International Journal of Religion
2024
Volume: 5| Number 11 | pp. 4435 – 4447
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/6rjzgr58

Legal Protection for Cyberbullying Victims Based on The Principle of Justice

Guruh Tio Ibipurwo[1], Slamet Suhartono[2], Yovita Arie Mangesti[3] and Erny Herlin Setyorini[4]

Abstract

One of the negative impacts information technology is cyberbullying. Cyberbullying requires specific legal framework that provides clear definitions and elements to ensure law enforcement and guarantee protection for victims. This article employs conceptual, statute, and comparative approaches to analyze how the protection of cyberbullying victims based on the principle of justice. The findings suggest that, although cyberbullying is a criminal offense, it necessitates clear regulation within laws and regulations. Cyberbullying should include victim protection and recovery, not merely punishment for perpetrators. Such guarantees should be embedded in material legal norms, specifically in Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, in a distinct article rather than merely in the Elucidation of Article 29 of the ITE Law. The scope of cyberbullying should extend not only containing threats of violence and/or intimidation, evidenced by comparative analysis with other countries.

Keywords: *Cyberbullying, Victims, Justice.*

INTRODUCTION

Globally, the use of information and communication technology has significantly altered people's behavior and ways of living. The world has become borderless due to the rapid advancement of information technology, bringing about profound and swift changes in social, cultural, economic, and law enforcement patterns. While information technology brings numerous positive impacts, it also introduces negative ones. These negative impacts affect aspects of law, SARA (ethnicity, religion, race, and inter-group relations), social, economic, and personal aspects, as well as the safety of individuals. Every year, the number of active users on social media continues to increase.

Cyberbullying first gained widespread attention in 2000. Cyberbullying, or bullying in the digital space, occurs when a person persistently abuses, harasses, or mocks others through the internet, mobile phones, or other electronic gadgets, which causes damage and involves a power imbalance and repeated victimization (Hinduja & Patchin, 2018). This behavior can manifest through emails, text messages, instant messages, and websites that contain slander, fake news, gossip, and violence. Cyberbullying is a subset of "electronic bullying" that uses electronic devices and/or the internet, fitting the exact definition. While repetition results from several persons being able to constantly witness the activity over a brief period, anonymity and the skillful use of technology by those who commit these crimes can lead to freedom from social and moral norms and power imbalances (M. Mikhaylovsky et al., 2019). Direct or indirect cyberbullying can take place when the perpetrator writes terrible things about the target victim online and receives negative feedback from others, both of which are harmful to the target victim. Research conducted across 30 countries revealed that one in three students reported being victims of cyberbullying, and one in five of these students admitted to missing school due to bullying and cyberviolence (UNICEF, 2019). From 2018 to 2022, the top three countries with the highest parent-reported cyberbullying cases were India at 37%, Brazil at 29%, and the United States at 26%. In contrast, Russia, Japan, and Chile had the lowest reported cases, at 1%, 5%, and 8% respectively (Cook, 2022).

Previous studies state that cyberbullying in some countries is a criminal offense and has been clearly regulated in laws and regulations. Sweden adheres to a system where all actions prohibited offline are also prohibited

[1] Faculty of Law, University of 17 Agustus 1945, Surabaya, Indonesia, Telp: +62 857-7712-1344, Email: guruhtio94@gmail.com, (Corresponding Author)

[2] Faculty of Law, University of 17 Agustus 1945, Surabaya, Indonesia

[3] Faculty of Law, University of 17 Agustus 1945, Surabaya, Indonesia

[4] Faculty of Law, University of 17 Agustus 1945, Surabaya, Indonesia

online (Lopez, 2020). Meanwhile, South Korea has several laws preventing cyberbullying in schools and other public places (Shin et al., 2018) by providing sanctions for violators (Korea, 2017). Although several studies regarding cyberbullying have been conducted in Indonesia, the absence of adequate laws and regulations makes it difficult for law enforcement to prosecute perpetrators (Wulandari & Suranto, 2023) and ensure protection and justice for victims.

Cyberbullying is a social problem that can result in mental health issues with physical, psychological, and social impacts. The imbalance of power causes victims to feel helpless because they cannot stop or escape digital bullying. Victims of cyberbullying have the right to justice and to hold perpetrators accountable.

Laws regarding cyberbullying are still relatively new and limited to certain countries. Several countries, including Sweden, Canada, the USA, New Zealand, South Korea, and the Philippines, have legal enforcement instruments to prevent cyberbullying. Other supporting factors, apart from government participation, involve active efforts to prevent repeated negative actions within family environments. Some countries still rely on other relevant laws, such as those on harassment and threats of violence.

Cyberbullying requires comprehensive, clear legal instruments that provide protection for victims. In Indonesia, cyberbullying regulations are outlined in Article 29 of Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (hereafter referred to as the ITE Law). Article 29 states:

"Any person who intentionally and without authorization sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at an individual." (Indonesia, 2024)

The Elucidation of Article 29 states:

"A victim is a person who experiences physical, mental suffering, and/or economic loss resulting from a criminal act. "Included in the acts referred to in this provision is bullying in the digital space (cyberbullying)."

In Article 29 of the ITE Law, cyberbullying is limited to acts of threatening violence and/or intimidation (Nansi, 2023). Increasingly sophisticated technology must be balanced with laws and regulations that address all forms of violations (Paat, 2020). Inadequate legal regulations in the national legal system regarding cyberbullying, especially concerning the definition, types, and elements, have limited law enforcement to certain cases. Many court cases involve threats of violence directly related to cyberbullying as a criminal offense under the ITE Law. Perpetrators often feel they have excessive or unlimited power because they do not face the victim directly (disinhibition) and can hide their identity (anonymity) (Ardiyani & Muhdi, 2021).

