

Comparative Law Between Indonesia And Malaysia In The Resolution Of Cyberbullying Crimes

Afifah Nur Rahmawati, Aditya Wiguna Sanjaya

Fakulta Hukum, Universitas Negeri Surabaya

email*: 24131585008@mhs.unesa.ac.id

Abstract

The development of information technology has given rise to various forms of cybercrime, one of which is cyberbullying, which is increasingly prevalent in society. The main problem of this research is how the legal regulations between Indonesia and Malaysia differ in resolving cyberbullying crimes. The purpose of this study is to analyze the similarities, differences, and effectiveness of the legal systems of both countries in providing legal protection to victims. The research method used is a normative-comparative approach by examining the laws and regulations in force in Indonesia, such as the Criminal Code and the Electronic Information and Transactions Law (UU ITE), as well as laws in Malaysia through the Communications and Multimedia Act 1998 and the Personal Data Protection Act. Supporting data is taken from reports of cyberbullying cases in Indonesia and Malaysia in 2024–2025. The results show that Indonesia has a broader legal scope with severe criminal penalties, but its weaknesses lie in the formulation of articles that are open to multiple interpretations and ineffective implementation. In contrast, Malaysia has more specific regulations with practical reporting mechanisms and strong personal data protection, although the criminal sanctions are relatively light. Thus, it can be concluded that Indonesia has a normative advantage, while Malaysia has a practical advantage in addressing cyberbullying.

Keywords: Cyberbullying, Comparison Of Indonesian And Malaysian Law.

Abstrak

Perkembangan teknologi informasi telah memunculkan berbagai bentuk kejahatan siber, salah satunya cyberbullying yang kian marak di masyarakat. Pokok permasalahan penelitian ini adalah bagaimana perbedaan pengaturan hukum antara Indonesia dan Malaysia dalam menyelesaikan tindak pidana cyberbullying. Tujuan dari penelitian ini adalah untuk menganalisis persamaan, perbedaan, serta efektivitas sistem hukum kedua negara dalam memberikan perlindungan hukum kepada korban. Metode penelitian yang digunakan adalah pendekatan normatif-komparatif dengan menelaah peraturan perundang-undangan yang berlaku di Indonesia, seperti KUHP dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta hukum di Malaysia melalui Communications and Multimedia Act 1998 dan Personal Data Protection Act. Data pendukung

diambil dari laporan kasus cyberbullying di Indonesia dan Malaysia pada tahun 2024–2025. Hasil penelitian menunjukkan bahwa Indonesia memiliki cakupan hukum yang lebih luas dengan ancaman pidana yang berat, namun kelemahannya terletak pada rumusan pasal yang multitafsir dan implementasi yang belum efektif. Sebaliknya, Malaysia memiliki pengaturan yang lebih spesifik dengan mekanisme pelaporan yang praktis dan perlindungan data pribadi yang kuat, meskipun sanksi pidananya relatif ringan. Dengan demikian, dapat disimpulkan bahwa Indonesia unggul secara normatif, sedangkan Malaysia lebih unggul secara praktis dalam upaya penyelesaian tindak pidana cyberbullying.

Kata Kunci : Cyberbullying, perbandingan hukum Indonesia dan Malaysia

INTRODUCTION

Law enforcement can be interpreted as an effort and endeavor to respect and comply with the norms and rules contained in the existing legislation.¹ Law enforcement is also closely related to the series of procedural laws, one of which is evidence. Evidence is a series of processes that ensures that the actions taken by the defendant have violated substantive law to be assessed and judged by the judge in court to render a decision. The procedures for conducting evidence have also been regulated in the legislation that encompasses the methods, procedures, and mechanisms that must be fulfilled by each party in court.²

In the realm of conventional crime, the process of proof typically relies on physical evidence, witness testimony, or real documents. However, as digital technology has evolved, the legal world faces new challenges with the emergence of cybercrime. This type of offense has different characteristics from ordinary crime, as it is committed through the internet by utilizing technological devices. Its forms and modus operandi are also very diverse, ranging from the theft of personal data, online fraud, system hacking, to the dissemination of illegal content.

