



Cyberbullying In the Perspective of Islamic Criminal Law

Ending Solehudin¹ Mukhlis Akbar Ramadhani² Adinda Putri Hutabarat³ Alwi Almisky Munthe⁴

¹Sunan Gunung Djati State Islamic University, Bandung

²³⁴State Islamic University of North Sumatra

E-mail: endingsolehudin@uinsgd.ac.id rmukhlisakbar@gmail.com

Info Articles	Abstract
Article History Received: 2024-12-05 Revised: 2024-12-11 Published: 2024-12-30 Keywords: <i>Cyberbullying, Islamic law Perspective, Criminal Law</i>	The rapid development of information and communication technology has significantly transformed patterns of social interaction while simultaneously giving rise to new forms of crime, including cyberbullying. Cyberbullying has become a serious legal issue due to its detrimental effects on victims' psychological well-being, personal dignity, and reputation. Although Indonesia has enacted Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Electronic Transactions (ITE Law), the regulation does not explicitly define cyberbullying as a distinct criminal offense but addresses related acts such as defamation, threats, extortion, and intimidation committed through electronic media. This study aims to analyze the legal regulation of cyberbullying under the ITE Law and examine its legal consequences from the perspective of Islamic criminal law. This research employs a normative juridical method with a descriptive-analytical approach based on statutory, conceptual, and literature studies. The findings indicate that cyberbullying constitutes a form of cybercrime involving electronic media to threaten, intimidate, humiliate, or damage another person's reputation. Under Indonesian positive law, perpetrators may be prosecuted under several provisions of the ITE Law and the Criminal Code depending on the nature of the offense. From the perspective of Islamic criminal law, cyberbullying is categorized as a <i>ta'zir</i> offense because no specific punishment is prescribed in the Qur'an or Hadith. Consequently, the determination of sanctions is left to the discretion of the legitimate authority (<i>ulil amri</i>) to ensure justice, public order, and the protection of individual honor. The study concludes that both Indonesian positive law and Islamic criminal law share the same objective of protecting human dignity and preventing harm caused by cyberbullying, despite adopting different legal approaches to determining criminal sanctions.

I. INTRODUCTION

With today's technological advancements, everyone should have a computer network. Advances in communication tools have resulted in a variety of new technologies that accelerate human communication, open up new market spaces, and encourage investment in computer and mobile phone development. Internet-connected people use information technology for a variety of purposes every day. In 2009, approximately 40 million people in Indonesia used the internet, making it one of the highest numbers in Southeast Asia.(Febriyantoro & Arisandi, 2018). "Freedom of expression is the right of every citizen to convey his ideas or opinions, whether verbally, in writing, or in other ways, freely and responsibly, in accordance with

applicable laws and regulations." This is regulated in Article 1 of Law Number 9 of 1998, as part of a state that respects the right to this freedom.

One of the fundamental rights that can be restricted is freedom of expression. Therefore, every human rights law worldwide has stipulated that freedom of expression can only be restricted under very limited circumstances, and these restrictions must be carefully determined and in accordance with applicable laws and regulations.(Guntara & Herry, 2022). Therefore, freedom of speech must be accompanied by the ability to take responsibility. Actions that cause insults, harassment, slander, or intimidation when speaking in public, as regulated by the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). In

Indonesia, this problem occurs not only in the general public, but also in the information technology (IT) industry. Although the internet offers many benefits, this technology also has negative impacts. One of these is the potential for the internet to be used as a means to commit illegal or unlawful acts.