Cyberbullying, which knows no boundaries of time or place, often involves numerous bystanders, and its victims can be anyone with internet access and electronic devices, leading to a loss of privacy even within their own homes. Online cyberbullying carries a permanent characteristic due to the internet, where each occurrence can be archived indefinitely. Cyberbullies exploit the anonymity provided by the internet and electronic devices—such as Instant Messaging (IM), chatrooms, anonymous polling sites, blogs, Bluetooth bullying, social networking sites, online games, and mobile phones—to evade accountability and direct consequences for their actions, often demonstrating a lack of empathy and awareness of the negative impact of their behavior. Moreover, the absence of physical proximity between cyberbullies and their victims diminishes social barriers.

Types of cyberbullying include flaming (harsh arguments), harassment (repeated negative messages), denigration (attacks against character), impersonation/masquerading (the perpetrator pretends to be the victim) (Inayah & Nugroho, 2024), outing (embarrassing the target victim through the victim's personal data), trickery (deceiving the target victim to provide personal information), exclusion (ostracizing the target victim from online groups), cyberstalking (stalking and intimidating), sexting (posting sexual messages, comments, photos, or videos) (Minin, 2017), happy slapping (recordings of the victim being humiliated), online polls, and prank calls. Some types of cyberbullying are classified as criminal acts, while others are not yet regulated. An illustrative case from the same period involved a child in Tasikmalaya who was forced to engage in sexual relations with a cat, recorded, and the footage was distributed by his friends (BBC, 2022). This incident led to the victim experiencing severe depression, embarrassment, illness, and ultimately death. Cyberbullying incidents

contribute to various maladaptive emotional, psychological, behavioral, and physical issues (M. N. Mikhaylovsky et al., 2019), with one of the most severe consequences being an increased risk of suicidal behavior. Cyberbullying poses a more significant risk than traditional bullying, potentially exacerbating the risk of suicidal behavior. Therefore, laws and regulations should align philosophically with the foundational principles of the state. Sociologically, laws should meet the justice needs of society, and juridically, laws must be able to resolve legal problems that occur.

Based on the problems mentioned previously, two main issues will be discussed: the classification of cyberbullying as a criminal offense under current laws and regulations in Indonesia and the concept of legal protection for cyberbullying victims based on the principle of justice.

METHODS

This research employed normative legal research methods, specifically utilizing Legislative, Conceptual, Case, and Comparative Approaches to explore the subject of the study. The focus of this research included, firstly, reviewing the ITE Law, particularly the Articles that regulate cyberbullying and other relevant laws and regulations. Secondly, it examined aspects of legal protection for victims by reconstructing cyberbullying as a criminal act based on the principles of justice. This study employed three types of legal sources: primary, secondary, and tertiary. Relevant laws and regulations served as primary legal sources essential for a thorough study. Secondary legal sources—such as books, papers, journals, and relevant websites—offered context and depth to the identified research problems. Tertiary legal sources included legal dictionaries, such as Black's Law Dictionary, and commentary on court decisions. These secondary and tertiary legal materials were relevant and helped explain the selected primary legal materials.

The approach using these three sources highlighted the incompleteness of norms regulating cyberbullying crimes, particularly in the ITE Law and in several other laws considered relevant.

The Reality of Cyberbullying as a Criminal Act Based on Current Laws and Regulations in Indonesia

Cyberbullying differs from traditional bullying in several key aspects:

Reach and Persistence: The potential reach of cyberbullying is far more significant due to the rapid transmission of harmful information across many internet platforms. This can lead to a prolonged and intense experience of bullying for the victim, making it challenging for them to escape the consequences.

Anonymity: Cyberbullies often remain anonymous, which makes it much more difficult for victims to protect themselves, creating a distinct power imbalance. This anonymity can also make bullies more inclined to act aggressively, as they do not have to face the immediate reaction of the target.

Role of Bystanders: In traditional bullying, bystanders typically witness the bullying in a specific physical setting. In contrast, cyberbullying can potentially involve a large number of people, as others on the same medium can become aware of it instantly and spread the word, further complicating the situation for the victim.

Technological Facilitation: Cyberbullying commonly employs technology to harass, intimidate, or embarrass others, making it easier for bullies to be cruel without seeing the immediate reaction of the target. This can lead to a lack of hesitation in engaging in aggressive behavior, as the bully is sheltered from the victim's response.

Supervision and Feedback: Cyberbullying often lacks direct supervision and feedback, contributing to the anonymity and lack of accountability that cyberbullies may feel. This can make them more inclined to act aggressively without fear of consequences.

Publicity: Cyberbullying can be highly public, with the potential for a large audience to become aware of the bullying. This can lead to a greater sense of humiliation and isolation for the victim.

Overlapping Involvement: Many individuals involved in cyberbullying are also involved in traditional bullying, indicating significant overlap between the two forms of bullying (Wang et al., 2019).

These differences highlight the unique challenges and complexities associated with cyberbullying, which require distinct approaches to prevention, intervention, and support for victims.