Among the various types of cyber crimes, one increasingly prevalent phenomenon that has serious impacts is cyberbullying. Unlike traditional bullying that occurs in physical spaces, cyberbullying takes place in digital spaces that are often difficult to define. Through social media, instant messaging apps, and other online platforms, perpetrators can easily carry out intimidation, insults, or the spread of slander against victims. This situation poses significant challenges for law enforcement, as the evidence

¹ Zainab Ompu Jainah, “Penegakan Hukum Dalam Masyarakat,” *Journal of Rural and Development*, 2012.

² Risma Savhira D.L., Alaika M. Bagus Kurnia PS Alaika, and Dhomirotul Firdaus, “Called Al-Quran Digital Perspective; Answer To Raising Hoax In Era Of Disruption,” *Tribakti: Jurnal Pemikiran Keislaman* 31, no. 2 (2020): 237–252.

left behind is often in the form of digital footprints that require special expertise to verify.³

Cyberbullying can be defined as aggressive behavior that utilizes electronic devices and technology with the aim of making others uncomfortable and disturbed.⁴ Cyberbullying is a part of cybercrime. In today's modern era, cybercrime is increasingly rampant with incidents such as online fraud, fake checks, carding, hijacking, pornography, and others including cyberbullying. This action is carried out by irresponsible individuals repeatedly using malicious words to insult, threaten, and defame the victim.⁵ The role of the state in providing legal protection for victims of cyberbullying is important to establish legislation that ensures legal protection both preventively and repressively.

Cyberbullying or online harassment has become an increasingly real issue in Indonesia, especially among children and teenagers. According to research by Indonesia Indicator titled Trends in Digital Violence against Children, from January 1 to July 21, 2024, there were 24,876 posts containing digital violence against children on social media, with an engagement of 3,004,014 times.⁶ Among the various types of digital violence, bullying or harassment (including cyberbullying) has become the most common issue, followed by pedophilia, online fraud, doxxing, and cyberstalking.

In addition, surveys and government data show that cyberbullying occurs not only openly on social media but also in private spaces such as personal conversations or friend groups, which makes it difficult to detect and report. For example, in July 2025, the Minister of Communication and Digital (Menkomdigi) Meutya Hafid mentioned that 48 percent of children who had ever used the internet admitted to experiencing cyberbullying.⁷

The high prevalence is also related to the characteristics of technology use among the youth: a relatively high internet penetration, access to social media, and a lack of digital literacy in several age groups. Data from the KBGO (Gender-Based Online Violence) study in the first quarter of 2024 indicates an increase of 118 cases compared

³ Yandri Setia Bakti, "Differential Association Pada Remaja (Studi Kasus Pada Remaja Yang Terpengaruh Dunia Gemerlap Dugem Di Kota Dumai)," *Jom Fisip* 5 (2018): 1–15.

⁴ Aini silvi Nurrahmatin, "Studi Pustaka Pemicu Cyberbullying" (n.d.).

⁵ Yuliana Surya Galih, "Yuridiksi Hukum Pidana Dalam Dunia Maya" 7, no. 1 (2019): 59–74.

⁶ Nadila Salsabila and Untung Sumarwan, "Analisis Cyberbullying Pada Masa Pilpres 2024 Berdasarkan Social Bonds Theory" 6, no. 4 (2024): 669–679.

⁷ Kiki Safitri and Danu Damarjati, "Menkomdigi: 48 Persen Anak Pengguna Internet Mengalami Perundungan Online," *Kompas.Com*, last modified 2025, https://nasional.kompas.com/read/2025/07/04/17354401/menkomdigi-48-persen-anak-pengguna-internet-mengalami-perundungan-online?utm_source=chatgpt.com.

to the same period last year, with the majority of victims aged 18-25, followed by victims under 18.

In Indonesia, to reduce the level of cyberbullying, there are several regulations that prohibit acts of cyberbullying in the Criminal Code & Law No. 19 of 2016 amending Law No. 11 of 2008 concerning Information and Electronic Transactions. In article 310 paragraph (1), it is stated that anyone who deliberately commits acts of defamation or tarnishes someone's honor by insulting a matter to be known publicly may be punished by imprisonment for 9 (nine) months.

