

## A Comparative Legal Analysis of Cyberbullying Among Children on TikTok in Indonesia and Singapore

Submitted 8 March 2026, Revised 10 July 2026, Accepted 30 July 2026, Published 9 August 2026

Bintang Mas Wahyu Esa Suryo Alif<sup>1</sup>, Nabilla Desyalika Putri<sup>2</sup>

<sup>1,2</sup>Faculty of Law, State University of Surabaya, Surabaya, Indonesia

Email Corresponding Author: [bintang.23649@mhs.unesa.ac.id](mailto:bintang.23649@mhs.unesa.ac.id)

DOI: <https://doi.org/10.35879/jik.v20i2.725>

### Abstract

The rapid growth of algorithm-driven platforms such as TikTok has expanded children's opportunities for interaction while intensifying risks of cyberbullying, including insults, threats, doxxing, stalking, and other digital harassment. In Indonesia, protection is dispersed across the ITE Law, Criminal Code, and Child Protection Law, leaving no dedicated framework that comprehensively defines child cyberbullying or regulates prevention, response, and recovery. This study compares Indonesia and Singapore in defining, preventing, and responding to child cyberbullying on TikTok and assesses how Indonesia can strengthen regulation within the ASEAN framework. Using normative legal research with legislative and comparative approaches, the study finds that Indonesia has legal bases for addressing cyberbullying but relies on a fragmented, offence-based model. Singapore adopts a more integrated and victim-focused approach through the Protection from Harassment Act 2014 and the Online Safety (Relief and Accountability) Act 2025, covering harassment, doxxing, stalking, image-based child abuse, and impersonation. Indonesia meets several standards under the ASEAN Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse, but implementation gaps remain. Indonesia should harmonise definitions, strengthen specialised institutions and reporting systems, improve victim recovery and digital literacy, and increase platform accountability.

**Keywords:** cyberbullying, TikTok, Indonesia, Singapore, child protection, online safety regulation

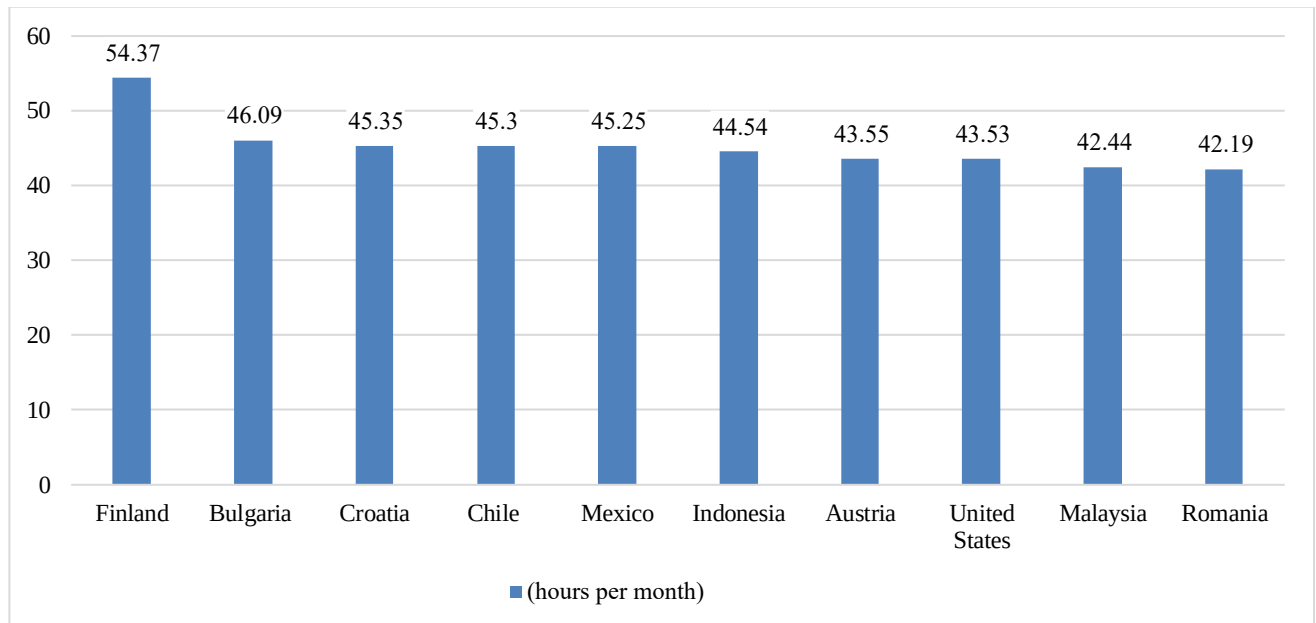
Copyright (c) 2026 Jurnal Ilmu Kepolisian



This work is licensed under a Creative Commons Attribution 4.0 International License.

### INTRODUCTION

In the era of globalisation, technological advancements have progressed rapidly, particularly in the domains of information and communication technologies, which have engendered significant societal transformation (Karomah & Masyuri, 2024). According to The Global Statistics' digital report through 2025, TikTok boasts approximately 108 million active users aged 18 and above, positioning Indonesia as one of the largest markets worldwide. Despite a notable decline of approximately 19.1 million users between January 2024 and January 2025, TikTok remains the leading application for mobile app downloads and ranks as the second most popular platform (The Global Statistics, 2026). This data is depicted in the accompanying chart.



**Figure 1:** Countries that Spend the Most Time on Social Media (February, 2025).

**Source:** GoodStats Indonesia (Wafa, 2025).

GoodStats reports that Indonesia ranks within the top 10 countries for TikTok usage, with users spending around 44.54 hours monthly or about 1 hour and 29 minutes daily (Wafa, 2025). Social media use in Indonesia is very widespread, encompassing messaging applications and content creators that keep Indonesians linked, involved, and interactive (Murphy, 2025). TikTok is a social media platform focused on short videos, enabling users to create, edit, and share their video content (Daulay, 2024). TikTok's algorithm is centred around the *FYP* (For You Page), employing a recommendation system to deliver a tailored experience to users. It suggests content based on factors such as comments, likes, shares, and watch duration (Alwi, 2024). On one hand, this algorithm influences content to go viral more quickly and can be beneficial for digital marketing (Chandra, 2023). This *platform* is generally used as a source of information and a channel for users' creativity (Siroj & Zulfa, 2024).

Nevertheless, the presence of these algorithms results in several adverse consequences, including users being exposed to harmful content, including violence, sexual blackmail, and terrorism (Spring & Radford, 2026), and impacts on mental health (Luthfiani et al., 2025), as a result of viral TikTok content receiving a large number of repeated derogatory, sarcastic, and aggressive comments. Comments and messages received on TikTok may constitute a form of cyberbullying (Aser et al., 2022). This kind of bullying can happen through text messages, instant messages, and chat rooms (Dio Manik et al., 2026). Nevertheless, notwithstanding its beneficial effects, the platform is also susceptible to misuse for criminal activities such as cyberbullying. Perpetrators often engage in actions including the dissemination of negative comments, insults, and even threats directed at their victims, irrespective of their age (Tan & Kornelis, 2022). This is different from Instagram, whose algorithm emphasises users' social networks to compile their feeds. Instagram's algorithm gives priority to content from accounts users follow, especially those they interact with regularly (Syambas, 2024).

Cyberbullying on TikTok encourages more people to post negative comments because the platform's algorithm favours recent and viral content, leveraging its extensive reach to facilitate widespread dissemination (Salsabila et al., 2026). Victims of cyberbullying often face serious outcomes like depression and anxiety. Ongoing fear leads them to frequently feel unsafe at school and home (Aulia et al., 2026). Victims often see a decrease in self-confidence due to cyberbullying, which can result in lower academic performance or trouble concentrating. Additionally, those affected frequently encounter social sanctions within their local communities (Siroj & Zulfa, 2024).

Regulations on cyberbullying in Indonesia are outlined in Article 433, paragraphs (1) and (2), and Article 436 of Law No. 1 of 2023 on the Criminal Code. Furthermore, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions includes Article 27A, Article 27B, paragraphs (1) and (2), Article 45B, and Article 29. Despite these regulations, there remains ambiguity in the legal standards governing cyberbullying (Saputra et al., 2026). The Criminal Code predominantly addresses overarching legal principles related to actions detrimental to the honour, dignity, and sense of security of the victim. In the digital era, behaviours that previously transpired in physical interactions are increasingly moving into the digital domain. Consequently, the provisions of the Criminal Code must be reformulated to reflect the contemporary digital landscape while preserving its fundamental essence (Permaisuri et al., 2025). Law No. 1 of 2024, which amends Law No. 11 of 2008 on Information and Electronic Transactions, includes articles that mainly focus on assault and defamation. However, cyberbullying involves more than just defamation and harassment, and the law does not clearly specify the limits of criminal offences related to defamation and insults (Herman, 2025).