Sociologically, incorporating acts of cyberbullying into laws and regulations will provide guarantees of justice, especially for victims, and efforts to enforce and prevent repeating acts in the future. The existence of legal certainty as an important instrument in law enforcement, including the provision of sanctions, ensures security and protection for victims of cyberbullying. Philosophically, cyberbullying damages the noble values of Pancasila. Cyberbullying contravenes the second principle of Pancasila, "just and civilized humanity." This behavior stems from a lack of respect for an individual's rights and dignity, where unequal treatment is based on perceived superiority in specific aspects, manifesting as violations of other people's individual rights (power imbalance). Juridically, the regulation of cyberbullying norms as a criminal act is needed to address the incomplete norms in the ITE Law. The incompleteness of norms leads to problems of legal uncertainty and undermines the protection and guarantee of justice for victims. This gap also results in multiple interpretations, which can lead to violations of victims' rights in law enforcement. One of the reasons for the high number of bullying and cyberbullying victims, which often ends tragically, is the absence of state intervention to provide protection to the victims, giving the impression that perpetrators are free from consequences. This issue is exacerbated by the unclear concept of reporting cyberbullying, whether it is a complaint or ordinary offense, potentially causing victims to fear reporting due to shame. Furthermore, existing regulations often fail to provide clear certainty and justice for the victims.

The psychological, physical, and social impacts of cyberbullying, can be more severe than traditional bullying. Psychological impacts include feelings of helplessness, poor concentration and focus, isolation and secrecy, depression, anger and aggression, anxiety, low self-esteem, suicidal thoughts (Ardiyani & Muhdi, 2021), eating disorders, substance abuse, and Post Traumatic Stress Disorder (PTSD). Physical impacts can be both direct and indirect, such as self-abuse, self-injury, self-torture through not eating, and even suicidal behavior (Opp, 2020). Social impacts include a loss of interest in social activities, such as missing school, not working, or not participating in recreational activities. Additionally, social issues often involve carrying sharp weapons in public places to harm others or commit suicide (Alcera, 2020).

Key characteristics of cyberbullying include:

It can occur anywhere and at any time, with continuous access, and its effects can be permanent.

Information spreads rapidly to a broad audience.

The behavior is repeatable, and material can be easily copied and widely distributed.

Perpetrators can remain anonymous, avoiding direct confrontation with their victims.

Tracking cyberbullying perpetrators is more challenging.

Victims of cyberbullying struggle to confront their bullies in person.

Victims also face difficulties in social interactions.

The perpetrator and victim do not need to be in the same geographical location.

Cyberbullying typically involves verbal, emotional, and psychological abuse, rather than physical.

There is a tendency for more damaging attacks due to online disinhibition effects and a lack of monitoring of online behavior (Kenworthy, 2019).

Cyberbullying encompasses several aspects, including:

Repetition

Repetition is the most important element of intimidation. It is easily recognizable and often occurs in cyberspace, causing significant distress to victims (Ziems et al., 2020).

Intention

Intention in the context of intimidation is defined as an action carried out deliberately to harm someone.

Harm

Harm in the context of intimidation is defined as something dangerous that can injure the victim in various ways. The disadvantages of this dangerous concept can be physical, social, psychological, behavioral, or emotional.

Power Imbalance

Power imbalance occurs when the bully has actual or perceived greater power than the victim (Pyżalski et al., 2022).

Cyberbullying regulations in the ITE Law are explicitly stated in the Elucidation of Article 29, which states:

"Any person who intentionally and without authorization sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at an individual (Indonesia, 2024).

Meanwhile, Article 45 B states:

"Any person who intentionally and without authorization sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at an individual as referred to in Article 29 shall be punished with imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR750,000,000.00 (seven hundred and fifty million rupiahs).

Referring to the Elucidation of Article 29 in conjunction with Article 45B of the ITE Law reads: "The provisions in this article also include bullying in the digital space (cyberbullying) which contains elements of threats of violence or intimidation and results in physical and psychological violence and/or material loss." This partial regulation suggests that cyberbullying is limited to the regulations in Article 29 of the ITE Law. However, its application is broader than the Elucidation of Article 29 of the ITE Law. The incomplete regulation of cyberbullying in Indonesia's ITE Law raises problems of legal certainty regarding whether cyberbullying is included in Indonesian laws and regulations as a criminal offense. The Elucidation of Article 29 of the ITE Law is an extension of the criminal act of threatening violence and/or intimidating online. However, it is necessary to clarify the definition, types, and elements of criminal acts of cyberbullying, which should be normalized in the ITE Law and its implementing regulations. Several actions outside Article 29 of the ITE Law can be categorized as criminal acts of cyberbullying.

The current ITE Law requires additional norms, especially regarding cyberbullying in aspects of prevention, protection, and guaranteeing justice for victims. Cyberbullying cannot be equated with ordinary immoral acts, attacks on honor, or threats of violence. There are important parts that should be regulated in the ITE Law, its derivatives, and other laws, specifically the protection of victims and restoration of conditions (Dahri & Yunus, 2022).

Cyberbullying is a crime that falls under cybercrime, which is regulated in CHAPTER VII concerning Prohibited Actions in the ITE Law. In the ITE Law, cyberbullying perpetrators can be charged under Article 27 paragraph (1), paragraph (3), paragraph (4), Article 28 paragraph (2), and Article 29, provided they fulfill the elements and scope of these provisions. However, cyberbullying is not clearly and unequivocally described in the ITE Law. The norms for fulfilling these elements still use articles that are considered relevant and can be linked to general crimes in the digital space (cybercrime) that threaten the privacy of others. However, there has been no effort to specifically address the cyberbullying offense in the ITE Law. The term "cyberbullying" is only implicitly included in the Elucidation of Article 29 of the ITE Law without providing any definition, scope, or elements of this action. No regulations in other laws, including the new Criminal Code (Law Number 1 of 2023), clearly and completely address the elements and protection of victims of cyberbullying.