Throughout the year 2024, Malaysia recorded a significant surge in cyberbullying cases. Data from the Malaysian Communications and Multimedia Commission (MCMC) indicates that there were 8,399 reports received until November, averaging 27 reports per day. In response, MCMC removed more than 8,700 pieces of content related to cyberbullying, a sharp increase compared to 2023, which had only around 1,700 pieces of content. The relevant ministry also emphasized that reported cases have drastically increased from 326 in 2021 to over 6,500 cases in 2024.⁸ This phenomenon primarily involves young people, with about 70 percent of the cyberbullying content handled relating to high school students.

As we enter 2025, the threat of cyberbullying remains high and requires special attention. An Ipsos survey reveals that nearly a quarter of parents in Malaysia state that their children have been victims of online bullying, while nearly half of others are aware of similar cases in their surroundings. This situation indicates that cyberbullying is not just an individual issue but a social problem that has widespread effects, with the majority of victims coming from the adolescent age group. Malaysia indeed does not yet have specific regulations governing this crime. Currently, matters related to cyberbullying are regulated under the Communications and Multimedia Act 1998.⁹ This makes the main challenge for Malaysia ahead to strengthen digital literacy, increase parental awareness, and tighten regulations on child protection so that the digital space becomes a safer environment.

Based on the description of the problem above, the author intends to conduct further research and analyze the comparison of regulations in Indonesia and Malaysia regarding cyberbullying offenses and the elements contained within them. Therefore, this research is titled "A Comparative Study of Law Between Indonesia and Malaysia in the Resolution of Cyberbullying Crimes".

⁸ Ivan Loh, "Cyberbullying Cases Involving Youth See Significant Increase, Says Noraini Ahmad," *The Star*.

⁹ M Raihan Nafis, "Studi Perbandingan Hukum Tentang Pengaturan Tindak Pidana CyberBullying DiIndonesia, Singapura Daan Malaysia," 2023.

RESEARCH METHODS

This research uses a normative legal method with a comparative approach. The normative legal method is chosen because the focus of the research is on the analysis of the applicable laws in Indonesia and Malaysia, especially related to the regulation of cyberbullying crimes. The comparative approach is used to compare the legal substance, criminal sanctions, and victim protection mechanisms in both countries.

The data used in this research consists of secondary data, including primary legal materials (the Criminal Code, Law Number 11 of 2008 on Electronic Information and Transactions and its amendments, the Communications and Multimedia Act 1998, and the Personal Data Protection Act), secondary legal materials (literature, journals, previous research findings, and official news), and tertiary legal materials (legal dictionaries and encyclopedias).

Data collection techniques were carried out through library research, while data analysis used descriptive qualitative analysis, namely by outlining the content of legal norms, comparing legislation in Indonesia and Malaysia, and drawing conclusions about the advantages and disadvantages of each legal system in handling cyberbullying offenses.

RESULTS AND DISCUSSION

Humans are dynamic beings who continuously change in accordance with the development of the times, and to this day, there has been an evolution in behavior patterns and also in human thinking towards a more modern direction. This development is accompanied by a sense of curiosity that ultimately drives the creation and innovation of new things that can support daily life. This development certainly also occurs within the scope of information technology, where if it is not controlled, it can lead to conflicts between groups, loss of life, and even instability in a nation. Therefore, the law must be present and play a strategic role in regulating information technology along with telecommunications to prevent the rise of cybercrime.¹⁰

One of the forms of cybercrime that has become a prevalent problem in society is violence or insult through electronic media or cyberbullying. This term refers to actions that intentionally use information technology and communication tools continuously, aimed at causing harm to others through intimidatory actions, threats, and insults, in order to provoke conflicts between individuals or with certain groups. The term cyberbullying originates from two words, namely cyber and bullying. Cyber refers to an

¹⁰ Firdaus Muhamad Iqbal, "Kontribusi Sistem Civil Law (Eropa Kontinental) Terhadap Perkembangan Sistem Hukum Di Indonesia," *Jurnal Dialektika Hukum* 4, no. 2 (2022): 180–200.

electronic network system that connects one user with another, for example, the internet. Meanwhile, bullying is an aggressive act manifested in the form of abuse, both physically and verbally.