Through a retributive approach and digital policies, ASEAN countries have united to establish the Declaration on the Elimination of Bullying of Children in ASEAN. This declaration embodies a collective commitment to safeguarding children from all forms of bullying, including cyberbullying (ASEAN, 2021a). This commitment encourages Indonesia, an ASEAN member, to enhance digital literacy, bolster the national legal framework for child protection, and collaborate on law enforcement efforts concerning cyberbullying (ASEAN, 2021c).

Similar to Indonesia, Singapore is among the ASEAN nations that endorse and enforce this declaration. It has a relatively high average monthly viewing duration on TikTok within ASEAN, approximately 34 hours and 29 minutes (aww.media, 2025). Singapore already implements regulations to safeguard minors on social media. The Infocomm Media Development Authority (IMDA) specifically works to shield minors from harmful content and can direct platforms to block such material. Its goal is to promote online safety, particularly for children (Infocomm Media Development Authority, 2026). To improve online safety, specific Social Media Services (SMS) must adopt extra measures to protect children. These include preventing children from being exposed to content that could harm their physical or mental health, applying stricter account controls for younger users, and offering tools that allow children or their parents to oversee safety (Ministry of Digital Development and Information, 2024).

Children's utilisation of social media is also strictly regulated due to their high vulnerability to becoming targets of cybercrime. Excessive usage of social media platforms is a significant concern, linked to issues such as anxiety, depression, insomnia, and stress. These associations depend on the duration, frequency, and the number of social media platforms accessed. In TikTok's Annual Online Safety Report, covering the period from April 1, 2023, to March 31, 2024, TikTok reported the removal of 57,500 accounts from Singapore, suspected of having owners under the age of 13. Although numerous accounts belonging to users under 13 have been blocked, a substantial number of active accounts still exist, leaving them vulnerable to negative content and comments.

This study aims to address the research question: How do the legal frameworks of Indonesia and Singapore differ in defining, preventing, and responding to cyberbullying against children on TikTok? Additionally, it considers a secondary research inquiry: How can Indonesia enhance its regulations in accordance with the ASEAN guidelines on cyberbullying? This research aims to analyse the differences between the legal frameworks of Indonesia and Singapore concerning the addressing, prevention, and definition of cyberbullying against children on TikTok. Furthermore, it seeks to ascertain how Indonesia can address ambiguities in its current regulations by aligning them with the ASEAN guidelines on cyberbullying.

This paper employs a normative legal research method, focusing on analysing regulations at the normative level and concepts related to cyberbullying and criminal law in Indonesia. To enrich the research, the author employs a statutory and comparative approach, comparing regulations on cyberbullying in Indonesia and Singapore. The author uses primary legal sources, specifically laws and regulations on cyberbullying in Indonesia and Singapore, as well as international legal instruments on cyberbullying in the ASEAN region.

Regarding secondary legal sources, the author uses books, journal articles, reports, and non-legal materials such as information from websites, dictionaries, and other relevant data. The data were processed through qualitative descriptive analysis, presented narratively and focused on the substance or content of the regulations. The author also presented the data using tables.

## DISCUSSION

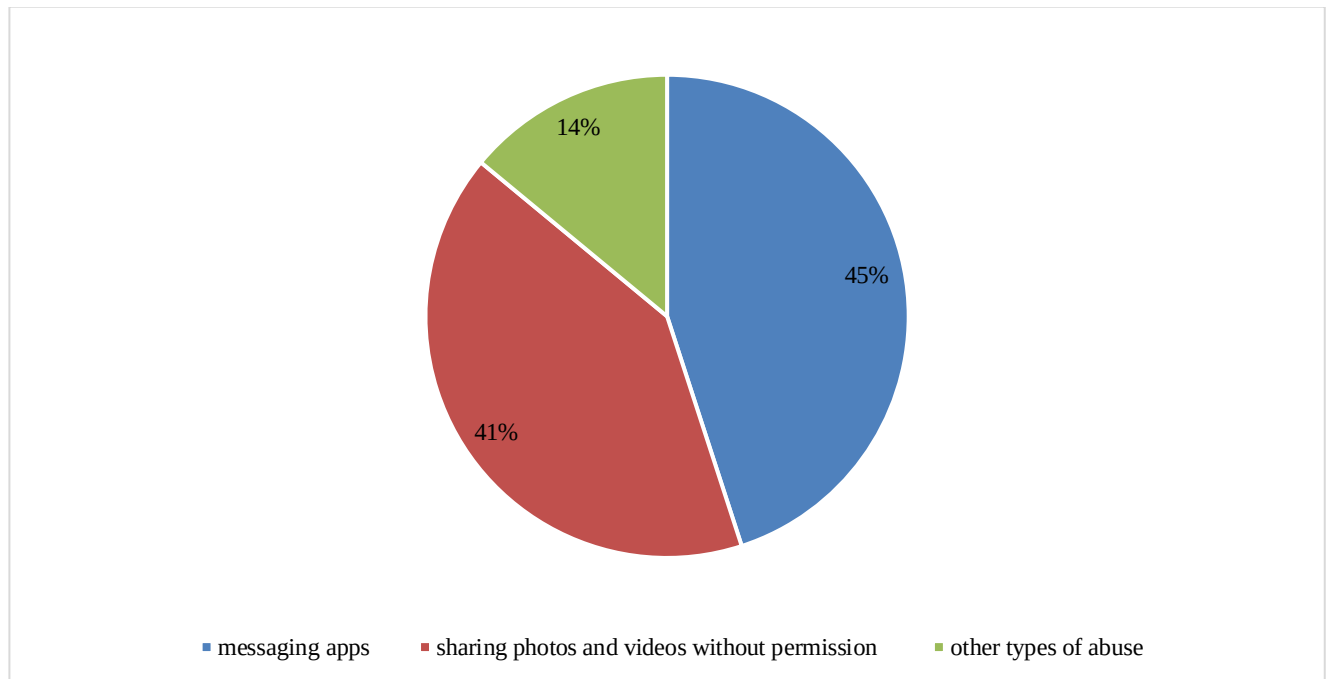
### *Regulations on Cyberbullying in Indonesia*

Cyberbullying is a type of violence involving harassment through digital devices like cell phones, computers, and tablets, and can happen on digital and social media platforms (United Nations Indonesia, 2025). In the digital age, effective detection and intervention against cyberbullying depend heavily on a clear definition of its concept and characteristics. Łosiak-Pilch et al. (2022) define cyberbullying as aggressive, intentional behaviour carried out by perpetrators using electronic communication tools to repeatedly target victims who cannot easily defend themselves (Łosiak-Pilch et al., 2022). Meanwhile, Li (2024) characterises cyberbullying as a form of deliberate aggressive conduct aimed at an individual or a group through digital devices, capable of occurring at any time and in any location, with particular emphasis on the targeting of victims (Permaisuri et al., 2025).

Research by Xiaoting Yang et al. (2022) identifies four key features of cyberbullying: targeting, aggression, repetition, and harmfulness (Yang et al., 2022). This study defines targeting as “cyberbullying directed at specific individuals or groups,” while aggression refers to “the frequent manifestation of cyberbullying as online verbal violence or harmful expressions” (Sadiq et al., 2021). Repetition is noted as “it may involve multiple aggressive messages or persistent harassment”. While harmfulness is “emphasised in most studies as a core consequence of cyberbullying behaviour”.

Victims of cyberbullying are individuals who experience abusive comments that cause emotional distress on social media. As a result, cyberbullies can continue to intimidate victims even when they are alone, outside of school, or at home. Victims lack a safe space because threats can occur at any moment, leading to anxiety, depression, and feelings of isolation (Marbun & Bengkel, 2024). Cyberbullying manifests in various forms, including flaming, slandering, identity theft, exposing secrets, and removing or blocking individuals from groups. Examples encompass abusive language attacks, unauthorised use of someone’s identity, spreading rumours to shame others, and excluding disliked individuals from groups. These categories were identified through research in Songkhla, Thailand, an area with demographics similar to those of Indonesia (Handono et al., 2019).

According to data from the Ministry of Communication and Digital Economy, 48 per cent of Indonesian children have experienced cyberbullying (Kementerrian Komunikasi dan Digital, 2025). UNICEF has identified cyberbullying as a priority issue that must be addressed to uphold children’s rights, particularly in protecting children from violence, especially in the digital space (Rusyidi, 2020). A U-Report survey of 2,777 Indonesian youth aged 14-24 found that 45% of them have experienced cyberbullying. The reporting rate among boys was slightly higher than among girls (49% compared to 41%).