This situation is not in line with Article 28G paragraph (1) and paragraph (2) of the 1945 Constitution of the Republic of Indonesia, which reads:

Every person has the right to protection of himself, his family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear of doing something which is a human right.

Every person has the right to be free from torture or treatment that degrades human dignity and has the right to obtain political asylum from another country (Indonesia, 2002).

The norming of cyberbullying as a criminal act should be included in the ITE Law to ensure legal certainty and provide accessibility to justice and guarantees of protection for victims. These norms must be written (lex scripta) in both laws and government regulations and stated clearly and completely, including the elements, criminal threats, fines, restitution, compensation, forms of rehabilitation, public participation, and the roles of the state and related authorities and institutions.

Concept Of Legal Protection for Victims of Cyberbullying Based on The Principle of Justice

Cyberbullying Regulatory Policies in Several Countries

Table 1. Comparison between New Zealand and Indonesia

Difference Clause	New Zeland	Indonesia
Regulation in Legislation	It is specifically regulated in the Harmful Digital Communication Act (HDCA), which includes law enforcement efforts and protection against cyberbullying, stalking, and online harassment. It covers all harmful digital communications, such as text, email, or social media content containing racist, sexist, and intolerant comments.	It is limited to relevant laws addressing elements of threats of violence and/or intimidation.
Compensation imposed on perpetrators for victims	In the HDCA, compensation for victims, both from perpetrators and the government, is clearly regulated.	Compensation is limited to criminal acts of human rights violations, trafficking in persons, and terrorism. Restorative justice for certain criminal acts is only regulated internally by the Police, Prosecutor's Office, and Supreme Court, not yet by law.
Institutional Role	There is an independent institution with the authority to provide education, services, and protection to victims of cyberbullying called NetSafe. This institution has the authority to provide a way out for victims before they go to the police or district court. Officially, Netsafe's responsibilities include handling complaints related to harmful digital communications, educating the New Zealand population about such issues, and supporting the online safety community serving New Zealand. Netsafe has a responsibility to help resolve reports regarding alleged violations of the ten communication principles.	There is no specific institution with full responsibility to provide education and services for victims of cybercrime. Litigation is the main method of dispute resolution for cyber crimes. Cyberbullying lacks specialized institutions.
Dispute Resolution	Reports to NetSafe can be used as a basis for victims to demand compensation from perpetrators, both civilly and criminally, for the impacts caused.	Dispute resolution relies on amicable approaches, exacerbated by low awareness among victims' families regarding the legal processes for cyberbullying. In fact, it is common for the victim's family to accept that the victim died or committed suicide and consider it a disaster. Another resolution route is litigation, but due to incomplete norms, law enforcement officials often provide a peaceful resolution.
Repetition	In New Zealand law, the penalties for repeated criminal acts, especially for criminal acts in the digital space, will be very severe: Imprisonment of up to three years for the new crime of incitement to suicide.	Sanctions for repeated criminal acts have not yet been regulated in the ITE Law and only refer to the Criminal Code.
Sanctions	Criminal sanctions that may be imposed under the HDCA 2015 are a fine of up to $50,000 for individuals or up to $200,000 for legal entities, or up to two years of imprisonment for posting or sending digital communications with intent to cause harm.	Regulated in Article 45B in conjunction with Article 29 of the ITE Law with a maximum penalty of 4 years and/or a maximum fine of IDR750,000,000 (seven hundred and fifty million rupiah). Actions that are punishable by crime are only limited to threats of violence and/or intimidation (for criminal acts that actually regulate cyberbullying).
Criminal Act	Expanded complaint offense	Complaints of several relevant offenses. For example, Article 27 paragraph (3) of the ITE Law concerning insults and/or defamation is a complaint offense.

Source: Author, 2024

Table 2. Comparison between South Korea and Indonesia

Difference Clause	South Korea	Indonesia
Elements of cyberbullying in criminal law regulations	Regulated in: 1. Act on the Promotion of Information and Communications Network Utilization and Information Protection (penal); 2. Act on the Prevention of and Countermeasures Against Violence in Schools (non-penal). Some of the regulated actions include flaming, harassment, denigration, impersonation, outing, trickery, and cyberstalking.	Regulated in: 1. The ITE Law (Article 29 in conjunction with Article 45B); 2. Several other laws and regulations considered relevant (though not clearly include cyberbullying), such as the Criminal Code, the Witness and Victim Protection Law, and the Personal Data Protection Law.
Sanctions	- Criminal threats specifically mention the criminal threat of cyberbullying. The criminal threat depends on the type of cyberbullying act committed. For example, in Article 44-7 paragraph (1), defamation by revealing untrue facts or facts that degrade someone's reputation is punishable under Article 70 paragraph (2) with imprisonment for up to 7 years and a fine not exceeding 50 million won. In Article 70-2, spreading malicious programs is punishable by imprisonment for up to 7 years or a fine of not more than 70 million won. - There are also sanctions in school environments.	Regulated in Article 29 in conjunction with Article 45B of the ITE Law: "Any person who intentionally and without authorization sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at an individual as referred to in Article 29 shall be punished with imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR750,000,000.00 (seven hundred and fifty million rupiah)."
Others sanctions	These sanctions only apply in the school environment for perpetrators of crime and violence, including cyberbullying, as regulated in the Act on the Prevention of and Countermeasures Against Violence in Schools. For perpetrators under this law, there are no fines or prison sanctions, only administrative sanctions/punishments applicable in schools. Sanctions for Aggressor Students: 1) Requirement to issue a written apology to the victim; 2) Ban on contacting, threatening, or retaliating against victims or students who report school violence; 3) School services; 4) Community service; 5) Completion of special education or psychological treatment by internal or external experts; 6) Attendance suspension; 7) Class changes; 8) Transfer to another school; 9) Expulsion from school. Sanctions for Students leaking data: A maximum prison sentence of 1 year or a fine of 10 million won.	Other sanctions are not regulated normatively.