Bullying actions are generally aimed at specific individuals based on ethnicity, religion, race, gender, sexual orientation, or personal abilities. Cyberbullying itself is an extension of bullying behavior that follows technological developments, where perpetrators spread gossip or negative information about someone on the internet. This information can include hate speech or matters related to the victim's personal identity, which can cause embarrassment and tarnish their reputation.¹¹

Some experts provide definitions regarding cyberbullying as follows:

Olweus (1993) defines bullying as aggressive actions that are carried out repeatedly over time by an individual or group that holds greater power than the victim.¹² This definition was then adapted by Hinduja and Patchin (2009) as well as Smith and colleagues (2008), who explain that cyberbullying is a form of intense and repeated aggressive behavior, carried out by an individual or group using technology and electronic media as a means to hurt or attack specific individuals.¹³

Kowalski (2008) states that cyberbullying is a type of bullying that occurs through digital media such as instant messaging, email, chat rooms, websites, video games, as well as through images or messages sent via mobile phones.¹⁴ Cyberbullying falls into the category of verbal and non-verbal bullying that occurs by utilizing electronic devices such as computers or mobile phones, for example, sending hate messages, uttering hurtful words during online conversations, or spreading false information about someone on the internet. Ignoring someone in a chat room or mocking them through social media also falls into this behavior. In general, cyberbullying is an act of misuse of information technology that is done intentionally, repeatedly, and is harmful to hurt or harass others.

According to Willard (2007), there are several forms of cyberbullying, including: flaming (sending angry messages), harassment (abuse or disturbance), denigration (slandering), impersonation (pretending to be someone else), outing (leaking personal

¹¹ Fitria Aulia Imani, Ati Kusmawati, and H. Moh. Tohari Amin, "Pencegahan Kasus Cyberbullying Bagi Remaja Pengguna Sosial Media," *KHIDMAT SOSIAL: Journal of Social Work and Social Services* 2, no. 1 (2021): 74–83.

¹² Muhammad Fajar Shidiqi and Veronika Suprapti, "Pemaknaan Bullying Pada Remaja Penindas (The Bully)," *Jurnal Psikologi Kepribadian dan Sosial* 2, no. 2 (2013): 93, <http://journal.unair.ac.id/download-fullpapers-jpkds3ed32a0002full.pdf>.

¹³ Muhammad Alam Akbar and Prahastiwi Utari, "Cyberbullying Pada Media Sosial" (n.d.): 1–20.

¹⁴ Imani, Kusmawati, and Amin, "Pencegahan Kasus Cyberbullying Bagi Remaja Pengguna Sosial Media."

information), trickery (deception), exclusion (excluding others), and cyberstalking (behavior of stalking or terrorizing online).¹⁵ Meanwhile, research by Price and Dalgleish (2009) revealed that the types of cyberbullying that occur frequently include name-calling, abusive comments, rumor spreading, threatened physical harm, being ignored or excluded, opinion slammed, online impersonation, sending upsetting images, and spreading images of the victim.¹⁶

In the scope of the legal system in Indonesia, efforts to combat cyberbullying are regulated through the Criminal Code (KUHP) and Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). On the other hand, according to Clara S.A.T, Soponyono, and Astuti (2016), the penal provisions found in both regulations are considered to still have many weaknesses in effectively addressing and enforcing cyberbullying cases. In the KUHP itself, the provisions deemed relevant for regulating cyberbullying offenses are outlined in Chapter XVI concerning defamation, specifically in Articles 310 paragraphs (1) & (2).¹⁷

In verse (1) it is explained that anyone who intentionally damages the dignity or reputation of someone through certain accusations intended to be known by the public can be subject to criminal defamation, with a maximum prison sentence of nine months or a maximum fine of four thousand five hundred rupiahs.

Conversely, paragraph (2) specifies that if the defamation occurs through writings or images that are shared, shown, or posted in public areas, the offender may face criminal charges for written defamation, with a maximum prison sentence of 1 year and 4 months or an equivalent fine.

