Positive Criminal Law Regulations Regarding the Crime of Cyberbullying as a Form of Cyber Crime

Richard Chandra Adam

richardc@fh.untar.ac.id

Faculty of Law, Tarumanagara University

Article Info

Received: 2023-11-16
Revised: 2024-02-12
Accepted: 2024-03-19

Keywords:
Cyberbullying; ITE Law; Criminal Law; Freedom of Speech; Victim Protection

Abstract

This research aims to examine positive criminal law regulations related to criminal acts of cyberbullying as a form of cybercrime in Indonesia. Through a legislative approach, this research analyzes related legal developments in cyberbullying, with a focus on Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and amendments through Law Number 19 of 2016. The research results show that the ITE Law provides a strong legal basis for dealing with cyberbullying, with heavy sanctions for perpetrators. However, this regulation has also drawn criticism regarding potential restrictions on freedom of speech. Thoughtful law enforcement, education, and awareness of online ethics are important in addressing this problem. Legal changes and a holistic approach are needed to face challenges in the ever-evolving digital era.

I. Introduction

Criminal act of cyberbullying, which refers to harassment via electronic media, is an increasingly pressing issue in today's digital age. In the context of criminal law in Indonesia, related regulations on cyberbullying have experienced relevant developments and changes. This article will review changes in laws and regulations related to criminal acts of cyberbullying in Indonesia, with a focus on Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as well as amendments accommodated through Law Number 19 of 2016. Apart from that, this article will also discuss the definition of cyberbullying, the surrounding legal implications, as well as the sanctions that apply to the perpetrator of cyberbullying. Cyberbullying refers to aggressive and malicious behavior carried out by individuals or groups, using electronic media such as the internet and electronic-based devices, such as cellphones, computers, and social media platforms. Action of cyberbullying is often repeated and aimed at someone who is considered less capable of resisting these actions. The power differential in this context refers to perceptions of physical and mental capacity, with the victim often placed in a more vulnerable position than the perpetrator.

Before the ratification of the ITE Law, regulations were often used to handle cases of cyberbullying that were the Criminal Code. Article 310 paragraphs (1) and (2) of the Criminal Code regulates insults and defamation. However, the Constitutional Court Decision Number 50/PUU-VI/2008 has provided clarification that this provision cannot be used to overcome acts of cyberbullying. In 2016, Indonesia issued Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. These changes involve adding provisions that explicitly regulate acts of cyberbullying, which in turn provides a stronger legal basis for dealing with such cases.

One of the most relevant legal regulations related to cyberbullying in Indonesia is the ITE Law and its amendments which are regulated through Law Number 19 of 2016. Article 45 paragraph (3) of the ITE Law regulates acts of cyberbullying as a criminal offense that states, "Any person who intentionally and without right distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing insulting and/or defamatory content as intended in Article 27 paragraph (3) shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of IDR 750,000,000.00 (seven hundred and fifty million rupiah)." Meanwhile, article 27 paragraph (3) of the ITE Law states that every person intentionally and without right distributes and/or transmits and/or makes information accessible electronic and/or electronic documents containing insulting and/or defamatory content shall be punished with a maximum imprisonment of 6

(six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

Legal arrangements that include cyberbullying in the ITE Law have serious legal implications for the perpetrators of these actions. Action cyberbullying involving insults and defamation through electronic media is considered a criminal offense. Perpetrator cyberbullying can be sentenced to a criminal sentence of up to 4 years in prison and/or a fine of IDR 750,000,000.00. These implications create a solid legal basis for pursuing action cyberbullying and protect victims from online harassment. However, it should be emphasized that the law must be implemented wisely and fairly, considering the complexity and variety of cases involved cyberbullying.

Although the ITE Law has provided a legal basis for handling cyberbullying, this regulation has also attracted criticism and controversy, especially in several aspects. One of the main criticisms is that the ITE Law can be used to limit freedom of expression and opinion. Several cases of law enforcement under the ITE Law have been criticized because they are considered to hamper freedom of speech and opinion in cyberspace. Apart from that, the ITE Law has also been criticized because the sanctions are very heavy and not always commensurate with violations that may be relatively minor. These high fines and imprisonment can be considered a tool of excessive pressure, especially in the context of the action cyberbullying which may not always have serious consequences commensurate with the penalties imposed.

