel (*smaadschrift*), regulated under Article 310 paragraph (2) of the former Criminal Code or Article 433 paragraph (2) of the National Criminal Code. Secondly, calumny (*laster*) is regulated under Article 311 of the former Criminal Code or Article 434 paragraph (1) of the National Criminal Code. Thirdly, minor insult (*eenvoudige belediging*) is regulated under Article 315 of the former Criminal Code or Article 436 of the National Criminal Code. Fourthly, false accusation (*lasterlijke aanklacht*) is regulated under Article 317 of the former Criminal Code or Article 437 of the National Criminal Code. Fifthly, false suspicion (*lasterlijke verdachtmaking*) is regulated under Article 318 of the former Criminal Code or Article 438 of the National Criminal Code. Thus, not all forms of insult are punishable when committed through electronic or cyber media. Furthermore, as of 2 January 2026, the criminal provisions under Article 45 paragraph (1) in conjunction with Article 27 of the Electronic Information and Transactions Law will be repealed and will cease to apply once the National Criminal Code enters into force (Article 622 (1) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional)).

Following the repeal of the criminal provisions under Article 45 paragraph (1) in conjunction with Article 27 paragraph (3), as well as several other criminal provisions in the Electronic Information and Transactions Law, the five forms of insult under the National Criminal Code will also apply where such acts are committed through electronic information systems, with aggravated penalties. This is expressly provided in Article 441 paragraph (1) of the National Criminal Code. Where an act of cyberbullying contains elements that violate decency, it may be prosecuted not only under the Pornography Law but also under Article 407 of the National Criminal Code concerning pornography. Accordingly, in the author's view, the regulation of cyberbullying in Indonesia remains less specific than that in Malaysia and has not yet covered all forms of cyberbullying. In Indonesia, the legal boundaries of cyberbullying remain limited to insult, indecency, and threats. Moreover, one particular form of cyberbullying, namely the so-called "killer finger", has not yet been specifically regulated under statutory law. In fact, this form of cyberbullying has already resulted in the death of a victim, as illustrated by

the case of a man in Ciledug, Tangerang City (Muhammad Egi Tri Setia, 2024). In light of this situation, the question arises: how many more lives must be lost in cyberbullying cases before Indonesian lawmakers enact a specific criminal provision on cyberbullying? Even the National Criminal Code, which will enter into force on 2 January 2026, has not yet succeeded in formulating a specific offence of cyberbullying.

4. Conclusion

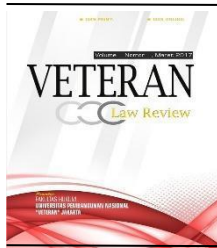
The conception of cyberbullying in Indonesia and Malaysia reveals a significant gap. In Malaysia, the forms of cyberbullying are clearly formulated in statutory law, whereas in Indonesia the regulation remains relatively unspecific. There is also a notable difference in how the two countries have responded to cyberbullying. Malaysia acted promptly by introducing specific provisions on cyberbullying into its Penal Code following a case involving one of its citizens. This differs substantially from Indonesia, where no comparable legal reform has been undertaken despite cyberbullying cases involving Indonesian citizens. In Indonesia, when cyberbullying occurs, law enforcement generally relies on provisions concerning insult, pornography, or threats, as regulated under the Electronic Information and Transactions Law, the Pornography Law, and the National Criminal Code. However, these provisions do not specifically regulate cyberbullying as a distinct criminal offence. By contrast, Malaysia's amended Penal Code has further clarified and strengthened the legal framework governing cyberbullying.

References

- Adiarti, D. I., & Fadhilah, N. (2025). Membangun Ketahanan Digital Remaja Desa: Analisis Kekerasan Seksual Digital Melalui Perspektif Perkembangan Anak Dan Gender. *Jurnal Ilmiah Ilmu Sosial dan Pendidikan*, 3(1).
- Agustina, R., & Purwanto, G. H. (2024). Kejahatan Impersonation terhadap Public Figure dalam Perspektif Undang-Undang Tindak Pidana Kekerasan Seksual (Studi Kasus di Kabupaten Bojonegoro). *Jurnal Pembangunan Hukum Indonesia*, 6(2). <https://doi.org/DOI:https://doi.org/10.14710/jphi.v6i2.315-327>
- Ahmad Razali, N., Nawang, N. I., & Syed Nong Mohamad, S. N. A. (2022). Cyberbullying In Malaysia: An Analysis of the Existing Laws. *International Journal of Law, Government and Communication*, 7(30), 124–135. <https://doi.org/10.35631/IJLGC.730011>
- Amy Dwyer & Patricia Easteal. (2013). Cyber Bullying In Australian Schools the Question of Negligence and Liability. *Alternative Law Journal*, 38(2).