Regarding cyberbullying, the provisions are stated in the Law on Information and Electronic Transactions (ITE Law) along with its amendments, specifically in Article 27 paragraph (3). The article stipulates that anyone who intentionally or without authorization disseminates, sends, or allows traceable electronic information or documents containing elements of ridicule and/or defamation can be subject to criminal penalties.¹⁸

Indonesia has several legal foundations in the form of legislation that can address acts of cyberbullying. Under the ITE Law, acts of cyberbullying are subject to heavier

¹⁵ Ipah Saripah and Ajeng Nurul Pratita, "Kecenderungan Perilaku Cyberbullying Peserta Didik Berdasarkan Jenis Kelamin," *Pedagogia* 16, no. 3 (2018): 180.

¹⁶ Ibid.

¹⁷ Irfan Arief Kurniawan, Hadi Mahmud, and Nourma Dewi, "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang - Undang No. 11 Tahun 2008," *Jurnal Inovasi Penelitian* 2, no. 2 (2021): 1-7.

¹⁸ Julio Lasamahu, Margie Gladies Sopacua, and Astuti Nur Fadillah, "Kajian Yuridis Kejahatan Cyber Bullying Di Media Sosial," *SANISA: Jurnal Kreativitas Mahasiswa Hukum* 5, no. 1 (2025): 1.

penalties because they are considered serious crimes as outlined in the following Articles:

1. 1. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), Article 45 paragraph (1), which states that anyone who acts in accordance with what is stipulated in Article 27 paragraph (1), paragraph (3), and paragraph (4) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000 (one billion rupiah).
2. 2. Law Number 11 of 2008 concerning ITE Article 45 paragraph (2) states that a person who acts in accordance with what is stipulated in Article 28 paragraph (2) is punished with a maximum prison sentence of 6 (six) years and/or a fine of up to Rp1,000,000,000 (one billion rupiah).
3. 3. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) Article 45 paragraph (3) states that anyone who acts as referred to in Article 29 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of IDR 2,000,000,000 (two billion rupiah).

As one of the Commonwealth countries, Malaysia's legal system also utilizes the common law system. However, there are differences in its implementation in Malaysia, considering that the majority of Malaysians practice Islam. Therefore, the common law rooted in England is applied alongside the Islamic law practiced in Malaysia.¹⁹

Malaysia has not yet formulated specific legislation regulating cyberbullying. This is similar to Indonesia, which incorporates cyberbullying offenses into general law within the telecommunications sector. In fact, Malaysia has been discussing the formulation of such legislation since 2017. However, until now, cyberbullying cases are handled and tried using the Communications and Multimedia Act 1998 as follows:²⁰

1. Section 233 of the Communications and Multimedia Act (1998)

Regulating the misuse of network services, particularly when someone uses the internet to deliver comments, requests, suggestions, or other types of communication that are obscene, indecent, false, threatening, or harmful. If such communication is carried out with the intention of disturbing, harassing, threatening, or abusing others, it constitutes a legal violation. The perpetrator may be subject to a maximum fine of RM 50,000 and imprisonment for up to one year. In addition, if the violation continues after the sentence period ends, the perpetrator may also be subject to an additional fine of RM 1,000 for each day the violation persists.

¹⁹ Miko Aditiya Suharto and Maria Novita Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risalah Hukum* 17 (2021): 98–107.

²⁰ Sigit Somadiyono, "Perbandingan Sistem Hukum Antara Indonesia Dan Malaysia," *Wajah Hukum* 4, no. 2 (2020): 414.

The Malaysian government regulates matters related to cyberbullying crimes along with protections through several arrangements. This is certainly aimed at providing a sense of security for citizens to avoid cyberbullying and also a sense of justice for victims who experience harassment in the virtual world. Various efforts are carried out by the Malaysian government in addressing cyberbullying, including:²¹

a. *Communication And Multimedia Act (1998)*

The Communication and Multimedia Act 1998 serves as an umbrella regulation for all activities in the communication and multimedia sector in Malaysia. Article 233 stipulates that anyone who engages in acts of an indecent or false nature, through threats, or deliberately provokes others to feel disturbed or threatened via the internet can be subject to criminal penalties.

b. *Personal Data Protection Act*

Malaysia also has laws regarding the protection of personal data as a form of protection and security, as well as prevention against cyberbullying actions involving personal data of protected subjects that have been misused by certain individuals..

c. *Reporting Mechanism to MCMC Complaint Portal*

Malaysia has a website for submitting complaints related to communication and multimedia, which can be accessed at aduan.skm.gov.my, where one can report posts or uploads on social media that are perceived to harm the reporter as a victim.