**Figure 2:** The Most Common Types of Online Bullying Against Children According to U-Report.

**Source:** U-Report Indonesia (U-Report Indonesia, 2019).

According to 1,207 U-Report respondents, the most common form of cyberbullying occurs via chat apps. The growth of social media, which has minimal usage restrictions, allows children to interact freely, increasing their risk of harassment within these chat platforms. This type accounts for 45%, the highest among various cyberbullying forms, as perpetrators can easily conceal their identities online (U-Report Indonesia, 2019). This situation makes it simpler and more convenient for perpetrators to target children with bullying, since children are particularly vulnerable and easily deceived due to their limited understanding of the negative aspects of social media. The absence of parental supervision is another weakness that bullies can take advantage of. Concerning the unauthorised sharing of personal photos or videos, children often post such content impulsively because of their limited social media knowledge. This exposes them to cybercriminals who can easily gather information about them and use their photos or videos for cyberbullying. Other harassment types include Identity-Based Harassment and Verbal Harassment.

Law No. 23 of 2022 on Child Protection, along with its amendments, particularly Law No. 35 of 2014, defines 'violence' as any act causing physical, psychological, or sexual distress, suffering, neglect, or threats, coercion, or unlawful detention of a child. The amendment to Article 59(2)(i) clarifies that children victims of physical or psychological violence are entitled to special protection. Additionally, the amendment to Article 69 highlights that this protection includes awareness campaigns about legal rights and mechanisms for monitoring, reporting, and sanctions. Therefore, the Child Protection Law sets a clear framework for addressing violence against children and provisions for protection, including sanctions. However, the law leaves some ambiguity by not explicitly covering the "digital space" in cases of cyberbullying (Pakaya & Mahyani, 2022).

Regulations on cyberbullying in Indonesia are outlined in multiple laws, including Law No. 1 of 2024, which amends Law No. 11 of 2008 (the ITE Law), and Law No. 1 of 2023 of the Criminal Code. An analysis of these laws is provided in the following table.

**Table 1.** Regulations Governing Cyberbullying in Indonesia

| Law                                                                                                          | Aspects and Articles                                                                | Substance of the Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Forms of Cyberbullying                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "Law No. 1 of 2024 on Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions"     | Prohibited Acts, Article 27A in conjunction with Article 45, paragraphs (4) and (5) | "Any person who intentionally attacks the honour or reputation of another person by making an accusation, with the intent that such matter be made known to the public in the form of Electronic Information and/or Electronic Documents transmitted through an Electronic System."                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | The explanatory notes state that "attacking the honour or reputation" refers to acts that demean or damage another person's reputation or self-respect, thereby causing harm to that person, including defamation and/or slander. This offence is complaint-based.                                                                                                                                                                                                                                                                                                                                                                  | Attacking someone's honour (demeaning, damaging their reputation, or self), defaming, and/or making accusations in a manner intended for public knowledge in electronic form. |
| "Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions" | Prohibited Acts, Article 27B(1) and (2) in conjunction with Article 45(7) and (8)   | <ol style="list-style-type: none"> <li>"Any person who intentionally and without authorisation distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or another person, and forces a person through the threat of violence to:               <ol style="list-style-type: none"> <li>hand over goods, whether in whole or in part, belonging to that person or to another person; or</li> <li>grant a loan, acknowledge a debt, or write off a receivable</li> </ol> </li> <li>Any person who intentionally and without authorisation distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or another person, by threatening to defame or by threatening to disclose a secret, thereby compelling a person to:               <ol style="list-style-type: none"> <li>hand over goods that are partly or entirely owned by that person</li> </ol> </li> </ol> | <p>The explanatory notes state that "threats of violence" refer to Electronic Information and/or Electronic Documents containing content intended to instil fear, anxiety, or concern regarding the commission of violence. Furthermore, "threats of defamation" refer to threats to attack another person's honour or reputation by accusing with the intent that such accusation become public knowledge.</p> <p>This article is an addition to the chapter on "Prohibited Acts," so the article in question also outlines several elements of the criminal offence of cyberbullying.</p> <p>This offence is complaint-based.</p> | Threats of violence and threats of defamation in digital form.                                                                                                                |



| Law                                                                                                          | Aspects and Articles        | Substance of the Article                                                                                                                                                                                                                                             | Notes                                                                                                                                                                                                                                                                                                                                                        | Forms of Cyberbullying                                                             |
|--------------------------------------------------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| "Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions" | Prohibited Acts, Article 29 | <p>or by another person;<br/>or</p> <p>b. grant a loan, acknowledge a debt, or write off a receivable."</p>                                                                                                                                                          | <p>The explanatory notes state that the term "victim" refers to a person who suffers physical, mental, and/or economic harm as a result of a criminal act. The acts referred to in this provision are cyberbullying. Thus, it is evident that this article can be used to identify "victims" who suffer as described above as a result of cyberbullying.</p> | Threats of violence and/or intimidation                                            |
|                                                                                                              |                             | "Any person who intentionally and without authorisation sends Electronic Information and/or Electronic Documents directly to a victim that contain threats of violence and/or intimidation."                                                                         |                                                                                                                                                                                                                                                                                                                                                              |                                                                                    |
| "Law No. 1 of 2023 on the Criminal Code"                                                                     | Article 156                 | "Violence is any act, with or without the use of physical force, that poses a danger to the body or life, resulting in physical, sexual, or psychological suffering, and depriving a person of their liberty, including rendering a person unconscious or helpless." | This article, which contains the definition, does not specify that violence includes that occurring in the digital realm; however, the definition is specified in Article 158 regarding "in public."                                                                                                                                                         | "Posing a danger" includes psychological harm                                      |
|                                                                                                              | Article 157                 | "Threat of Violence is any act in the form of speech, writing, images, symbols, or body movements, whether or not using electronic or non-electronic means, that can cause fear, anxiety, or concern that violence will be committed."                               | This article, which contains the definition, does not specify that threats of violence include those occurring in the digital space; however, the definition is provided under "in public" in Article 158.                                                                                                                                                   | Causing a sense of fear, anxiety, or concern regarding the commission of violence. |
|                                                                                                              | Article 158                 | "In Public means a place or space that can be seen, visited, known, or witnessed by others, either directly or indirectly through electronic media that allows the public to access electronic information or electronic documents."                                 | This article broadens the meaning of the "locus delicti" to include electronic media as part of what is meant by "in public."                                                                                                                                                                                                                                |                                                                                    |
|                                                                                                              | Article 242                 | "Any person who, in public, expresses feelings of hostility, hatred, or contempt toward a single or several groups of the                                                                                                                                            | This article clarifies the prohibited acts, namely expressing feelings of hostility, hatred, or                                                                                                                                                                                                                                                              |                                                                                    |

| Law | Aspects and Articles                | Substance of the Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Notes                                                                                                                | Forms of Cyberbullying                 |
|-----|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------|
|     |                                     | Indonesian population based on race, nationality, ethnicity, skin colour, gender, mental disability, or physical disability, shall be punished with imprisonment for a maximum of 3 (three) years or a fine not exceeding Category IV."                                                                                                                                                                                                                                                                                     | contempt toward one or more groups or segments of the population based on the classifications listed in the article. |                                        |
|     | Article 262                         | "Any person who, openly or in public and in concert with others, commits violence against a person or property shall be punished by imprisonment for a maximum of 5 (five) years or a fine not exceeding Category V."<br>1. "Any person who verbally attacks the honour or reputation of another person by making an accusation, with the intent that such accusation be made known to the public, shall be punished for defamation with imprisonment for a maximum of 9 (nine) months or a fine not exceeding Category II. | This article clarifies the prohibited act, namely committing violence against a person in public.                    | The form is violence against a person. |
|     | Article 433, paragraphs (1) and (2) | 2. If the act referred to in paragraph (1) is committed through writing or images that are broadcast, displayed, or posted in a public place, the offender shall be punished for written defamation with imprisonment for a maximum of 1 (one) year and 6 (six) months or a fine not exceeding Category III."                                                                                                                                                                                                               | This article clarifies the criminal offence of defamation committed verbally, in writing, or through images.         | The form is insulting.                 |



| Law | Aspects and Articles | Substance of the Article                                                                                                                                                                                                                                                                                                                                                                                                             | Notes                                      | Forms of Cyberbullying  |
|-----|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-------------------------|
|     | Article 436          | "Insult that does not constitute defamation or Written defamation committed against another person, whether in public, verbally or in writing, or in the presence of the person being defamed, verbally, through conduct, or through a written communication sent to or received by that person, is punishable as a misdemeanour of defamation by imprisonment for a maximum of 6 (six) months or a fine not exceeding Category II." | This article pertains to minor defamation. | The form is defamation. |

**Source:** Compiled by the Authors, 2026.

Based on the regulatory mapping provided in Table 1, it can be asserted that the regulation of cyberbullying in Indonesia remains disjointed across conceptual, normative, and law enforcement dimensions. This disjointedness stems from the absence of cyberbullying being recognised as a distinct category of legal conduct with a comprehensive definition, elements, forms, characteristics, and mechanisms for victim protection. Instead, various behaviours that may substantively be classified as cyberbullying are dispersed across multiple provisions within the ITE Law and the Criminal Code. Consequently, Indonesian positive law tends to address cyberbullying through an offence-based framework.