- Anne Wagner. (2019). E-victimization and E-Predation Theory as the Dominant aggressive Communication: The Case of Cyber Bullying. *Social Semiotics*, 29(3). <https://doi.org/10.1080/10350330.2019.1587832>
- B, U., Nn, A., R, F., P, B., & Nn, A. (2018). Student and Teachers Perspective on Cyber-Bullying. *Journal of Forensic Psychology*, 03(01). <https://doi.org/10.4172/2475-319X.1000132>
- Choi, K.-S., Cronin, S., & Correia, H. (2016). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police Practice and Research*, 17(2), 149-159. <https://doi.org/10.1080/15614263.2015.1128161>
- Elpemi, N., & Isro'i, N. F. (2020). Fenomena Cyberbullying Pada Peserta Didik. *IJoCE: Indonesian Journal of Counseling and Education*, 1(1). <https://doi.org/DOI:https://doi.org/10.32923/ijoce.v1i1.1138>
- Emily Zakia. (2025). Lonjakan Statistik Kasus Bullying di Indonesia, Ini Data Setiap Tahunnya! *GoodStats*. <https://goodstats.id/article/data-kasus-bullying-di-indonesia-yG3WL>
- Hadi, A. M. (2025). Tindak Pidana Cyberbullying oleh Anak dalam Perspektif Undang-Undang ITE dan Sistem Peradilan Pidana Anak. *Journal of Law Society and Islamic Civilization (JoLSIC)*, 13(2).
- Hay, C., Meldrum, R., & Mann, K. (2010). Traditional Bullying, Cyber Bullying, and Deviance: A General Strain Theory Approach. *Journal of Contemporary Criminal Justice*, 26(2), 130-147. <https://doi.org/10.1177/1043986209359557>
- Hiariej, E. O. S. (2024). *Prinsip-Prinsip Hukum Pidana Edisi Penyesuaian KUHP Nasional*. Rajawali Pers.
- Info Psikologi. (2024). Apa Itu Denigration? Ini Definisi dan Dampaknya bagi Korban. *Kumparan*. <https://kumparan.com/info-psikologi/apa-itu-denigration-ini-definisi-dan-dampaknya-bagi-korban-2288Irl5TR>
- Kiki Safitri & Dani Prabowo. (2025). 48 Persen Anak Jadi Korban Cyberbullying, Menkomdigi: Sulit Terdeteksi. *Kompas.com*. <https://nasional.kompas.com/read/2025/07/04/17292961/48-persen-anak-jadi-korban-cyberbullying-menkomdigi-sulit-terdeteksi>
- Langos, C. (2015). Cyberbullying: The Shades of Harm. *Psychiatry, Psychology and Law*, 22(1), 106-123. <https://doi.org/10.1080/13218719.2014.919643>
- Laws of Malaysia Act A1750 Penal Code (Amendment) Act 2025.
- Maheza Nurmiagita. (2024). Influencer Malaysia Bunuh Diri karena Tak Tahan Di-bully di Media Sosial, Pelakunya Cuma Didenda Rp 300 Ribuan. *Liputan 6*. <https://www.liputan6.com/lifestyle/read/5817058/influencer-malaysia-bunuh-diri-karena-tak-tahan-di-bully-di-media-sosial-pelakunya-cuma-didenda-rp300-ribuan>

- Marija Draganic, Snežana Grbovic, & Antoaneta Adžić Zec'evic. (2024). , et al., "The Incidence and Forms of Cyberbullying and the Connection Between Cyberbullying and Self-Esteem Among High School Students in Montenegro", Sage Journals, 2024, hlm. 3. *Sage Journals*. <https://doi.org/10.1177/21582440241239124>
- Mona O'Moore. (2012). Cyber-Bullying: The Situation in Ireland. *Pastoral Care in Education*, 30(3). <https://doi.org/10.1080/02643944.2012.688065>
- Muhammad Dani Ihkam & I Gusti Ngurah Parwata. (2016). Tindak Pidana Cyber Bullying Dalam Perspektif Hukum Pidana di Indonesia. *Jurnal Kertha Wicara*, 9(11).
- Muhammad Egi Tri Setia. (2024). Killer Finger: Slowly and Quietly. *Yayasan Pulih*. <https://www.yayasanpulih.org/our-resources/article/Killer-Finger-Slowly-and-Quietly>
- Muhammad Yasin & Norman Edwin Elnizar. (2019). Cyberbullying, Pelajaran dari Kasus Amanda Todd. *Hukum Online*. <https://www.hukumonline.com/berita/a/icyberbullying-i--pelajaran-dari-kasus-amanda-todd-lt5cd3dc51893bd/>
- Nancy E. Willard. (2007). *Cyberbullying And Cyberthreats: Responding to The Challenge Of Online Social Aggression, Threats, And Distress*. Research Press.
- Nazli bin Ismail. (2025). *Legal Professional Ethics in the Digital Era: Challenges and Transformations*.
- Paripurna, A. (2021). *Viktimologi dan Sistem Peradilan Pidana*. Deepublish.
- Patchin, J. W., & Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148-169. <https://doi.org/10.1177/1541204006286288>
- Phintraco Group. (2023). Cyber Threat: Pengertian, Jenis, dan Cara Mengatasinya. *Blogspot*. <https://phintraco.com/cyber-threat/>
- Sidauruk, J., Gultom, M. H., & Silalahi, K. A. P. (2024). Perspektif Hukum Pidana terhadap Fenomena Cyberbullying di Media Sosial. *Jurnal Hukum De' Rechtsstaat*, 10(2).
- Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, 24(6), 367-376. <https://doi.org/10.1089/cyber.2020.0253>
- Titania Nurrahim. (2019). 7 Perundungan Siber di Medsos. *Indonesiabaik.id*. https://indonesiabaik.id/motion_grafis/7-perundungan-siber-di-medsos#:~:text=Keenam%2C%20exclusion%20atau%20pengucilan%2C%20adalah,dari%20grup%20daring%20secara%20sengaja
- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional), Legislation Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842.



Veteran Law Review

Volume: 9

Issue: 1

P-ISSN: 2655-1594

E-ISSN: 2655-1608

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Windy Freska. (2023). *Bullying dan Kesehatan Mental Remaja*. Mitra Edukasi Negeri.