In the Communication and Multimedia Act 1998, various types classified as cyberbullying activities are included:

a. *Article 233 of the Communication and Multimedia Act (1998)*

Explains that anyone who uses the internet network and intentionally acts, informs, comments, or engages in other types of communication containing obscene, false, threatening, offensive elements, or with the intent to cause harm, misuse, threaten, or harass certain individuals or groups may be subject to criminal penalties, namely a maximum imprisonment of 1 year and a maximum fine of RM 50,000.²²

Each country has its own regulatory elements in managing cyberbullying crimes. However, there is a common deficiency that exists in both countries, namely the scope

²¹ Jocelyn Valerie et al., "Melawan Bullying: Perbandingan Uu Antarnegara Dan Pemanfaatan Aplikasi Pelaporan Di Sekolah" 1, no. 3 (2024): 3063–7821.

²² Viva Budy Kusnandar, "ITU: Keamanan Siber Indonesia Kalah Dari Singapura Dan Malaysia," *Databoks*, last modified 2022, <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/7a3f7ed8aabdb4f/itukeamanan-siber-indonesiakalah-dari-singapura-dan-malaysia>.

of actions that can be classified as cyberbullying. When compared, the differences are as follows:²³

1 Legal Substance

Indonesia, through the ITE Law (Law No. 11 of 2008 in conjunction with Law No. 19 of 2016), regulates cyberbullying, particularly in Article 27 paragraph (3) concerning defamation, with very severe criminal penalties (up to 6 years in prison and a fine of IDR 1 billion, and even up to 12 years in prison for Article 29). However, its weakness lies in the formulation of the articles, which are general and open to multiple interpretations. The ITE Law does not explicitly use the term "cyberbullying," instead categorizing it under defamation, insult, or the dissemination of content containing hate. As a result, this broad scope often creates legal uncertainty and is even prone to being misused to restrict freedom of expression.

Malaysia, through the Communications and Multimedia Act 1998 (Section 233), regulates cyberbullying more specifically in the context of network misuse. Its formulation emphasizes communication that is "obscene, false, threatening, or harmful." Although it is clearer in terms of terminology, its drawback lies in the limited scope: only four main categories (harassment, flaming, cyberstalking, denigration). Compared to Indonesia, which covers more forms (impersonation, outing, trickery, etc.), Malaysia still has minimal variation in the elements of actions.

Indonesia excels in the scope of criminal acts, but is weak in the clarity of formulation. Malaysia is the opposite: clearer and more focused, but still limited in regulating actions.

2 Criminal Sanctions

Indonesia imposes severe criminal penalties (up to 12 years in prison and fines of billions of rupiah). This approach emphasizes that cyberbullying is taken seriously. However, in practice, law enforcement is often disproportionate, as many minor cases (such as rude comments) are met with heavy sanctions, which has led to criticism from civil society.

Malaysia only imposes a maximum prison sentence of 1 year and a fine of RM 50,000 (around IDR 165 million), with an additional daily fine of RM 1,000 if the violation continues. This punishment is considered light and poses a low

²³ Che Audah Hassan et al., "Theoretical Perspectives on Electronic Monitoring and Police Supervision Order as Crime Prevention Modalities in Malaysia," *International Journal of Academic Research in Business and Social Sciences* 12, no. 11 (2022): 144–154.

risk of deterrence. However, this flexibility makes Malaysian law more realistic and not excessive when faced with cases of minor cyberbullying.

Indonesia emphasizes deterrence through heavy penalties but tends to be repressive. Malaysia emphasizes proportionality, but the threats are too light for serious cases, such as cyberstalking that leads to the victim's suicide.