The initial form of fragmentation is seen in how cyberbullying elements are spread across various offences with specific legal aims. Article 27A of the ITE Law aims to protect honour and reputation by banning the act of making accusations intended for public awareness through electronic information or documents. This can cover cyberbullying behaviours like insults, defamation, or digital reputation attacks. However, its effectiveness relies on proving the act of “making an accusation” and the intent to make it public. Therefore, not all digital acts of belittling, humiliating, mocking, or threatening victims fit neatly into Article 27A. This is significant because cyberbullying often involves repeated teasing, derogatory comments, image manipulation, spreading humiliating memes, digital ostracism, or collective attacks, which may not always qualify as factual accusations. Additionally, since Article 27A is complaint-based, unclear boundaries around what constitutes insult and defamation can lead to several legal ambiguities.

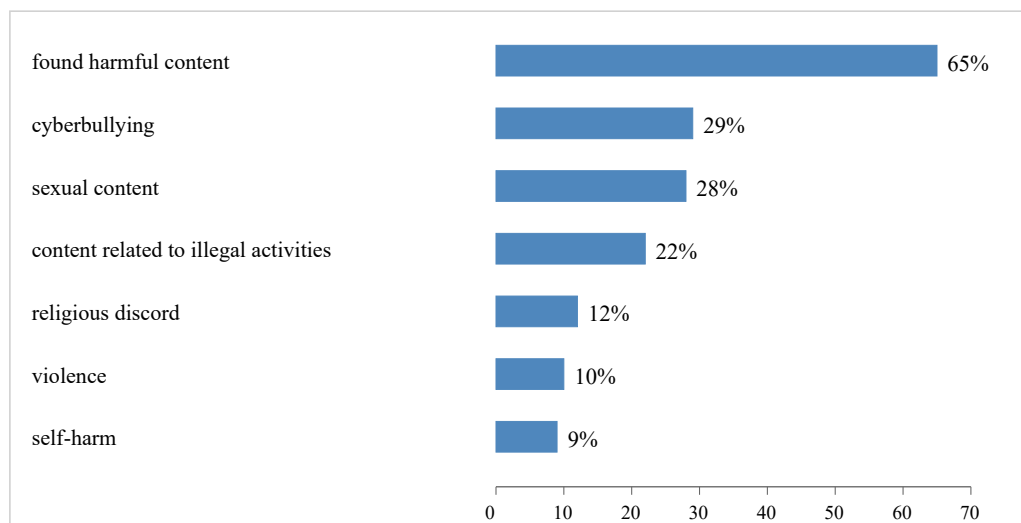
In general, Article 27B of the ITE Law bans anyone from intentionally and without permission distributing, transmitting, or creating electronic information or documents with illegal content that can be accessed via an electronic system. This ban includes various types of content such as pornography, gambling, defamatory or slanderous material, and content that involves extortion or threats (Putra, 2019). This article primarily aims to prevent the spread of harmful, immoral, or illegal content through digital platforms like the internet and social media. Its goal is to shield the public from the misuse of information technology that could threaten dignity, security, and public order. It frequently provides the legal foundation for prosecuting cybercrimes, such as cyberbullying, which are often carried out electronically and may contravene this article (Hadi, 2025).

Article 29 of the ITE Law is more directly relevant because it addresses the transmission of electronic information or documents containing threats or intimidation to a victim. The explanatory notes explicitly include cyberbullying within this scope. However, this recognition has not led to a comprehensive legal framework for cyberbullying, mainly because the offence is narrowly defined, focusing on threats of violence or intimidation and requiring that communication be sent “directly to the victim.” In practice, much

cyberbullying happens indirectly through public posts, anonymous accounts, digital groups, sharing content with third parties, online forums, mass comments, or algorithmic amplification. Therefore, the mention of cyberbullying in Article 29's explanation does not equate to a broad legal regulation covering all cyberbullying forms.

The relationship between the ITE Law and the national Criminal Code adds further complexity. The Criminal Code has incorporated developments in the digital realm through various definitions and offences. For example, Article 157 addresses threats of violence via speech, writing, images, symbols, or bodily movements, whether or not electronic means are used. Similarly, Article 158 broadens the definition of "in public" to include electronic media accessible to the public, recognising the digital space as a relevant venue for certain crimes. Despite this, inconsistencies remain. Some Criminal Code provisions are still based on traditional categories such as violence, threats, defamation, slander, and minor insults without fully accounting for cyberbullying's unique features like content persistence, perpetrator anonymity, unlimited replication, virality, coordinated attacks, and digital power imbalances. Articles 433 and 436 are broadly applicable to cyberbullying through defamation and minor insults, offering a general legal framework. These provisions mark progress in criminal fines, contrasting with the previous Criminal Code, which primarily mandated custodial sentences under Articles 310, 311, and 315 (Oktavira, 2023).

Although regulations are still fragmented, Indonesia currently has some legal provisions on cyberbullying through the Criminal Code and the ITE Law. These laws complement each other: the Criminal Code provides the overall legal framework and addresses incidents in public spaces, while the ITE Law enhances cybercrime regulation by focusing on electronic conduct (Lalisu et al., 2026). The aspiration is that these regulations will enhance initiatives aimed at safeguarding victims of cyberbullying. This is essential because, beyond offering protection, it assists victims in feeling secure and helps avert the creation of new victims (Hikmawati, 2024).



**Figure 3:** Survey Conducted by the Ministry of Digital Development and Information (MDDI).

**Source:** Ministry of Digital Development and Information (Ministry of Digital Development and Information, 2024).

### ***Regulations on Cyberbullying in Singapore***

Singapore's cyberbullying regulations are primarily outlined in the Protection from Harassment Act, which covers threatening, insulting, or distressing conduct online or in person, implicitly including cyberbullying as online harassment. Additionally, the newly introduced Online Safety (Relief and Accountability) Act explicitly targets cyber harm, extending to doxing, stalking, and harassment, thereby enhancing protections in the digital environment.

A survey by the Ministry of Digital Development and Information (MDDI) reveals that about 65% of children have encountered harmful content on social media, the highest among various platforms. Although social media has its downsides, as shown in the table, Singapore actively addresses this issue through the IMDA. The IMDA has identified six major Social Media Services (SMS) with significant reach or influence in Singapore: Facebook, HardwareZone, Instagram, TikTok, X (formerly Twitter), and YouTube. These platforms must follow the Code of Practice for Online Safety (Online Safety Code), which came into effect on July 18, 2023. This code mandates that designated Social Media Services (SMS) implement additional safety measures for children, such as preventing the targeting of harmful content, enforcing stricter account settings for minors, and providing tools for children and parents to manage safety effectively.

Singapore has introduced warning labels on social media platforms to inform minors about their usage, including duration, frequency, and the number of platforms involved. Parents suspecting their children may be addicted to social media can turn to service providers like Touch Community Services, which offers counselling and intervention programs for adolescents. Alternatively, they can seek assessments and help from specialised units such as the National Addictions Management Service (NAMS). The country supports parents from early on, even before birth, and is committed to implementing more effective measures to guide social media habits. The Ministry of Health (MoH) and the Ministry of Social and Family Development (MSF) oversee early childhood care through child, maternal, and preschool programs, aiming to establish clearer guidelines on device use and screen time, communicated consistently across healthcare settings with increased reminders (Ministry of Digital Development and Information, 2024).

Singapore does not possess a specific law that explicitly delineates cyberbullying. Instead, the nation has developed a comprehensive legal framework through various complementary regulatory instruments to address diverse forms of conduct in the digital domain. Regulations about cyberbullying in Singapore can be located within the Protection from Harassment Act 2014, which addresses doxing, harassment, threats, and stalking, whether executed directly or through social media platforms. As cyberbullying has advanced, Singapore has enhanced its legal provisions by enacting the Online Safety (Relief and Accountability) Act 2025, which broadens protections against such conduct. In addition to affording victims the right to prompt redress, the OSRA establishes the Online Safety Commission, empowered to issue directives to perpetrators, platform administrators, and digital service providers to remove or restrict access to content that causes harm to victims. An analytical overview of these statutory provisions is presented in the ensuing table.