Existing legal arrangements also provide protection for victims cyberbullying. Victims can report the action cyberbullying to the authorities, who can then take legal steps to prosecute the perpetrator. Additionally, many social media platforms and other online services also have anti-cyberbullying and reporting mechanisms that enable victims to report acts of harassment. So education and awareness play an important role in efforts to protect victims cyberbullying and prevent such actions. Education regarding online etiquette, respectful behavior, and awareness of the impact of action cyberbullying can help reduce these incidents.

There are several cases of cyberbullying emerging in Indonesia that illustrate the complexity of this problem and its impact on society. One well-known case is that of Baiq Nuril Maknun, a teacher who was convicted of distributing audio recordings of sexual harassment she experienced by her superiors. This case sparked discussions about protection for victims of sexual harassment and the need for legal changes that are more judicious in handling cases of this kind. However, there are legal regulations regarding criminal acts of cyberbullying in Indonesia that have experienced development over time. The ITE Law and its amendments through Law Number 19 of 2016 provide a strong legal basis for handling actions of cyberbullying involving insults and defamation through electronic media. The serious legal implications, including imprisonment and high fines, aim to protect victims and deter reoffenders of cyberbullying

However, this legal arrangement has also attracted criticism and controversy, especially regarding the potential for abuse and violation of freedom of speech. Therefore, law enforcement must be carried out wisely and fairly, taking into account the context and impact of the action of cyberbullying. Apart from the law, education and awareness regarding online ethics are also important in prevention efforts of cyberbullying and protect victims. Thus, legal changes and a holistic approach are needed to address this serious problem in the ever-evolving digital era. The aim of this research is to further explore the legal consequences of actions of cyberbullying, assess the effectiveness of existing regulations in protecting victims, and explore the debate around the limits of free speech and regulation in the digital realm. Through additional research, more effective and balanced solutions are expected to address this pressing problem in the ever-evolving digital era.

2. Research Method

Library research and normative juridical is a type of research that researchers undertake by using books, journals, and laws related to cyberbullying. The approach used in this research is the statutory approach (statute approach). The material collection technique used by the author in this research was to collect primary, secondary, and tertiary legal research materials that the researcher took, namely literature. Techniques for collecting materials to search for data by reading and reviewing documents regarding criminal acts of cyberbullying. The primary data source used is Law No. 19 of 2016 concerning ITE in Article 27 Paragraph (3). Secondary data sources used by researchers include books, tafsir books, journals, previous research related to the research of the authors taken. Tertiary data sources or what can be called non-legal materials are data or materials that support the clarification of primary and secondary legal materials in the form of the Big Indonesian Dictionary, Encyclopedia, and Law Dictionary.

The data analysis technique that the researcher took and used was a normative juridical technique, namely by examining the norms and principles of legal science which refer to statutory regulations and legal norms existing in society, including data reduction, data presentation, and drawing conclusions. In understanding and simplifying the data obtained in a good, systematic, and structured manner in the data testing method, the author uses the triangulation data testing method.

3. Results and Discussion

The enforcement and application of punishment to individuals who commit acts of cyberbullying in the social media platform are in accordance with the provisions in Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE).

The development of electronic information technology has changed many aspects of people's lives. This gives people access to freedom of opinion, to be creative with their ideas, and to obtain information that is important for advancing the nation and improving general welfare through the use of electronic information technology. However, the right to freedom of expression is not absolute because it is limited by the applicable law.

One of the consequences of this technological development is the increase in crime in the internet world or cybercrime. These crimes can be easily accessed and spread, leading to the spread of illegal and detrimental information. This information often contains insults, violations of decency, fake news, threats, blackmail and hate speech involving ethnicity, religion, race, and certain groups, which has the potential to cause divisions in society. The existence of this dangerous information can harm individuals personally and can be easily distributed, transmitted, and discussed without time limits, which shows the need for stricter regulations in the use of electronic information technology to protect society from its negative impacts (Paat, 2020).