With the development of the internet and information technology, new crimes have emerged. Crimes known as cybercrime, crimes committed over the internet, can threaten anyone with a very low risk of arrest, but can cause significant harm to society and the state. In general, cybercrime refers to attempts to access or utilize computer facilities or networks without permission in an illegal manner, either with or without causing changes or damage to the computer system being used. (Yunus, 2014) Cyber law, also referred to as "cyber law" or "telematics law," regulates the use of information technology, cyberspace, and cyber law to prevent these cybercrimes. These terms arose because crimes that utilize computer systems and communication systems, which utilize computer-based information technology, which is an electronic system that can be seen visually. (Ramli et al., 2020). The first paragraph of Article 310 of the Criminal Code regulates insults as follows:

"Whoever intentionally damages the honor or good name of someone by accusing him of committing an act with the clear intention of making the accusation public, shall be punished for blasphemy with a maximum prison sentence of nine months or a maximum fine of four thousand five hundred rupiah."

Furthermore, Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) was enacted to reduce crimes committed via the internet. Cyberbullying, which is now increasingly common, is an act of violence or harassment perpetrated by an individual or group using electronic devices against a targeted victim. In other words, it is a form of intimidation carried out by one or more individuals online to pressure or deceive another person.

Cyberbullying cases have begun to increase along with the growing number of internet users

in Indonesia. One example is the Twitter account @triomacan2000 which was reported to have made posts that threatened and disturbed several people, including President Joko Widodo. This case was then reported to the police and taken to court for legal processing. The account owner was threatened with Article 29 and Article 45 paragraph (3) of the Electronic Information and Transactions Law. This case reflects a form of Cyberbullying that is prohibited by law. In addition, there are still many other cases of Cyberbullying that have not been reported by the media. Despite this, many writings and images that violate the law related to bullying have not been brought to the legal realm.

In Islam, punishment (uqubah) is prescribed to maintain order and the interests of society. Depending on whether the crime is regulated by sharia or not, Islamic law is divided into several types. Depending on whether the punishment is found in the Quran or Hadith, punishments can be divided into two categories: (Sari, 2023)

- a) Punishments that have texts include hudud, qishash, diyat and kafarat
- b) The punishment for which there is no text is ta'zir.

In the Koran, namely QS. al-Hujurat (49) verse 11, Allah swt. said:

"O you who believe, don't let a group of men look down on another group, maybe the one being laughed at is better than them. And don't let a group of women look down on another group, maybe the one being humiliated is better. And don't like to criticize yourselves, and don't call yourself names that contain ridicule. The worst call is that which is bad after faith and whoever does not repent, then they are the wrongdoers. (Qs. al-Hujurat verse 11)".

As reflected in the verse, acts of intimidation and defamation of others are forbidden, which is in line with cyberbullying. Islam, as a religion that upholds honor, forbids its followers from inciting, gossiping, speaking harshly, calling someone by offensive nicknames, or engaging in any action that could damage a person's honor, dignity, or reputation in the eyes of others. Furthermore, Islam reminds us to guard the tongue, which God

has given us, to prevent sin or slander. In Islam, those who engage in such acts are considered wicked.

II. RESEARCH METHODS

This study employed a normative juridical research method with a descriptive-analytical approach. Normative legal research was selected because the study focuses on examining legal norms governing cyberbullying under Indonesian positive law and Islamic criminal law. The research relied exclusively on library research by collecting and analyzing legal materials relevant to the research topic.

The approach used in this study consisted of the statutory approach, conceptual approach, and comparative approach. The statutory approach examined the provisions of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Electronic Transactions (ITE Law), the Indonesian Criminal Code, the Criminal Procedure Code, and other relevant legislation. The conceptual approach analyzed legal doctrines and scholarly opinions concerning cyberbullying, cybercrime, criminal liability, and Islamic criminal law (*fiqh jinayah*). Meanwhile, the comparative approach was employed to compare the regulation of cyberbullying under Indonesian positive law with the principles of Islamic criminal law, particularly the concept of *ta'zir* punishment.

The legal materials consisted of primary, secondary, and tertiary legal sources. Primary legal materials included statutory regulations and relevant legal provisions. Secondary legal materials comprised books, scientific journal articles, previous studies, and legal commentaries discussing cyberbullying, cybercrime, and Islamic criminal law. Tertiary legal materials included legal dictionaries, encyclopedias, and other reference materials supporting the interpretation of legal concepts.