**Table 2.** Regulations Governing Cyberbullying in Singapore

| Regulation                                           | Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Description                                                                                                                                               | Forms of Cyberbullying                      |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| <b>"Protection From Harassment Act, 2014 (POHA)"</b> | <b>"Intentionally causing harassment, alarm, or distress"</b><br>3. (1) No individual or entity shall, with the intent to cause harassment, alarm, or distress to another person (referred to in this section as the "target person"), by any means ,<br>(a) use any threatening, abusive, or insulting words or behaviour;<br>(b) make any threatening, abusive, or insulting communication; or<br>(c) publish any identifying information about the target person or a person related to the target person, and thereby causing the target person or any other person (each referred to in this section as the "victim") harassment, alarm, or distress." | This section focuses on preventing cyberbullying, which includes harassment, alarm, and distress intentionally inflicted by an individual or legal entity | harassment, alarm, distress, or humiliation |
|                                                      | <b>"Harassment, Alarm, or Distress"</b><br>4. (1) An individual or entity must not, by any means,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | This section focuses on protecting victims                                                                                                                | harassment, alarm, distress, or humiliation |

| Regulation                                           | Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Description                                                                                                                                                                                   | Forms of Cyberbullying                                                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Act, 2014 (POHA)"</b>                             | <p>(a) use any threatening, abusive, or insulting words or behaviour; or</p> <p>(b) make any threatening, abusive, or insulting communication, which, when heard, seen, or otherwise perceived by any person (referred to in this section as the victim), is likely to cause harassment, alarm, or distress."</p> <p><b>"Fear, provocation, or facilitation of violence</b></p> <p>5. (1) An individual or entity must not, by any means, direct toward another person (referred to in this section, except subsection (1A), as the victim) any threatening, abusive, or insulting words or behaviour, or make any threatening, abusive, or insulting communication to another person (also referred to in this section, except subsection (1A), as the victim), either,</p> <p>(a) with the intent ,</p> <p>(i) to cause the victim to believe that unlawful violence will be used by any person against the victim or any other person; or</p> <p>(ii) to provoke the use of unlawful violence by the victim or another person against any other person; or</p> <p>(b) whereby ,</p> <p>(i) the victim is likely to believe that the violence mentioned in paragraph (a)(i) will be used; or</p> <p>(ii) it is likely that the violence mentioned in paragraph (a)(ii) will be provoked.</p> <p>(1A) An individual or entity must not, by any means, publish any identifying information about another person (referred to in this subsection as the victim) or a person related to the victim, either ,</p> <p>(a) with the intent ,</p> <p>(i) to cause the victim to believe that unlawful violence will be used against the victim or any other person; or</p> <p>(ii) to facilitate the use of unlawful violence against the victim or any other person; or</p> <p>(b) knowing or having reasonable grounds to believe that it is likely ,</p> <p>(i) to cause the victim to believe that unlawful violence will be used against the victim or any other person; or</p> <p>(ii) to facilitate the use of unlawful violence against the victim or any other person."</p> | <p>from harassment, alarm, and distress caused by a person or legal entity</p> <p>This section focuses on violence and provocation through social media intended to incite greater unrest</p> |                                                                                                                       |
| <b>"Protection From Harassment Act, 2014 (POHA)"</b> | <p><b>"Unlawful Stalking</b></p> <p>7. (1) An individual or entity must not unlawfully stalk another person.</p> <p>(2) Subject to subsection (7), an individual or entity (referred to in this section as the accused) unlawfully stalks another person (referred to in</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>This section focuses on protecting individuals from online stalking that causes the</p>                                                                                                    | <p>Provocative, abusive, or insulting words or behaviour</p> <p>unlawful stalking, harassment, alarm, or distress</p> |

| Regulation                                                         | Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Description                                                                                                                                                                                     | Forms of Cyberbullying                                             |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
|                                                                    | <p>this section as the victim) if the accused engages in a course of conduct that ,</p> <p>(a) involves acts or omissions associated with stalking;</p> <p>(b) causes harassment, alarm, or distress to the victim; and</p> <p>(c) the accused ,</p> <p>(i) intends to cause harassment, alarm, or distress to the victim; or</p> <p>(ii) knows or ought reasonably to know that such conduct is likely to cause harassment, alarm, or distress to the victim."</p>                    | <p>victim or another person to experience pressure and anxiety</p>                                                                                                                              |                                                                    |
| <b>"Online Safety (Relief and Accountability) Act 2025 (OSRA)"</b> | <p><b>"Online Harassment</b></p> <p>9. (1) In this Act, "online harassment" means the communication of online material that a reasonable person would conclude is ,</p> <p>(a) threatening, abusive, insulting, sexual, or indecent; and</p> <p>(b) likely to cause a person (referred to in this section as the victim) harassment, alarm, distress, or humiliation."</p>                                                                                                             | <p>This section focuses on harassment on social media that causes the victim to experience pressure, anxiety, or humiliation.</p>                                                               | <p>harassment, alarm, distress, or humiliation.</p>                |
|                                                                    | <p><b>"Doxing</b></p> <p>10. (1) In this Act, "doxing" means the publication of any identity information of a person that a reasonable person would conclude was likely intended to cause harassment, alarm, distress, or humiliation to that person or any related person (each referred to in this section as the victim)."</p>                                                                                                                                                      | <p>This section focuses on the dissemination of personal information without the victim's consent with the intent to harass the victim and cause the victim to experience fear or distress.</p> | <p>doxing</p>                                                      |
| <b>"Online Safety (Relief and Accountability) Act 2025 (OSRA)"</b> | <p><b>"Online Stalking</b></p> <p>12. (1) In this Act, "online stalking" means a course of online conduct engaged in by one person (referred to in this section as the online stalker) with respect to another person (referred to in this section as the victim) ,</p> <p>(a) that involves online acts or omissions associated with stalking; and</p> <p>(b) that a reasonable person would conclude is likely to cause the victim harassment, alarm, distress, or humiliation."</p> | <p>This section focuses on online stalking that causes the victim to experience pressure, anxiety, or humiliation.</p>                                                                          | <p>harassment, alarm, distress, or humiliation for the victim.</p> |
| <b>"Online Safety (Relief and Accountability) Act 2025 (OSRA)"</b> | <p><b>"Image-Based Child Abuse</b></p> <p>14. (1) In this Act, "image-based child abuse" means the communication of online material that contains any of the following:</p>                                                                                                                                                                                                                                                                                                            | <p>This section focuses on the distribution of intimate images</p>                                                                                                                              | <p>Outing &amp; Exploitation, Image-based Child Abuse</p>          |

| Regulation                                                         | Article                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Description                                                                               | Forms of Cyberbullying |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------------------------|
| <b>"Online Safety (Relief and Accountability) Act 2025 (OSRA)"</b> | (a) an image or recording of a person (referred to in this section as the victim) being subjected to child abuse;<br>(b) an offer to sell or distribute a child abuse image or recording of the victim;<br>(c) an advertisement for a child abuse image or recording of the victim;<br>(d) (d)any material that appears to be designed or communicated in such a way as to lead to any child abuse image or recording of the victim."                                      | of children under 16 years of age.                                                        |                        |
|                                                                    | <b>"Online Impersonation"</b><br>15. In this Act, "online impersonation" means online activity conducted by one person (referred to in this section as "X") with respect to another person (referred to in this section as "the victim") that ,<br>(a) involves X pretending to be the victim without the victim's consent; and<br>(b) would lead a reasonable person to believe that the online activity was conducted by the victim when this was not in fact the case." | This section focuses on the use of another person's identity for entertainment or satire. | Online impersonation   |

**Source:** Compiled by the Authors, 2026.

According to the regulatory mapping in Table 2, Singapore's cyberbullying regulations are broadly scoped. This extensive scope highlights an adaptive strategy to the evolving nature of information technology and the diverse forms of online bullying. Overall, Singapore's cyberbullying laws are quite comprehensive, evidenced by various legal instruments that, while not explicitly using the term "cyberbullying," substantively encompass different behaviours that qualify as cyberbullying.

The Protection from Harassment Act 2014 is the main legal framework in Singapore addressing cyberbullying and related behaviours. It covers various harassment forms, including online abuse. Victims can pursue civil remedies, such as protection orders, to stop the perpetrator's harassing actions. Additionally, if a false statement of fact is published, the court can issue another type of order. Part 2, Offences Article 3 criminalises intentionally causing harassment, alarm, or distress through threatening, insulting, or degrading words or communications. This emphasises intent as the key element for liability, setting clear boundaries for cyberbullying offences. Conversely, Article 4 broadens protection by removing the intent requirement, focusing instead on the harm caused, which benefits child victims by addressing the actual impact of cyberbullying.