Source: Author, 2024

Penal and Non-Penal Policies in Overcoming Cyberbullying Crimes

In the ITE Law, perpetrators of cyberbullying can currently be charged under Article 27 paragraph (1), paragraph (3), paragraph (4), Article 28 paragraph (2), and Article 29, even if they do not fulfill the elements and scope of the definition of the action. Norms in fulfilling these elements still use articles that are considered relevant in relation to cybercrime in general, which threatens other people's privacy (for example, insults in cyberspace) without any effort to perfect the cyberbullying offense in the ITE Law. Meanwhile, the word "cyberbullying" is only explicitly included in the Elucidation to Article 29 of the ITE Law and does not provide limitations on the definition, scope, and elements of this action.

According to Article 29 of the ITE Law, sanctions for student aggressors encompass cyberbullying, which involves threats of violence or intimidation leading to physical and psychological violence and/or material loss. However, in applying this article, it must be taken into account that the element of "threat of violence or personal intimidation" needs to be seen as stating someone's intention to do something harmful or detrimental

to another party with violence or physical pressure. In this case, the statement is delivered via electronic media or an electronic system such as SMS, telephone, or email. Meanwhile, scaring is carrying out actions using or through electronic systems or electronic media in various ways to make someone afraid or feel threatened in their right to privacy or feel unsafe. Threats of violence or actions that scare must be directed at certain people and result in a substantial adverse effect on the victim's emotional state or well-being, such as causing pain, prolonged stress, or worry. The application of Article 29 of the ITE Law is different from the element of cyberbullying, as Article 29 is a general offense, with a threat that can materialize even with a single instance. This creates a difference with the elements of cyberbullying, especially when sent repeatedly. This regulation is a Joint Decree of Three Ministers Number 229 of 2021, Number 154 of 2021, and Number KB/2/VI/2021 on the Implementation Guidelines for Certain Articles in the ITE Law.

Marc Ancel's definition characterizes criminal policy or criminal politics as society's systematic and logical approach to addressing crime, termed "the rational organization of the control of crime by society." (Maroni, 2016) According to Barda Nawawi Arif in John Kenedi, diverse approaches to addressing crime through criminal policy include the "application of criminal law, prevention without punishment," and shaping societal perceptions of crime and punishment via mass media (Kenedi, 2017). Apart from employing repressive methods like the application of penal or criminal laws, criminal policy can also be implemented through non-penal approaches or preventive measures without resorting to punishment. Barda Nawawi Arief emphasizes the importance of exploring, developing, and utilizing community support and participation to enhance and effectively develop the existing "extra-legal" or "informal and traditional systems" through this non-penal means (Arief & Nawawi, 2005).

In addition to penal efforts in law enforcement against cyberbullying, a formulation of non-penal measures oriented towards protecting and restoring the victim's condition is required. In the ITE Law, the formulation of non-penal measures is not found. The ITE Law currently in effect only focuses on penal measures that lead to deterrence policies against perpetrators without paying attention to the interests of victims. The need for an adequate formulation regarding ongoing efforts towards victims is based on the existing fact that victims are people whose honor and dignity as human beings are oppressed by others. The victim is in the lowest and most disadvantageous position. Victims of cyberbullying do not know that they are affected by violations of irresponsible use of information technology by others, and they do not even know who the perpetrator is physically (anonymous). Non-penal efforts in reforming criminal law are needed as an effort to guarantee protection and justice for victims. Indonesia's Witness and Victim Protection Law should be able to expand and accommodate criminal acts that cause impacts not only physical but also mental/psychological and social, including cyber crimes.

Non-penal efforts that can be taken to prevent cyberbullying involve strategies that focus on preventing and controlling crime before a criminal act occurs. Some non-penal efforts that can be taken to prevent cyberbullying include:

Cultural Approach: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media.

Moral Approach: Increasing noble moral values through religious and moral education.

Scientific Approach: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through scientific education.

Technological Approach: Utilizing software, such as ReThink Stopcyberbullying, to prevent cyberbullying (Frensh & Zulyadi, 2023).

Religious Education: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through religious education.

Moral Education: Increasing noble moral values through moral education.

Scientific Education: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through scientific education.

Technology Education: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through technology education.

Dissemination of Internet Ethics: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through the dissemination of Internet ethics.

Participatory Supervision: Increasing public awareness about cyberbullying and the importance of ethics in interacting on social media through participatory supervision (Amalia et al., 2024).

Thus, these non-penal efforts can help prevent cyberbullying and increase public awareness about the importance of ethics in interacting on social media.

Reconstructing Cyberbullying Norms as a Protection Effort for Victims

Indonesia is a state of law, as explained in Article 1 paragraph (3) of the 1945 Constitution. Therefore, a proportional legal system is needed in social life to create a harmonious and orderly society. According to the founding fathers' ideals of the nation and the mandate of the law, Pancasila serves as the source of all sources of law in Indonesia, as stated in Article 2 of Law Number 12 of 2011 on the Establishment of Laws and Regulations, which has been amended by Law Number 13 of 2022 on the Second Amendment to Law Number 12 of 2011. Nonetheless, laws or regulations often fail to encompass all scenarios that arise in societal dynamics, posing challenges for law enforcement in resolving such matters. The enforcement and application of laws, particularly in Indonesia, frequently encounter challenges associated with societal development. The development of society, which is faster than the development of laws and regulations, often leads to issues that laws and regulations have not yet addressed or do not currently regulate, thereby potentially giving rise to legal vacuums, conflicting norms, incomplete norms, or vague norms.