Indonesia has been actively involved in international relations and has taken a role in dealing with various problems in the international world. One of the global challenges faced is internet crime, known as cybercrime. These crimes involve the use of advanced technology to carry out various criminal acts, which are typical in the internet context. To overcome and prevent cybercrime, it is important to have strict legal regulations both at the national and international levels. This regulation aims to coordinate cybercrime regulations throughout the world.

In Indonesia, legal regulations related to crimes in the internet world (cybercrime) have been implemented through Law No. 19 of 2016 concerning Electronic Transaction Information, which is a revision of Law No. 11 of 2008. However, these regulations must continue to develop and adapt to the values and norms of society, including social, cultural, and religious aspects. The aim is to maintain the integrity and unity of the country and achieve common interests in protecting society from the threat of crime in the internet world. Through the development of relevant legal regulations, Indonesia is trying to answer the challenges of cybercrime in the national and international scope (Niniek, 2009).

There were two opinions relating to the legal regulation of crimes committed on computers, also known as cybercrime, before the issuance of the Information and Electronic Transactions Law (UU ITE). The first opinion, held by Mardjano Reksodiputro,

is of the opinion that the Criminal Code (KUHP) already has an adequate legal framework to deal with crimes committed via computers. According to this view, computer crime is nothing new in the Criminal Code, and therefore, there is no need for special laws regulating cybercrime. Instead, this opinion proposes that computer crimes can be integrated into the existing Criminal Code.

The second opinion believes that regulations are needed that specifically regulate and handle cases of crimes committed on computers or cybercrime. This view indicates that the Criminal Code may not be sufficient to address specific aspects related to cybercrime. Therefore, this opinion advocates for explicit provisions both in the Criminal Code and through separate laws that focus on cybercrime. This is considered important in order to be able to apply appropriate sanctions and punishments for criminal acts committed via computer.

The decision between these two opinions will depend on the legal perspective and public views regarding the effectiveness of existing laws in dealing with computer crime. Over the last few years, the Information and Electronic Transactions Law (UU ITE) in Indonesia has become an example of special legislation that tries to address specific aspects of cybercrime. However, the assessment of whether the law is effective enough or still requires revision remains an ongoing debate (Suhariyanto, 2013).

Actions that violate the law and fall into the category of criminal acts in Indonesia are regulated by the Criminal Code (KUHP). The Criminal Code is the main legal regulation in determining the punishment and sanctions given to perpetrators of criminal acts. The Criminal Code is a legal document that regulates various types of criminal acts, ranging from crimes against state security to violations of the law involving individuals or groups. However, if the unlawful act is not regulated in the Criminal Code, then the legal regulations that regulate it are usually special laws. For example, legal regulations governing criminal acts in the field of information and electronic transactions in Indonesia are regulated by the Information and Electronic Transactions Law. Thus, the Criminal Code is the main reference in recognizing criminal acts, but there are special laws that regulate acts that may not be covered by the Criminal Code (Pradityo, 2016).

Regulations that can be used as a legal basis for criminal acts of insult on the internet or cyberspace (cyberbullying) are contained in Article 310, Article 311, and Article 315 of the Criminal Code (KUHP). However, among these articles, Article 315 is the most suitable to serve as reference material and legal basis for criminal acts of cyberbullying. This article explains about acts of insult that defame one's good name, whether intentionally or not, carried out directly or indirectly, verbally or in writing. The consequences of these actions include light insults, punishable by four months and two weeks in prison with a monetary fine amounting to four hundred thousand rupiah (Ihkam & Parwata, 2016).

Broadly speaking, criminal acts of insult are actions committed by attacking

someone's honor. Article 315 of the Criminal Code regulates criminal acts of light insult. The meaning of light insult in Dutch terms is called eenvoudige belediging, which means "ordinary" but experts translate it as "light" (Hamzah, 2015). In criminal acts of insults committed on the internet or cyberspace (cyberbullying), which has happened frequently in this decade, Article 315 of the Criminal Code is considered insufficient to provide the punishment required.