3 Victim Protection

Indonesia already has legal instruments for victim protection through the Witness and Victim Protection Act. Victims' rights such as confidentiality of identity, legal assistance, and even compensation are available. However, in practice, protection is more focused on general criminal cases (such as murder, terrorism), while cyberbullying cases are often not considered a priority. Furthermore, there is no specific reporting mechanism for cyberbullying, so victims have to go through the police channels, which tend to be complicated.

Malaysia stands out more in terms of accessibility and reporting mechanisms. Through the MCMC Complaint Portal, the public can directly report content containing cyberbullying. Coupled with the Personal Data Protection Act, Malaysia emphasizes preventing the leakage of victims' personal data. With this approach, Malaysia appears more proactive in both preventive and remedial measures, providing quick access for victims to remove content or protect their privacy.

Indonesia excels in the legal framework for victim protection (more comprehensive), but is weak in implementation. Malaysia excels in practical reporting mechanisms and data protection, although its legal basis is still limited.

4 Effectiveness of the Legal System

In Indonesia, the main problem lies in law enforcement. Many cases of cyberbullying go unreported because victims feel the process is complicated or fear that they might instead be counter-sued under other charges (such as defamation). Meanwhile, cases that are prosecuted are often selective and give an impression of discrimination.

Although Malaysia has relatively mild criminal penalties, it is more consistent in providing easily accessible reporting channels for the public. This mechanism contributes to an increase in the number of case reports (for example, in 2024, there were more than 8,399 reports). This means that the public has a higher awareness because its legal system allows room for public participation.

In terms of effectiveness, Malaysia is superior due to its simple and transparent reporting channels, while Indonesia is still hindered by bureaucracy and limited public trust in law enforcement officials.

CONCLUSION

Based on the research findings that have been reviewed and analyzed, it can be concluded that:

1. Indonesia uses the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) with a broad scope of criminal acts and severe penalties of up to 12 years in prison as well as fines worth billions of rupiah. However, its weakness lies in the articles being open to multiple interpretations, which can potentially create legal uncertainty. Malaysia, through the Communications and Multimedia Act 1998 and the Personal Data Protection Act, regulates cyberbullying more specifically with relatively mild sanctions (maximum 1 year in prison and a fine of RM 50,000). Thus, Indonesia emphasizes deterrent effects, while Malaysia emphasizes proportionality.
2. Indonesia has a more comprehensive normative legal framework for victim protection, but its implementation is still weak and reporting channels are often complicated. In contrast, Malaysia excels in practical mechanisms through the MCMC Complaint Portal as well as personal data protection, making the reporting system more accessible to the public. This indicates that Indonesia is superior in the normative aspect, whereas Malaysia is more effective in practical aspects and accessibility.

REFERENCES

- Akbar, Muhammad Alam, and Prahastiwi Utari. "Cyberbullying Pada Media Sosial" (n.d.): 1–20.
- Bakti, Yandri Setia. "Differential Association Pada Remaja (Studi Kasus Pada Remaja Yang Terpengaruh Dunia Gemerlap Dugem Di Kota Dumai)." *Jom Fisip* 5 (2018): 1–15. <https://ejournal.undiksha.ac.id/index.php/JJPBS>.
- Budy Kusnandar, Viva. "ITU: Keamanan Siber Indonesia Kalah Dari Singapura Dan Malaysia." *Databoks*. Last modified 2022. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/7a3f7ed8aabdb4f/itukeamanan-siber-indonesiakalah-dari-singapura-dan-malaysia>.
- Galih, Yuliana Surya. "Yuridiksi Hukum Pidana Dalam Dunia Maya" 7, no. 1 (2019): 59–74.
- Hassan, Che Audah, Ahmad Ridhwan Abd Rani, Habibah Omar, Ashran Haji Idris, and