Generally, Article 5 covers actions that create fear of violence or provoke cyberbullying against children. The provocation element refers to cyberbullying conducted intentionally to harass the victim repeatedly. Article 7 pertains to illegal stalking on social media, which can be seen as cyberstalking. This involves the perpetrator deliberately monitoring the victim to gather information, such as defaming or locating the victim's address for threats. This aspect makes the victim feel unsafe, even in social settings (United Nations Office on Drugs and Crime, 2019).

The Online Safety (Relief and Accountability) Act of 2025 further fortified regulations against cyberbullying, adapting to new digital challenges and emerging forms of abuse. Part 3, Article 9, utilises the "reasonable person" standard to assess whether content is objectively threatening, insulting, or sexually explicit, factors that can cause distress or humiliation. This expands the protection scope, especially for children, and offers a



potential standard of proof for cyberbullying victims. Meanwhile, Article 10 targets “doxing”, the act of sharing personal information to harm someone. This is especially critical because distributing personal data, notably about child victims, can escalate the risk of further exploitation (e-Safety Commissioner, 2025). Article 12 strengthens Article 7 of the Protection from Harassment Act 2014 by implementing a “course of conduct” approach, which is typical of cyberbullying. This change addresses weaknesses in the “reasonable person” standard of that article, as adult perceptions of reasonableness may not align with a child’s subjective experience, thus offering less protection (Ministry of Digital Development and Information, 2025). Article 14 explicitly offers special protection for children by prohibiting the dissemination of content and exploitation of minors, aiming to prevent children from being exposed to cyberbullying. It clearly states that minors are individuals needing protection and deserve special safeguards (Koh, 2026).

Furthermore, Article 15 addresses the aspect of anonymity, despite not explicitly mentioning it. The element of “disguised actions” is a significant concern often encountered in cyberbullying. The existence of this provision protects digital integrity, especially for children. The inclusion of this norm demonstrates that Singapore’s regulations have evolved towards adaptive safeguards against the challenges posed by digital anonymity.

Conceptually, laws like the Protection from Harassment Act 2014 form the main framework regulating various harmful activities online, including harassment, threats, doxing, and impersonation. POHA focuses on protecting victims and providing remedies, such as court-issued protection orders or content removal under the Online Safety (Relief and Accountability) Act 2025. This act enhances enforcement by empowering the OSC to instruct platforms and group admins to remove harmful content, restrict offenders’ online accounts, or, in the future, enable victims to post replies (Koh, 2026).

### ***A Comparison of Cyberbullying Regulations in Indonesia and Singapore in the Context of the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN***

The ASEAN Regional Plan of Action (RPA) for the Protection of Children from All Forms of Online Exploitation and Abuse was created collaboratively by ASEAN member states in response to increasing threats to children in the digital world (D’Cruz, 2022). This meeting was called to acknowledge that advances in information technology have opened new channels for violence and exploitation against children, including cyberbullying, digital sexual abuse, and grooming online. These issues can no longer be tackled effectively through isolated national efforts alone. There are also regulatory gaps among ASEAN member countries, highlighting the need for a common framework to harmonise child protection standards and bolster regional cooperation. The ASEAN RPA discussions extend beyond just developing or enhancing laws, covering seven essential areas (ASEAN, 2021b).

The Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse is grounded in a regional normative framework aimed at harmonising child protection standards across ASEAN nations. This plan is more than just a political statement; it also offers clear operational indicators across seven key areas for ASEAN members. The RPA acts as a standards benchmark, allowing for comparison of how well each country has integrated regional child protection standards into its legal frameworks.

**Table 3.** Comparative Analysis of Cyberbullying Regulations in Indonesia and Singapore Based on the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN

| No. | Focus Area                                                                                                                                                   | Action                                             | Indonesia           | Singapore           |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|---------------------|---------------------|
| 1.  | "Focus Area 1: Promote, develop, and implement comprehensive national legal frameworks in each ASEAN Member State and work toward improving child protection | a. "Activity 1. Conduct a legislative review"      | Already established | Already established |
|     |                                                                                                                                                              | b. "Activity 2. Strengthen legislative frameworks" | Already implemented | Already implemented |

| No. | Focus Area                                                                                                                                                                                                                                                                              | Action                                                                                                    | Indonesia                                                          | Singapore                                              |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------|
|     | standards and policies regarding all forms of online exploitation and abuse across ASEAN Member States"                                                                                                                                                                                 | c. "Activity 3. Adopt or strengthen national policies and action plans"                                   | Already meets the requirements but is not yet specific to children | Substantively met                                      |
| 2.  | "Focus Area 2: Enhance the capabilities of law enforcement, the judiciary, and legal professionals through regular, relevant, and up-to-date training, as well as the sharing and exchange of best practices in protecting children against all forms of online exploitation and abuse" | a. "Activity 1. Build the capacity of law enforcement and the judiciary"                                  | Already met, but not uniformly                                     | Has become more systematic                             |
|     |                                                                                                                                                                                                                                                                                         | b. "Activity 2. Ensure that law enforcement and the judiciary have adequate mandate, guidance, and tools" | Not yet fully optimal                                              | Already established                                    |
|     |                                                                                                                                                                                                                                                                                         | c. "Activity 3. Strengthen offender management systems"                                                   | Not currently implemented.                                         | Already implemented and more systematic                |
| 3.  | "Focus Area 3: Encourage the establishment of a national specialised unit with an explicit mandate to lead, support, and coordinate investigations"                                                                                                                                     |                                                                                                           | Already established but not yet centralised.                       | Already established, and more specific and coordinated |
| 4.  | "Focus Area 4: Ensure the effectiveness of rights-based, gender- and age-responsive child protection and support services, as well as social welfare programs"                                                                                                                          | "Activity 1. Ensure the quality and accessibility of rescue, recovery, care, and support services"        | Already established but not yet evenly distributed                 | Already more effective                                 |
| 5.  | "Focus Area 5: Strengthen data collection and monitoring, reporting, and referral mechanisms through hotlines to report online materials suspected of being illegal, including child sexual abuse material"                                                                             |                                                                                                           | Not fully optimised yet                                            | Already optimal                                        |
| 6.  | "Focus Area 6: Promote a national education program and school curricula to raise awareness of sexual and other forms of exploitation of children to empower children, young people, parents, guardians, caregivers, practitioners, and the community"                                  | a. "Activity 1. Strengthen and Expand Education on CSEA"                                                  | Already established but not yet evenly distributed                 | Already established and more systematic                |
|     |                                                                                                                                                                                                                                                                                         | b. "Activity 2. Awareness-raising"                                                                        | Already established but not yet uniform                            | Already established and more systematic                |

| No. | Focus Area                                                                                                                                                                                                                                                                                                                                                                                         | Action | Indonesia               | Singapore       |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------|-----------------|
| 7.  | "Focus Area 7: Mobilise and enhance engagement with the private sector and other relevant stakeholders to actively involve them in monitoring prevention and response measures through 15 regulations, corporate social responsibility, and collaboration for the development of effective measures to detect, remove, and report illegal content related to child sexual abuse and exploitation." |        | Not fully optimised yet | Already optimal |

**Source:** Compiled by the Authors, 2026

Within the framework of the ASEAN Regional Plan of Action for the Protection of Children from Online Exploitation and Abuse, Indonesia has met most indicators, especially in legal, educational, and policy areas. This is demonstrated by laws such as Law No. 1 of 2024, which amends Law No. 11 of 2008 on Electronic Information and Transactions; Law No. 1 of 2023, the Criminal Code; and Law No. 35 of 2014, amending Law No. 23 of 2002 on Child Protection. However, these laws remain largely normative and are not fully enforced. Indonesia's main weakness is the fragmented protection system, lacking a specific framework for children's protection in the digital space. Consequently, Indonesia relies on a general approach with uneven enforcement and faces technological and coordination challenges, resulting in a reactive stance toward issues like cyberbullying against children (Nafi & Nurhayati, 2026). Services tackling digital crimes against children, such as data systems, monitoring, and reporting, are inconsistent across Indonesia. The ASEAN Regional Plan of Action highlights the need for evidence-based policies to achieve more effective and measurable responses.

Indonesia has demonstrated relatively strong performance in education and awareness initiatives. These efforts can help decrease cyberbullying among children, though they are not yet fully or effectively implemented, especially in reporting systems, monitoring, and removing harmful content (Anastashia, 2026). In other words, Indonesia is officially aligned with ASEAN standards but has not yet reached a fully effective and integrated implementation level.

Singapore demonstrates a strong level of implementation, with nearly all focus areas covered by its regulations. This includes the legal framework, enforcement capacity, and private sector involvement in preventing cyberbullying. Key regulations like the Protection From Harassment Act 2014 and the Online Safety (Relief and Accountability) Act 2025 form the core foundation. These laws are not only normative but also include clear, swift, and adaptable enforcement mechanisms that keep pace with the rapidly changing digital landscape (International TradeTrust Compliance Network, 2026). Singapore employs a structured and coordinated strategy. Law enforcement agencies are well-resourced and operate under clear guidelines. Specialised units focused on preventing cyberbullying against children are vital for combating this issue. Concerning protection services and reporting systems, Singapore reacts swiftly to cyberbullying cases, supported by accessible, data-driven mechanisms.