Therefore, the insults contained in Article 315 of the Criminal Code are very limited because they only regulate insults carried out intentionally or not which have the nature of defaming someone's good name directly orally and indirectly in writing. So, Article 315 of the Criminal Code gives rise to multiple interpretations and unclearly defines light insults in any form that are intended to be called light insults. The Criminal Code does not explain in detail and clearly regarding insults; it only explains the broad meaning of regulating criminal acts of insults. The elements of Article 315 of the Criminal Code can be seen as follows: (Ndruru et al., 2020)

a. Objective Elements
   1) All actions that are insulting by defaming someone's good name, but what is said is unintentional, such as saying it correctly according to facts and reality, which is not intended to be insulting to defame his good name, but the person is offended and feels hurt because his honor has been insulted.
   2) Acts of insults carried out directly and indirectly, either verbally or in writing, carried out directly by carrying out the act in front of the person's own face or indirectly by sending writing or even comments via electronic media.
   3) If the act of insult is carried out indirectly through writing sent or written via a letter, both the person sending and receiving it can be used as evidence for the criminal act of insult.

b. Subjective Elements

   The Criminal Code itself does not directly explain the word intentional for actions carried out intentionally. Via MVT (Memorie van Teoclictihing) the sentence intentionally is defined as knowing and wanting, which can be concluded that the sentence intentionally is an action that has been desired and carried out previously. Basically, someone who commits a criminal act already knows about the act being committed and already knows about it. Article 315 of the Criminal Code only regulates light insults as contained in the elements in that article. However, this article does not explain clearly and in detail what actions are included in light insults. Article 315 of the Criminal Code in its objective elements fulfills the act of cyberbullying because the act of insulting was carried out either directly or indirectly by sending and receiving it verbally or in writing. Therefore, light insults committed on someone's physical body are included in cyberbullying.

Perpetrators of criminal acts of cyberbullying can be punished using Article 315 of the Criminal Code, which regulates the criminal act of insulting in the internet world (cyberbullying). Cyberbullying is an insulting act committed via the internet, either through direct messages or written comments that can be known by many people. Article 315 of the Criminal Code fulfills the elements needed to deal with criminal acts such as cyberbullying. Apart from Article 315 of the Criminal Code, there are also regulations outside the Criminal Code that regulate criminal acts of cyberbullying, namely Electronic Transaction Information Law No. 11 of 2008 concerning Electronic Transaction Information which has been revised to become Law No. 19 of 2016 concerning Electronic Transaction Information. This shows that law in Indonesia has accommodated criminal acts of cyberbullying in various regulations, so that the perpetrator can be punished according to the applicable provisions.

Law No. 11 of 2008 concerning Electronic Transaction Information (UU ITE) is a special law enacted to overcome internet crime or cybercrime. This law creates a relevant legal basis for regulating criminal acts that occur in the world of information, technology, and electronics. However, the implementation of the ITE Law has reaped a number of pros and cons in society. This controversy ultimately resulted in a revision of the law, and ITE Law No. 11 of 2008 was changed to Law No. 19 of 2016 concerning Electronic Transaction Information. This change was made to overcome several problems that have arisen since the enactment of the ITE Law, especially relating to Article 27 paragraph (4) of the ITE Law. Article 27 paragraph (4) of the ITE Law is the main concern in this controversy, because it is considered too broad and could lead to abuse. This article regulates acts of threats and blackmail via electronic media or electronic documents carried out without the right to transmit them.

The revision of the ITE Law aims to achieve several goals. First, these changes are intended to maintain public order and justice in society, while at the same time affirming the right to individual freedom in maintaining their honor. Second, this change in law is based on careful consideration, thereby trying to overcome a number of problems and concerns that arose during the implementation of the previous ITE Law. Thus, it is hoped that this change will create a balance between freedom of speech and protection of individuals and society from threats and extortion carried out through electronic media.