According to positive law, incomplete norms refer to the inadequacies in norms that regulate certain actions, leading to uncertainty in their application. The incompleteness of these norms may lead law enforcement officials to make superficial interpretations, which can result in injustice, especially toward victims. The incompleteness of norms in regulating positive law in the most recently passed ITE Law can arise from delays on the part of the authorities responsible for drafting legal regulations, namely the executive and legislative bodies. This extended timeframe may result in the regulation becoming outdated by the time it is enacted, as the societal conditions and issues it aims to address may no longer be relevant due to ongoing societal developments. Therefore, it is common for relevant regulations whose elements do not fully meet the definition of an offense to still be enforced. As is the case with the crime of cyberbullying, the formulation is only intended for Article 29 in conjunction with Article 45B of the ITE Law, which is limited to the formulation of the offense of threatening violence or causing personal intimidation. Meanwhile, the formulation of the offense of cyberbullying is quite broad and goes beyond what is formulated in that article. The government often finds inconsistency in implementing laws in an effort to ensure legal certainty in society.

Criminal law has experienced a paradigm shift, especially starting in Western European countries in the 1990s, which is universally applicable. The evolution of criminal law's functions is evident in the effectiveness of criminal law's punishments, which are no longer oriented towards retribution but have changed to just punishments with corrective, rehabilitative, and restorative functions. This shift cannot be separated from the neo-classical school of criminal law called *daaddader strafrecht*, meaning that criminal law is not only oriented toward the act but also towards the perpetrator. In its development, this paradigm also began to focus on victim protection, giving rise to what is called restorative justice. Corrective justice is oriented towards the perpetrator (accountability of the criminal) to be sanctioned. Restorative justice is oriented toward victims, while rehabilitative justice is oriented toward both perpetrators and victims. Rehabilitative justice aims to prevent the recurrence of crimes when the perpetrator has returned to social life. From the victim's perspective, the goal is to recover, rehabilitate, and protect the victim so that the victim's rights can be restored. The new paradigm in criminal law is a momentum for changing the functions of conventional criminal law toward modern criminal law. These legal functions are carried out to achieve the goals outlined in our constitution, namely safeguarding the entire Indonesian nation and its people.

Furthermore, Friedman states that a legal system (including the Indonesian legal system) includes at least the following subsystems or elements:

Legal Substance: This includes the regulations used by perpetrators and law enforcers when carrying out legal acts and legal relations. The legal substance is found or can be found in formal legal sources.

Legal Structure: This is a pattern that shows how the law is implemented according to its formal provisions.

Legal Culture: It is defined by Friedman as demands or requests from the people or users of legal services. These demands or requests are usually driven by interests, knowledge, experience, ideas, attitudes, beliefs, hopes, and opinions (judgments) regarding the law and its enforcement institutions (Rahardjo, 2000).

In legal theories, three aspects are usually distinguished regarding the application of law as a rule. Soerjono Soekanto states:

Legal rules apply juridically if their determination is based on rules of a higher level or more structured according to a predetermined method, or if they show a necessary relationship between a condition and its consequences.

Legal rules apply sociologically if the rule is effective, meaning that the rule can be enforced by the authorities even though it is not accepted by members of the community, or the rule applies because it is accepted and recognized by society.

Legal rules apply philosophically if they are in accordance with the ideals of law as the highest positive value (Shalihah, 2017).

Additionally, a moral/educational approach, a cultural approach, and even a global approach (international cooperation) are also required because this crime transcends national boundaries (is "transnational/transborder"), and often the perpetrators are anonymous and plural (Arief & Nawawi, 2005). Therefore, reforming the criminal law (the Civil Code) in the context of dealing with cyberbullying is a non-negotiable necessity.

Philosophically, the development of information globalization, which has placed Indonesia as part of the world information society, has resulted in a high intensity of communication and interaction. On the other hand, as a country that adheres firmly to the values of Pancasila and the 1945 Constitution, the reality of information globalization must still be positioned as a development that remains within the religious and moral values of the Indonesian nation and legal norms. Even though it seems as if the law is always limping along with changing times (*het recht hink achter de feiten aan*), the basic values of Pancasila need to be operationalized by making Pancasila the basis for formulating norms. Indonesia has a national law, which is a unified legal system based on Pancasila. Pancasila serves as a basic norm (*grundnorm*) or a fundamental norm of the state (*staatsfundamentalnorm*) in the hierarchy of legal norms. The values of Pancasila are then explained in various existing regulations. Laws and regulations in the country essentially include instrumental values as an elaboration of Pancasila values. Norming cyberbullying as a criminal act is an embodiment of the values of Pancasila, especially the second principle. Humans are placed in a civilized position to respect each other, and their rights are guaranteed to be protected.

Reconstruction of cyberbullying as a criminal act includes:

The inconsistency between the meaning of Article 29 of the ITE Law based on the Joint Decree of Three Ministers Number 229 of 2021, Number 154 of 2021, and Number KB/2/VI/2021 and the elements and characteristics of cyberbullying creates a space for legal uncertainty. First, the meaning of threats of violence and/or intimidation is one of the broad elements of cyberbullying, leading to a shallow interpretation of the elements presented in Article 29 of the ITE Law concerning cyberbullying. Second, Article 29 does not meet the characteristics of cyberbullying, namely repeated acts. Based on the Joint Decree of Three Ministers, it is formulated that these threats can be subject to criminal sanctions even if they are only sent once. This differs from cyberbullying, which involves repeated acts by the perpetrator.