The private sector plays a crucial role in combating cyberbullying by actively monitoring social media for harmful content. Singapore's government requires digital platforms to supervise their content, eliminate harmful posts, and establish a reporting system that channels complaints to authorities for further action (Infocomm Media Development Authority, 29 June 20226).

### ***The Urgency of Strengthening Legal Protection for Children in Cyberbullying Cases in Indonesia Based on the ASEAN RPA***

The RPA analysis in Table 3 shows that Indonesia continues to have notable gaps in fulfilling the ASEAN Regional Plan of Action standards. The RPA was created as an operational tool to implement the 2019 ASEAN Declaration on Protecting Children from Online Exploitation and Violence. It focuses on seven main areas:

legal framework, law enforcement capacity, specialised investigative units, victim services, data systems, education, and private-sector involvement.

Although Indonesia has various regulations on cyberbullying, their approaches are too general and don't specifically target different types of cyberbullying. In contrast, Singapore adopts a more comprehensive, progressive regulatory framework that clearly defines specific types of cyberbullying and enforces strict enforcement mechanisms. To effectively prevent cyberbullying, Indonesia must go beyond merely enacting laws; it must also improve implementation through a coordinated and adaptable system. Additionally, Indonesia should create a dedicated institution to combat cybercrime, especially against children, to ensure a quick and effective response to cyberbullying cases. The ASEAN RPA emphasises establishing a specialised national unit with a clear mandate to lead investigations, support victims, and coordinate responses. Singapore's experience shows that having such a dedicated unit is crucial for effectively managing cyberbullying cases involving children (Chia, 2025).

Conversely, Indonesia encounters difficulties in the form of unintegrated data and inconsistent reporting mechanisms. In the absence of accurate data, the policies implemented are likely to be reactive rather than evidence-based. Consequently, it is imperative for Indonesia to establish an integrated reporting system, inclusive of a digital complaint platform, and to develop definitive follow-up mechanisms (Putra, 2019). From an ASEAN perspective, these specialised units are part of a collective effort to develop a rapid, coordinated, and regional response system. Accordingly, Indonesia should enhance its institutional framework by providing a clear mandate to tackle cyberbullying and cybercrimes against children, following best practices adopted by other member states.

While Indonesia has shown good progress in education, there is a need to make its approach more systematic and fair. The country should introduce a more comprehensive digital literacy program for children, parents, and teachers to combat cyberbullying. This aligns with ASEAN RPA Focus Area 6, which promotes awareness about sexual and other forms of exploitation through national education and school curricula, empowering children and communities. However, in practice, education has not yet been fully integrated into the national curriculum and has not effectively reached every part of society (ASEAN, 2021b).

Indonesia therefore continues to face interpretive and implementation gaps in addressing cyberbullying. A clearer and more integrated framework is needed to protect children from harmful online conduct while giving law-enforcement and child-protection institutions more consistent legal guidance, digital child protection is also a regional concern. Indonesia should align domestic policy with the ASEAN Regional Plan of Action as part of its responsibility to support a safer cross-border digital environment for children.

## CONCLUSION

The comparison shows that Indonesia and Singapore differ substantially in how they define, prevent, and respond to child cyberbullying on TikTok. Indonesia has a legal basis for intervention, but protection remains fragmented across offences such as insult, defamation, threats, and intimidation, without a single framework defining child cyberbullying, prevention, response, and victim recovery. Singapore provides a more integrated and victim-focused model through its harassment and online-safety legislation. Indonesia has met several commitments under the ASEAN Regional Plan of Action, particularly in legal frameworks, education, awareness, and policy, but important implementation gaps remain. The central problem is therefore not simply the absence of criminal provisions, but fragmentation in definitions, institutions, reporting, recovery, and platform accountability. Indonesia should harmonise the legal definition and forms of child cyberbullying, strengthen specialised institutional coordination and reporting systems, improve victim recovery and digital literacy, and establish clearer responsibilities for digital platforms. These measures would better align domestic protection with ASEAN standards while preserving a child-centred approach to online safety.

## REFERENCES

- Alwi, M. N. (2024). Algoritma TikTok: Beginilah Cara TikTok Menampilkan Konten. *Dicoding Blog*. <https://dicoding.com/blog/algoritma-tiktok-beginilah-cara-tiktok-menampilkan-konten/>
- Anastashia, S. (2026). PENGARUH LITERASI DIGITAL TERHADAP PENCEGAHAN CYBERBULLYING DI KALANGAN REMAJA. *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora*, 3(1), 111-118.
- ASEAN. (2021a, January 3). *Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf*. <https://asean.org/wp-content/uploads/2021/01/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf>
- ASEAN. (2021b, April 11). *Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN*. [https://acwc.asean.org/wp-content/uploads/2024/06/4.-ASEAN-RPA-on-COEA\\_Final.pdf](https://acwc.asean.org/wp-content/uploads/2024/06/4.-ASEAN-RPA-on-COEA_Final.pdf)
- ASEAN. (2021c, October 14). *DECLARATION ON THE ELIMINATION OF BULLYING OF CHILDREN IN ASEAN*. ASEAN. <https://asean.org/wp-content/uploads/2021/10/14.-Declaration-on-the-Elimination-of-Bullying-of-Children.pdf>
- Aser, F. G., Paramita, S., & Sudarto. (2022). Fenomena Cyberbullying di Media Sosial TikTok. *Kiwari*, 1(3), 449-453. <https://doi.org/10.24912/ki.v1i3.15763>
- Aulia, B., Rahmaliza, A., & Puriani, R. A. (2026). Cyberbullying and Its Long-Term Impact on the Mental Health of Children and Adolescents. *Life Course Psychology*, 1(1), 16-24.
- Aww. media. (2025, March 7). What is the Best Time to Post on TikTok in Singapore? *Aww.Media*. <https://aww.media/what-is-the-best-time-to-post-on-tiktok-in-singapore/>
- Chandra, E. (2023). Kekuatan Algoritma Dalam Komunikasi Pemasaran Digital Aplikasi Tiktok. *Maha Widya Duta: Jurnal Penerangan Agama, Pariwisata Budaya, Dan Ilmu Komunikasi*, 7(2), 191-199. <https://doi.org/10.55115/duta.v7i2.3860>
- Chia, O. (2025, March 8). *New online harms support centre to operate from 2026, will offer victims faster recourse | The Straits Times*. [straitstimes. https://www.straitstimes.com/singapore/politics/new-online-harms-support-centre-to-begin-operation-in-2026](https://www.straitstimes.com/singapore/politics/new-online-harms-support-centre-to-begin-operation-in-2026)
- Daulay, A. Y. (2024, July 2). *DAMPAK PENGGUNAAN APLIKASI TIKTOK TERHADAP PERILAKU SOSIAL ANAK DI DESA SIUNGGAM TONGA KABUPATEN PADANG LAWAS UTARA* [Undergraduate thesis]. UIN Syekh Ali Hasan Ahmad Addary Padangsidimpuan.
- D'Cruz, N. (2022, February 11). Launch event: The Regional Plan of Action for Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (2021-2025). *ECPAT*. <https://ecpat.org/launch-event-the-regional-plan-of-action-for-protection-of-children-from-all-forms-of-online-exploitation-and-abuse-in-asean-2021-2025/>
- Dio Manik, Yeni Adventry Tanjung, Annisa Ananda Utomo, Amelia Amelia, & Muhammad Natsir. (2026). Discursive Toxicity and Cyberbullying in TikTok User Comments: A Critical Discourse Analysis Approach. *Student Scientific Creativity Journal*, 4(3), 327-338. <https://doi.org/10.55606/sscj-amik.v4i3.6177>
- eSafety Commissioner. (2025, May 28). *What is doxing?* <https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing>
- 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 Civilisation*, 13(2), 132-142. <https://doi.org/10.20961/jolsic.v13i2.106262>
- Handono, S. G., Laeheem, K., & Sittichai, R. (2019). Factors related to cyberbullying among the youth of Jakarta, Indonesia. *Children and Youth Services Review*, 99, 235-239. <https://doi.org/10.1016/j.childyouth.2019.02.012>
- Herman, A. S. T. (2025). Cyberbullying sebagai Tindak Pidana: Kajian Hukum Pidana di Era Digital. *Referendum: Jurnal Hukum Perdata Dan Pidana*, 2(2), 186-202. <https://doi.org/10.62383/referendum.v2i2.912>
- Hikmawati, P. (2024). Regulasi Cyberbullying dan Perlindungan Hukum terhadap Korbannya. *Negara Hukum: Membangun Hukum untuk Keadilan dan Kesejahteraan*, 15(1), 17-35. <https://doi.org/10.22212/jnh.v15i1.4383>