Provisions regarding acts that attack a person's good name with slander are regulated in general Indonesian law, namely the Criminal Code (KUHP). However, this provision also exists specifically in the ITE Law No. 19 of 2016 Article 27 paragraph (3). The articles that regulate someone's good name being tarnished and/or slandered in the Criminal Code are Article 310 and Article 311.

> *"Any person who deliberately attacks someone's honor or good name by making accusations about something with the clear intention of making it known to the public, is threatened for defamation with a maximum imprisonment of nine months or a*

maximum fine of four thousand five hundred rupiah."

And Article 311 paragraph (1):

"Whoever commits a crime by blaspheming or blaspheming in writing, if he is permitted to prove the accusation, if he cannot prove it and if the accusation is carried out carelessly, he will be punished for false slander with a maximum imprisonment of four years."

In the Criminal Law Provisions (KUHP), the criminal act of defamation is regulated as a complaint offense. This means that in order to sue someone who commits an act of defamation in accordance with the relevant articles in the Criminal Code, there is a requirement that the lawsuit must be filed by the party who feels aggrieved, namely the victim of the defamation. Complaint offenses have personal or private characteristics, so that prosecution can only be carried out on the initiative of the victim who feels that his good name has been tarnished. Consequently, in cases of complaint offenses, the continuity of the legal process is very dependent on the victim's willingness and desire to file a complaint. This also has an impact on the role of the prosecutor in the prosecution process, because the prosecutor cannot take the initiative on his own to pursue this case without a complaint from the party who feels aggrieved. Thus, this complaint offense focuses on protecting the personal interests of the party who feels aggrieved, and whether legal action will be taken or not, depends entirely on the victim who must take steps to file a legal claim in accordance with the applicable provisions of the Law. (Paat, 2020)

In the Information and Electronic Transactions Law (UU ITE), there are no clear elements regarding insulting acts committed on social media (cyberbullying). Looking at the shape or type of cyberbullying, i.e., harassment, flaming, cyberstalking, exclusion, impersonation, outing, and trickery, it is very clear that there are not only elements of threatening, blackmailing, and defaming someone's good name in the act of cyberbullying.

Cyberbullying has a definition that prioritizes verbal threats, where verbal threats of violence are regulated in the law contained in Article 27 paragraph (4). The article states that this paragraph directs the provisions regarding threats and extortion contained in the Criminal Code (KUHP) contained in Article 368 and Article 369 which reads: Article 368 paragraph (1):

"Any person who, with the intention of unlawfully benefiting himself or another person, forces someone by force or threat of violence to give something, which wholly or partly belongs to that person or another person, or in order to create a debt or write off a receivable, is threatened with extortion, with a maximum prison sentence of nine

*years."*and Article 369 paragraph (1):*"Anyone who, with the intention of benefiting himself or another person, violates the law by making threats of defamation in writing or written by threatening to reveal secrets in public, forces someone to give goods which entirely belong to that person or another person, in order to give and write off the receivables. , then be threatened with imprisonment for a maximum of four years."*

The article previously explained relates to threatening actions involving the disclosure of secrets to the public, as regulated in criminal law. This kind of threat can refer to Article 310 of the Criminal Code, which deals with acts of pollution. The act of threatening to reveal secrets aims to take advantage of someone's situation by threatening to reveal their secrets in public, which has the potential to defame someone's good name and reputation. In the digital era and internet media, threatening actions have also been regulated in Article 27 paragraph (4) of the Information and Electronic Transactions Law (UU ITE). This article regulates the actions of someone who sends messages containing threats and blackmail via electronic media and electronic documents with the intention of disseminating electronic information.

Blackmail is an action that forces someone to give goods or things requested by another party with certain threats or pressure. On the other hand, threats are actions that intimidate or frighten someone by committing blackmail. It is important to note that threatening behavior must involve a specific promise or agreement between the party being threatened and the party making the threat. If there is no prior agreement or promise, then the threatening action is considered unlawful and detrimental to the party being threatened. In the context of Article 29 and Article 27 paragraph (4) of the ITE Law, threats can occur without physical violence against the victims, but still have the potential to cause reputational and psychological harm (Suhariyanto, 2013).