Based on Law Number 13 of 2022 on the Second Amendment to Law Number 12 of 2011 on the Establishment of Laws and Regulations, Article 10 paragraph (1) point e, which addresses fulfilling legal needs in society, there is a need to accommodate acts of cyberbullying in the ITE Law. This ensures legal certainty and protection amidst the current development of information technology, as well as constitutes efforts to prevent similar repeated acts that could lead to other social problems.

In the formulation of Law Number 1 of 2023 on the Criminal Code, there is still no regulation regarding cyberbullying. Meanwhile, the legal basis that can currently be used, namely the ITE Law, especially in the Elucidation of Article 29 on the definition, scope, and elements, remains incomplete. It is still absolutely necessary to use the ITE Law in resolving cyberbullying cases, even though the existing legal norms are incomplete and there is a potential for a void in norms (recht vacuum).

There is no real victim protection contained in the ITE Law, especially in relation to victims of cyberbullying. Norms regarding victim protection should be accommodated in the ITE Law through reporting accessibility, restitution, and compensation, including rehabilitation efforts. It is necessary to broaden the offense classification based on the types of cyberbullying, extending beyond mere complaints to include specific acts of cyberbullying. This can involve expanding the offense of complaints (as outlined in Articles 411 and 412 of the new Criminal Code) or including general offenses (as outlined in Article 29 of the ITE Law).

Juridically, norms regarding cyberbullying offenses must be clearly defined in accordance with the scope that applies internationally. Cyberbullying, which can occur in multiple countries, requires regulation and identification of cyber acts, especially regarding cyberbullying.

Based on point e, addressing cyberbullying, which is an information technology crime, requires not only penal measures but also non-penal approaches Non-penal measures represent a balanced approach that lawmakers should consider to ensure protection, security, and justice for all users of information technology, particularly for victims.

Non-penal efforts include a culture-based approach by prioritizing cyber ethics; moral and educational approaches in schools, workplaces, and family environments; a scientific approach involving academics in studying aspects of prevention, formulating policies to eradicate cyberbullying, and protecting victims; a technological approach by installing parental control applications on children's gadgets; a government policy approach by establishing a supervisory institution, such as Netsafe in New Zealand, disseminating the dangers of cyberbullying, and creating anti-cyberbullying educational sites along with preventive and handling efforts, including closing accounts that are indicated to have committed cyber violations; an international cooperative approach, especially related to collaborative efforts through online media platforms, such as Instagram and Twitter, to limit the space for cyberbullying and hate speech; and a media/journalistic approach.

CONCLUSION

Cyberbullying is regulated under the Elucidation of Article 29 of the ITE Law, but the current provisions are incomplete and lack clear norms regarding cyberbullying as a criminal act. Many cases do not specifically address cyberbullying in lawsuits but instead rely on articles that are no longer relevant to the characteristics, types, and elements of cyberbullying. Types of cyberbullying include flaming, harassment, denigration, impersonation, exclusion, cyberstalking, sexting, happy slapping, prank calls, and pseudonyms. The impacts of cyberbullying are extensive, causing physical, psychological, and social harm to victims and even material losses. The ITE Law should expand its definition, types, and elements to encompass actions beyond the current provisions of Article 29.

The concept of reconstructing cyberbullying norms can be analyzed through sociological, philosophical, and juridical lenses: Philosophically, Pancasila can serve as the foundation for formulating these norms. Sociologically, addressing the criminal act of cyberbullying can involve non-penal efforts with an integral/systemic approach oriented towards cultural, techno-prevention, rehabilitative, and cultural and religious-based socio-educational approaches, which require collaboration between communities and government, supported by a clear and comprehensive legal framework, as well as international cooperation, particularly with social media platform providers. Juridically, it is essential to add norms to the ITE Law to

explicitly classify cyberbullying as a criminal offense. This includes expanding its definition, types, and elements. Cyberbullying could be categorized under either an expanded complaint offense or a general offense, depending on the nature of the crime. Moreover, the criminal liability should extend beyond the perpetrator to include individuals who participate in the recording and dissemination of such acts (e.g., "happy slapping") and internet trolls (provocateurs and instigators). Comparatively, research indicates that several countries, such as Sweden, New Zealand, and South Korea, have successfully incorporated regulations addressing cyberbullying within their laws and regulations.

REFERENCES

Alcera, E. C. (2020). What Are the Effects of Cyberbullying? Hackensack Meridian Health. https://www.hackensackmeridianhealth.org/en/healthu/2020/08/17/what-are-the-effects-of-cyberbullying

Amalia, C. R. S., Anggraini, A. U., Rato, D., & Setyawan, F. (2024). Non-Penal Policy In Tackling Cyber-Bullying Through Integrated Cyber-Prevention. Jurnal Legalitas, 17(1), 38-48. https://doi.org/10.33756/jelta.v17i1.24900

Ardiyani, I., & Muhdi, N. (2021, 12/16). Cyberbullying And Suicidal Behavior. International Journal of Research Publications, 92. https://doi.org/10.47119/IJRP100921120222653

Arief, & Nawawi, B. (2005). Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan, 1st ed. Citra Aditya Bakti.

BBC, H. K. (2022). Kasus Bullying Di Tasikmalaya, 3 Tersangka Dikembalikan Ke Orang Tua. BBC News. https://www.cnnindonesia.com/nasional/20220727154327-12-826933/kasus-bullying-di-tasikmalaya-3-tersangka-dikembalikan-ke-orang-tua.