- Infocomm Media Development Authority. (2026, March 31). *IMDA Issues Letters of Caution to X and TikTok* | *IMDA*. <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/imda-issues-letters-of-caution-to-x-and-tiktok>
- Infocomm Media Development Authority. (29 juni 20226). *Enhancing Online Safety in Singapore* | *IMDA*. Infocomm Media Development Authority. <https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet/online-safety>
- International TradeTrust Compliance Network. (2026, May 17). Singapore Escalates Digital Platform Regulation with Launch of Online Safety Commission and OSRAA Enforcement Regime, ITTC Network. *International TradeTrust Compliance Network*. <https://ittcnet.org/insights/singapore-escalates-digital-platform-regulation-with-launch-of-online-safety-commission-and-osraa-enforcement-regime/>
- Karomah, L., & Masyuri, M. (2024). *CULTURAL RESILIENCE IN THE ERA OF GLOBALIZATION: MAINTAINING HERITAGE AND LOCAL WISDOM FOR FUTURE GENERATIONS*. 2(2), 1635-1641.
- Kementerian Komunikasi dan Digital. (2025, July 7). *Ketika Kata Jadi Luka, Saatnya Lawan Cyberbullying Lewat Karya Anak Bangsa*. <https://www.komdigi.go.id/berita/artikel/detail/ketika-kata-jadi-luka-saatnya-lawan-cyberbullying-lewat-karya-anak-bangsa>
- Koh. (2026, June 29). OSRA, OCHA, POHA: The alphabet soup that governs Singapore's online space. *The Straits Times*. <https://www.straitstimes.com/tech/osra-ocha-poha-the-alphabet-soup-that-governs-singapores-online-space>
- Lalisu, N. A., Lembong, R. R., & Pongkorung, F. (2026). TINDAK PIDANA PENCEMARAN NAMA BAIK MELALUI MEDIA ELEKTRONIK PASCA BERLAKUNYA UNDANG-UNDANG NOMOR 1 TAHUN 2023 TENTANG KUHP. *LEX CRIMEN*, 15(3), 1-9.
- Łosiak-Pilch, J., Grygiel, P., Ostafińska-Molik, B., & Wysocka, E. (2022). Cyberbullying and its protective and risk factors among Polish adolescents. *Current Issues in Personality Psychology*, 10(3), 190-204. <https://doi.org/10.5114/cipp.2021.111404>
- Luthfiani, A., Zahra, H. A. M. A., & Khoerunisa. (2025). DAMPAK ALGORITMA TIKTOK TERHADAP KESEHATAN MENTAL REMAJA ISLAM. *Jurnal Penelitian Ilmiah Interdisipliner*, 9(12), 141-149.
- Marbun, A. O. & Bengkel. (2024). Dampak Cyberbullying Terhadap Kondisi Psikososial Remaja di Kelurahan Padang Bulan Kota Medan. *Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced*, 2(4), 829-837. <https://doi.org/10.61579/future.v2i4.214>
- Ministry of Digital Development and Information. (2024, July 2). *MCI's response to PQ on regulations on social media platforms to protect children*. Ministry of Digital Development and Information. <https://www.mddi.gov.sg/newsroom/pq-on-regulations-on-social-media-platforms-to-protect-children/>
- Ministry of Digital Development and Information. (2025, November 5). *Second Reading Opening Speech By MOS Rahayu Mahzam On The Online Safety (Relief And Accountability) Bill*. Ministry of Digital Development and Information. <https://www.mddi.gov.sg/newsroom/second-reading-opening-speech-by-mos-rahayu-mahzam-on-the-online-safety--relief-and-accountability--bill/>
- Murphy, P. (2025, November 11). Digital 2026: Top digital and social media trends in Indonesia. *We Are Social Indonesia*. <https://wearesocial.com/id/blog/2025/11/digital-2026-top-digital-and-social-media-trends-in-indonesia/>
- Nafi, K. F. N., & Nurhayati, S. (2026). *Kebijakan Perlindungan Saksi Dan Korban Di Era Digital Terhadap Tantangan Administratif Dan Hukum*. 4(2), 6252-6263.
- Oktavira, B. A. (2023). *Jerat Hukum Pelaku Cyberbullying* | *Klinik Hukumonline*. <https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-icyberbullying-i-lt6063521a8e344/>
- Pakaya, R. D., & Mahyani, A. (2022). LANDASAN PERUMUSAN LOCUS DELICTI DALAM SURAT DAKWAAN PADA KEJAHATAN SIBER. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 2(1), 673-686. <https://doi.org/10.53363/bureau.v2i1.160>
- Permaisuri, C. M. A. G., Sitorus, M. A., Devi, S., Putri, G. A., & Agustin, Y. (2025). Efektivitas Penegakan UU ITE terhadap Pidana Cyber Bullying pada Anak di Bawah Umur. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(4), 7400-7406. <https://doi.org/10.31004/riggs.v4i4.4780>
- Putra, E. N. (2019, January 30). Merunut lemahnya hukum cyberbullying di Indonesia. *AMINEF - American Indonesian Exchange Foundation*. <https://www.aminef.or.id/merunut-lemahnya-hukum-cyberbullying-di-indonesia/>



- Rusyidi, B. (2020). MEMAHAMI CYBERBULLYING DI KALANGAN REMAJA. *Jurnal Kolaborasi Resolusi Konflik*, 2(2), 100-110. <https://doi.org/10.24198/jkrk.v2i2.29118>
- Sadiq, S., Mehmood, A., Ullah, S., Ahmad, M., Choi, G. S., & On, B.-W. (2021). Aggression detection through a deep neural model on Twitter. *Future Generation Computer Systems*, 114, 120-129. <https://doi.org/10.1016/j.future.2020.07.050>
- Salsabila, F., Pawennai, M., & Mangarengi, A. A. (2026). *Hate Comment di Media Sosial: Tinjauan Hukum Berdasarkan Undang-Undang ITE*. 1(2), 1-19.
- Saputra, H. E., Abraridhandra, M. R., Hermawan, M. Z., & Suherman, A. (2026). Analisis Cyberbullying Dalam Undang-Undang Informasi Dan Transaksi Elektronik. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, 2(2), 524-527.
- Siroj, M., & Zulfa, A. (2024). *Dampak Cyberbullying Pada Remaja di Media Sosial The Impact of Cyberbullying on Teenagers on Social Media*. 1(2), 1124-1130.
- Spring, M., & Radford, M. (2026, March 16). *Meta and TikTok let harmful content rise after evidence outrage drove engagement, Whistleblowers*. BBC. <https://www.bbc.com/news/articles/cqj9kgxqjwjo>
- Syambas, N. G. (2024, September 9). *Membagongkan! Bedanya Algoritma Tiktok vs Instagram* -. <https://dipstrategy.co.id/blog/algoritma-tiktok-vs-instagram/>
- Tan, C., & Kornelis, Y. (2022). TINJAUAN YURIDIS ATAS TINDAKAN CYBERBULLYING TERHADAP PERLINDUNGAN HUKUM BAGI KONTEN KREATOR PADA APLIKASI TIKTOK. 5(1), 52-62.
- The Global Statistics. (2026, June 3). Indonesia TikTok Statistics 2026 | TikTok Active Users. *The Global Statistics*. <https://www.theglobalstatistics.com/indonesia-tiktok-user-statistics/>
- United Nations Indonesia. (2025, October 12). *Cyberbullying, Definition and Facts*. <https://indonesia.un.org/id/305496-cyberbullying-atau-perundungan-siber-pengertian-dan-fakta-faktanya>
- United Nations Office on Drugs and Crime. (2019). *Cyberstalking and cyberharassment*. : <https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html>
- U-Report Indonesia. (2019, June 3). *U-Report Indonesia*. <https://indonesia.ureport.in>
- Wafa, I. (2025). *Publik RI Habiskan Hampir 45 Jam Sebulan di TikTok, Kalahkan Rata-rata Global*. GoodStats Data. <https://data.goodstats.id/statistic/publik-ri-habiskan-hampir-45-jam-sebulan-di-tiktok-kalahkan-rata-rata-global-OxYPF>
- Yang, X., Lv, W., Reusens, M., Zhang, B., & Baesens, B. (2022). A benchmark framework for detecting cyberbullying: Conceptual and operational definitions, dataset development, and methods evaluation. *Information Processing & Management*, 63(8), 104903. <https://doi.org/10.1016/j.ipm.2026.104903>