The regulations contained in the Electronic Transaction Information Law (UU ITE) generally provide a legal basis for dealing with cases of cybercrime or cybercrime that use computers and internet networks as tools to carry out criminal activities. In this context, Article 27 paragraph (3) of the ITE Law explains acts of insult and defamation that occur in electronic media or electronic documents, which involve the distribution and transmission of information without permission that can be accessed. Meanwhile, Article 27 paragraph (4) refers to acts of threats and extortion carried out through electronic media or electronic documents, as well as the distribution and transmission of information without permission that can be accessed. These two articles are in line with the provisions contained in the Criminal Code (KUHP) which target individuals who violate the law. The offense of insult in the context of the ITE Law mainly refers to Article 27 paragraph (3), and although the articles in the Criminal Code are different, they are closely related to the rules regulated in Article 27 paragraph (3) regarding insulting acts that occur on the internet, such as cyberbullying. Thus, the ITE Law provides a relevant legal basis for enforcing the law against crime of cyberbullying and similar acts involving

the use of information technology (Ihkam & Parwata, 2016).

If Article 27 paragraph (3) of the ITE Law is examined further, it appears that there are no provisions that explicitly specify insulting acts committed online. This article only states general provisions regarding insults and defamation, so the article can give rise to many interpretations. These offenses often involve relatively mild insults, which are also characteristic of criminal offenses of cyberbullying. This kind of insult generally also fulfills the elements of insult contained in the Criminal Code, namely Article 315. Therefore, until now, the main guideline in handling and providing punitive sanctions for criminal acts of insult in cyberspace (cyberbullying) is Article 27 paragraph (3) of the ITE Law, as long as the act meets the qualifications of a criminal act of insulting with a computer used as a tool to commit the crime (Minin, 2017).

Article 27 paragraph (3) of the ITE Law contains three elements that are relevant to the elements in the Criminal Code that apply to the general public, namely the elements of transmitting, making accessible, and distributing. With these elements, ITE law provides a clear legal basis for actions involving information or communication via the internet. Therefore, it is important for law enforcement officials to carry out their duties as well as possible in dealing with cases of internet crime or cybercrime. Apart from that, protection of individual rights and privacy must also be maintained, so that the authority held is not misused. However, it should be noted that the offense of insulting which refers to Articles 310, 311, and 315 of the Criminal Code has been recognized as a form of interpretation and understanding of Article 27 paragraph (3) of the ITE Law regarding insulting acts committed in cyberspace. This shows that ITE law and the Criminal Code can complement each other in dealing with insulting acts in the online environment so that these cases can be handled fairly and in accordance with applicable legal regulations (Wulan, 2020).

Social and Legal Impacts Resulting from the Implementation of Related Positive Criminal Law RegulationsCyberbullying

Implementation of positive criminal law regulations related to *cyberbullying* in Indonesia has significant social and legal impacts. This impact includes protection for victims *cyberbullying*, but also raises questions about individual rights, free speech, and the effectiveness of law enforcement. Here is a more detailed analysis:

a. Protection for Victims of Cyberbullying

Criminal law regulations on cyberbullying provide a strong legal framework to protect victims of cyberbullying by presenting a clear legal basis for law enforcement against perpetrators of actions of cyberbullying. The existence of this legal framework plays a vital role in providing a sense of protection for victims who may feel vulnerable and devastated by the online harassment they experience. With the existence of strict laws and clearly defined punitive

sanctions, it is hoped that there will be a deterrent impact on actions of cyberbullying themselves.

Law enforcement against cyberbullying is an important part of helping victims obtain justice and preventing the spread of these abusive acts. The existence of strict laws can be an effective deterrent for those who may intend to take action of cyberbullying, because they are aware of the serious consequences they may face if found guilty. This also sends a message that society and the government are serious about fighting cyberbullying, which in turn can encourage behavior change and safer online behavior.