Cook, S. (2022). Cyberbullying Statistics and Facts for 2023. Comparitech. https://www.comparitech.com/internet-providers/cyberbullying-statistics/

Dahri, I., & Yunus, A. S. (2022). Pengantar Restorative Justice. Guepedia.

Frensh, W., & Zulyadi, R. (2023). Kebijakan Non Penal Dalam Upaya Penanggulangan Perundungan Di Ruang Siber. Journal Justiciabelen (JJ), 3(02), 70-79. https://doi.org/10.35194/jj.v3i02.3081

Hinduja, S., & Patchin, J. (2018, 08/22). Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying. Journal of School Violence, 18, 1-14. https://doi.org/10.1080/15388220.2018.1492417

Inayah, J. N., & Nugroho, T. (2024). Criminal Implementation of Cyberbullying Based on Electronic Information and Transaction Law and Islamic Law. JURNAL USM LAW REVIEW, 7(1), 252-268.

Indonesia, R. (2002). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Amandemen Ke-4). Pub. L. No. Undang-Undang Dasar Republik Indonesia Tahun 1945, Sekretariat Negara Republik Indonesia 1.

Indonesia, R. (2024). Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Pub. L. No. 1, 39.

Kenedi, J. (2017). Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia, ed. Sirajuddin, Pustaka Pelajar, Cet. 1. Pustaka Pelajar.

Kenworthy, H. (2019). Cyberbullying in Education: A Literature Review. The University of Akron.

Korea, R. o. (2017). Problems and Improvements of The Act on the Prevention and Countermeasures against Violence in School. Pub. L. No. Act No. 15044, Korea Legislation and Research Institute 20. https://doi.org/10.31839/dalr.2018.02.78.405

Lopez, S. (2020). Online Harassment: How Is the Regulation in Sweden? The Newbie Guide to Sweden. https://www.thenewbieguide.se/online-harassment-how-is-the-regulation-in-sweden

Maroni, M. (2016). Pengantar Politik Hukum Pidana. CV. Anugerah Utama Raharja.

Mikhaylovsky, M., Lopatkova, I., Komarova, N., Rueva, E., Tereschuk, K., & Emelyanenkova, A. (2019, 11/15). Cyberbulling as a new form of a threat: a physiological, psychological and medicinal aspects. Electronic Journal of General Medicine, 16. https://doi.org/10.29333/ejgm/114268

Mikhaylovsky, M. N., Lopatkova, I. V., Komarova, N. M., Rueva, E. O., Tereschuk, K. S., & Emelyanenkova, A. V. (2019). Cyberbulling as a new form of a threat: a physiological, psychological and medicinal aspects. Electronic Journal of General Medicine, 16(6).

Minin, A. R. (2017). Kebijakan kriminal terhadap tindak pidana intimidasi di internet (Cyberbullying) sebagai kejahatan mayantara (cybercrime). Legalite: Jurnal Perundang Undangan dan Hukum Pidana Islam, 2(II), 1-18. https://doi.org/10.32505/legalite.v2iII.345

Nansi, W. S. (2023). Cyberbullying Formulative Problems Against Child Protection in Indonesia. Constitutional Law Review, 2(2), 113-128.

Opp, K.-D. (2020). Analytical criminology: Integrating explanations of crime and deviant behavior. Routledge.

Paat, L. N. (2020). Kajian Hukum Terhadap Cyber Bullying Berdasarkan Undang-Undang Nomor 19 Tahun 2016. Lex Crimen, 9(1).

Pyżalski, J., Plichta, P., Szuster, A., & Barlińska, J. (2022, 09/14). Cyberbullying Characteristics and Prevention-What Can We Learn from Narratives Provided by Adolescents and Their Teachers? International Journal of Environmental Research and Public Health, 19, 11589. https://doi.org/10.3390/ijerph191811589

Rahardjo, S. (2000). Ilmu Hukum, 3rd ed. PT. Citra Aditya Bhakti.

Shalihah, F. (2017). Sosiologi Hukum, Pustaka Ekspresi, Ed.1 Cet.1. Rajawali Press.

Shin, J. Y., Lim, J. W., Shin, D. W., Kim, S. Y., Yang, H. K., Cho, J., Jeong, A., Jo, D., Yim, C. Y., Park, K., & Park, J.-H. (2018, 01/15). Underestimated caregiver burden by cancer patients and its association with quality of life, depression and anxiety among caregivers. European Journal of Cancer Care, 27, e12814. https://doi.org/10.1111/ecc.12814

UNICEF, P. (2019). More than a third of young people in 30 countries report being a victim of online bullying. https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

Wang, C.-W., Musumari, P. M., Techasrivichien, T., Suguimoto, S. P., Tateyama, Y., Chan, C.-C., Ono-Kihara, M., Kihara, M., & Nakayama, T. (2019, 2019/12/30). Overlap of traditional bullying and cyberbullying and correlates of bullying among Taiwanese adolescents: a cross-sectional study. BMC Public Health, 19(1), 1756. https://doi.org/10.1186/s12889-019-8116-z

Wulandari, A., & Suranto, A. (2023). How do schools in Indonesia fight against cyberbullying? Jurnal Civics: Media Kajian Kewarganegaraan, 20(2), 333-340. https://doi.org/10.21831/jc.v20i2.57716

Ziems, C., Vigfusson, Y., & Morstatter, F. (2020). Aggressive, repetitive, intentional, visible, and imbalanced: Refining representations for cyberbullying classification. Proceedings of the International AAAI Conference on Web and Social Media,