- Suzaini Mohd Saufi. "Theoretical Perspectives on Electronic Monitoring and Police Supervision Order as Crime Prevention Modalities in Malaysia." *International Journal of Academic Research in Business and Social Sciences* 12, no. 11 (2022): 144–154.
- Imani, Fitria Aulia, Ati Kusmawati, and H. Moh. Tohari Amin. "Pencegahan Kasus Cyberbullying Bagi Remaja Pengguna Sosial Media." *KHIDMAT SOSIAL: Journal of Social Work and Social Services* 2, no. 1 (2021): 74–83. <https://jurnal.umj.ac.id/index.php/khidmatsosial/article/view/10433>.
- Iqbal, Firdaus Muhamad. "Kontribusi Sistem Civil Law (Eropa Kontinental) Terhadap Perkembangan Sistem Hukum Di Indonesia." *Jurnal Dialektika Hukum* 4, no. 2 (2022): 180–200.
- Kurniawan, Irfan Arief, Hadi Mahmud, and Nourma Dewi. "Penyebaran Virus Ransomware Wannacry Berdasarkan Undang - Undang No. 11 Tahun 2008." *Jurnal Inovasi Penelitian* 2, no. 2 (2021): 1–7.
- Lasamahu, Julio, Margie Gladies Sopacua, and Astuti Nur Fadillah. "Kajian Yuridis Kejahatan Cyber Bullying Di Media Sosial." *SANISA: Jurnal Kreativitas Mahasiswa Hukum* 5, no. 1 (2025): 1.
- Loh, Ivan. "Cyberbullying Cases Involving Youth See Significant Increase, Says Noraini Ahmad." *The Star*.
- Nafis, M Raihan. "Studi Perbandingan Hukum Tentang Pengaturan Tindak Pidana CyberBullying DiIndonesia, Singapura Daan Malaysia," 2023.
- Nurrahmatin, Aini silvi. "Studi Pustaka Pemicu Cyberbullying" (n.d.).
- Ompu Jainah, Zainab. "Penegakan Hukum Dalam Masyarakat." *Journal of Rural and Development*, 2012.
- Safitri, Kiki, and Danu Damarjati. "Menkomdigi: 48 Persen Anak Pengguna Internet Mengalami Perundungan Online." *Kompas.Com*. Last modified 2025. https://nasional.kompas.com/read/2025/07/04/17354401/menkomdigi-48-persen-anak-pengguna-internet-mengalami-perundungan-online?utm_source=chatgpt.com.
- Salsabila, Nadila, and Untung Sumarwan. "Analisis Cyberbullying Pada Masa Pilpres 2024 Berdasarkan Social Bonds Theory" 6, no. 4 (2024): 669–679.
- Saripah, Ipah, and Ajeng Nurul Pratita. "Kecenderungan Perilaku Cyberbullying Peserta Didik Berdasarkan Jenis Kelamin." *Pedagogia* 16, no. 3 (2018): 180.
- Savhira D.L., Risma, Alaika M. Bagus Kurnia PS Alaika, and Dhomirotul Firdaus. "Called Al-Quran Digital Perspective; Answer To Raising Hoax In Era Of Disruption." *Tribakti: Jurnal Pemikiran Keislaman* 31, no. 2 (2020): 237–252.
- Shidiqi, Muhammad Fajar, and Veronika Suprpti. "Pemaknaan Bullying Pada Remaja Penindas (The Bully)." *Jurnal Psikologi Kepribadian dan Sosial* 2, no. 2 (2013): 93.

JSH

Supremasi Hukum: Jurnal Penelitian Hukum

P-ISSN: 1693-766X ; E-ISSN: 2579-4663, Vol. 34, No 2, Agustus 2025, 123-136

<https://ejournal.unib.ac.id/supremasihukum/index>

DOI: <https://doi.org/10.33369/jsh.34.2.123-136>

<http://journal.unair.ac.id/download-fullpapers-jpk3d3ed32a0002full.pdf>.

Somadiyono, Sigit. "Perbandingan Sistem Hukum Antara Indonesia Dan Malaysia."

Wajah Hukum 4, no. 2 (2020): 414.

Suharto, Miko Aditiya, and Maria Novita Apriyani. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum* 17 (2021): 98–107.

Valerie, Jocelyn, Sri Pudjiastuti, Sekolah Menengah Atas Swasta Witama Nasional Plus Pekanbaru, and Guru Pembimbing. "Melawan Bullying: Perbandingan Uu Antarnegara Dan Pemanfaatan Aplikasi Pelaporan Di Sekolah" 1, no. 3 (2024): 3063–7821.