In this case, cooperation between law enforcement agencies, online service providers, and education about online ethics are key in protecting individuals from the negative impacts of cyberbullying. All of these elements work together to form a safer and more welcoming digital environment, where freedom of expression is balanced with strong responsibilities.

b. Individual Rights and Freedom of Speech

Legal arrangements also raise a series of profound questions about individual rights and the limits of free speech. There are concerns raised by the high penalties and broad provisions imposed by the Information and Electronic Transactions Law (UU ITE). This has resulted in significant criticism regarding the potential for misuse of the law and the feeling that the ITE Law is being used as a tool to limit freedom of expression in cyberspace. Several cases of law enforcement under the ITE Law have been deemed to impede freedom of speech and opinion, which is an issue that deserves attention in order to maintain a proper balance in criminal law relating to the digital world.

It is important to strike a balance between protecting victims of cyberbullying, which should not be underestimated, and individual rights in diverse digital contexts. Heavy penalties can raise questions about the extent to which violations that may be minor can be pursued with such legal action. Therefore, there is a need for a more in-depth study of how the law can be applied fairly and in balance, and provide guarantees that individual rights remain protected while still providing adequate protection for victims of cyberbullying. This is a complex challenge and needs to be considered carefully in the context of developing regulatory criminal law for cyberbullying.

c. Effectiveness of Law Enforcement

Another question that needs to be asked is the extent of legal regulation of cyberbullying effective in reducing incidents of cyberbullying themselves. Although legal arrangements with high penalties have the aim of preventing actions of cyberbullying, their effectiveness can be questioned. Most cases of cyberbullying involve an element of anonymity, where perpetrators often hide

behind false or anonymous identities. In this case, law enforcement becomes a challenge, as tracking and identifying perpetrators can be difficult. Thus, even with strict legal regulations, perpetrators may feel they can continue their actions without being arrested or prosecuted. Therefore, it is important to not only have strong laws, but also an efficient law enforcement system capable of pursuing and identifying perpetrators of cyberbullying quickly and precisely.

High punitive sanctions may become a tool of excessive pressure if not supported by efficient and effective law enforcement. In situations where laws are not strictly enforced, this can create uncertainty among the public about how the laws are implemented and the extent to which they are truly effective in protecting victims of cyberbullying. This, in turn, may result in a decline in trust in these legal regulations, which may reduce their effectiveness as a prevention tool. Therefore, it is important to evaluate not only existing punitive sanctions, but also the ability of the law enforcement system to identify and prosecute perpetrators of cyberbullying. This is an important challenge to consider in efforts to protect victims and reduce incidents of cyberbullying.

d. Victim Protection

Protection provided to victims of cyberbullying is an important aspect of these legal arrangements and has direct implications for their effectiveness. It is important to ensure that victims get the help and support they need, both in terms of physical safety and psychological wellbeing. It also includes further preventive measures, such as education about online safety and efforts to minimize risks of cyberbullying. In this case, government agencies, non-government organizations, and online service providers can work together to provide more comprehensive assistance to victims.

In addition to protection for victims, legal regulations must also ensure that perpetrators of cyberbullying are identified and punished as fairly as possible. In this case, cooperation between law enforcement agencies and online service providers is important to achieve fair results for all parties involved. This can include an efficient exchange of information and timely reporting from online service providers to regulatory authorities. In addition, there needs to be a mechanism that allows perpetrators to provide clarification and defend themselves if necessary, in line with the principles of justice. Thus, legal arrangements for cyberbullying must include a holistic approach involving multiple parties, including government agencies, online platforms, and society, to achieve a fair and effective balance in protecting victims, punishing perpetrators, and minimizing incidents of cyberbullying.

e. Education and Awareness

Education and raising awareness play a vital role in preventing incidents of

cyberbullying. In educational settings, the integration of digital ethics concepts, respectful behavior, and understanding of implications of cyberbullying in the school curriculum is an essential step. This will help create better awareness among the younger generation about the risks involved in cyberbullying, as well as giving them the tools to protect themselves and their peers. In addition, public awareness campaigns involving collaboration between the government, NGOs, and technology companies can also play a role in increasing public understanding of cyberbullying, creating a safer and more ethical online environment. Through this holistic approach, incidents of cyberbullying can be reduced substantially, upholding protection for victims, and encouraging more responsible behavior in the digital realm.

In the context of changing digital dynamics that continue to develop and shifts in online behavior, it is important to note that legal regulations regarding cyberbullying are a legal domain that is experiencing ongoing development. Sustainable legal arrangements reflect legal adaptation to the ever-evolving challenges in cyberspace. This is in line with the principle of legal evolution to answer contemporary issues. It is important to understand that the relevant legal arrangements for cyberbullying are dynamic and continuously tested and evaluated.

Continuous evaluation and changes in the legal framework reflect a commitment to maintaining a balance between protecting victims of cyberbullying and basic principles of democracy, especially in the context of freedom of speech. Therefore, further research is being carried out, which aims to explore the social and legal impacts resulting from the application of the relevant criminal law of cyberbullying in Indonesia. This research encourages the identification of the real impact of these legal changes in reducing incidents of cyberbullying and its impact on the balance of victim protection and free speech.

4. Conclusion

Law enforcement of actions of cyberbullying on social media platforms is done based on Law No. 19 of 2016 concerning Electronic Transaction Information (UU ITE). Article 27 paragraph (3) of the ITE Law regulates acts of insult and defamation in electronic media, although it does not yet specify the specific actions of cyberbullying. Apart from that, Article 27 paragraph (4) of the ITE Law refers to threats and blackmail via electronic media. Apart from the ITE Law, several articles in the Criminal Code (KUHP) also regulate insults and defamation, but do not specifically cover acts of cyberbullying. Law enforcement continues to develop in line with technological developments and changes in society's needs. It is important to ensure the protection of individual rights and freedom of expression while protecting society from the negative impacts of cyberbullying.

The application of related criminal law regulations of cyberbullying in Indonesia has significant social and legal impacts. This provides protection for victims and puts pressure on perpetrators of the action of cyberbullying. However, it also raises questions about individual rights and freedom of speech, especially in relation to high penalties. In addition, the effectiveness of law enforcement in identifying and punishing perpetrators is a challenge in itself. Victim protection, education, and awareness-raising must also be strengthened. In the changing digital dynamics that continue to develop, ongoing evaluation and changes in the legal framework reflect a commitment to maintaining a balance between the protection of victims and the basic principles of democracy.

Refrences

Hamza, A. 2015. Certain Offenses (Speciale Delicten) in the Criminal Code. Graphic Rays.

Ihkam, MD, and IGN Parwata. 2016. "The Crime of Cyber Bullying in the Perspective of Criminal Law in Indonesia." Kertha Speech Journal 9, no. 11: 1–10.

Minin, A. R. 2017. "Criminal Policy against Criminal Acts of Intimidation on the Internet (Cyberbullying) as a Mayantara Crime (Cybercrime)." Legalite: Journal of Islamic Legislation and Criminal Law 2, no. II: 1–18.

Ndruru, MK, I. Ismail, and S. Suriani. 2020. "Legal Regulations Regarding Body Image Insults (Body Shaming)." Tectum Journal 1, no. 2.

Niniek, S. 2009. Cyberspace Problems & Anticipation of Arrangements. Jakarta: Sinar Graphics.

Paat, L. N. 2020. "Legal Study of Cyber Bullying Based on Law Number 19 of 2016." Lex Crimen 9, no. 1.

Pradityo, R. 2016. "Criminal Law Policy in Efforts to Overcome Terrorism Financing Crimes." Rechts Vinding Journal: National Legal Development Media 5, no. 1: 17–31.

Suhariyanto, B. 2013. Information Technology Crime (Cybercrime): The Urgency of Regulation and Legal Loopholes.

Wulan, E. R. 2020. "Juridical Study of Article 27 Paragraph (1) of Law No. 11 of 2008 concerning Cyber Crime Crimes." BUSINESS LAW Journal 4, no. 1: 332–345.