The collected legal materials were analyzed qualitatively using descriptive and interpretative methods. The analysis was conducted by identifying, classifying, and interpreting legal norms, supported by legal doctrines and scholarly

opinions, to evaluate the regulation of cyberbullying under the ITE Law and its legal implications from the perspective of Islamic criminal law.

III. RESULTS AND DISCUSSION

A. Definition of Cyberbullying

The emergence of new types of crimes such as online harassment has been influenced by the era of globalization and advances in information technology. This phenomenon is widespread in many countries around the world, including Indonesia. Physical or mental violence perpetrated by one person or group of people, resulting in the victim feeling abused, is called cyberbullying. Bullying can occur in various aspects of life, such as social, political, cultural, sports, education, and family. Cyberbullying is essentially a form of harassment perpetrated by individuals known as bullies, which means harassing, intimidating, insulting, and harassing via the internet.(Aksin & Aini, 2022). Here are some definitions of cyberbullying according to experts:(Imani et al., 2021)

1. Cyberbullying is a form of abuse carried out by a person or group of people against a victim who has difficulty defending themselves, using electronic devices repeatedly.
2. Cyberbullying is the use of technology to intimidate, victimize, or bully an individual or group.

Based on the definitions explained above, cyberbullying can be defined as a form of intimidation, harassment, or verbal abuse carried out via the internet. Depression experienced by victims can be caused by fear or pressure, both physical and verbal. However, research shows that victims of cyberbullying tend to experience higher levels of depression than those who experience other forms of verbal abuse.(Imani et al., 2021).

Cyberbullying can also be understood as harassment and humiliation perpetrated by perpetrators against victims via the internet, such as social media, to demean them. Furthermore, cyberbullying can be defined as intimidation

carried out by perpetrators using certain technologies to harass victims online. Perpetrators can attack victims in various ways, such as sending cruel messages or spreading disturbing images to humiliate them publicly. This phenomenon occurs because perpetrators have access to the internet, which makes them feel they have control over the network, as if they have the right to determine the rules for its use, when in fact they do not have such control.

One type of cybercrime is cyberbullying, which allows perpetrators to conceal their identities by using computers as a means to commit crimes. While different from traditional bullying, cyberbullying still involves the use of computers as a tool to commit crimes. Crimes related to cyberbullying can be categorized as cybercrime if they meet the following criteria:(Dwipayana et al., 2020)

1. Non-violence
2. Minimize physical contact
3. Using equipment and technology
4. Utilizing global telematics (telecommunications, media, and informatics) networks.

By leveraging information technology to address various types of crimes, acts such as cyberbullying are very common online. This crime must be criminalized because the harm suffered by victims can be very serious and spread more quickly than crimes committed manually. Cyberbullying can take many forms, such as uploading photos or posts that impact the victim, mocking the victim, or misusing other people's social media accounts to threaten and create problems, such as creating websites to spread slander and threats via email.

B. Types of Cyberbullying

According to Willard, various types of cyberbullying can be categorized as follows:(Indrayani & Johansari, 2019)

1. Flaming is the act of sending text messages containing angry and offensive language. The term refers to words that incite conflict within the message. Flaming can mean insulting or making harsh comments about

someone, and it can also refer to a digression from the topic of conversation. More generally, the term encompasses actions that offend, mock, or insult other users.

2. Harassment is repeated harassing messages sent via email, SMS, or text messages on other social media platforms. Harassment perpetrators typically post comments to victims or targets with the aim of provoking their anger and often trying to encourage others to do the same.
3. Cyberstalking, which is disturbing and defaming someone's good name so that they are afraid.
4. Denigration (defamation), which is the process of spreading bad things or shame about someone via the internet to damage someone's reputation and good name.
5. Impersonation, the process of spreading bad things or shame about someone via the internet to damage someone's reputation and good name.
6. Outing and Trickery, namely outing spreading other people's secrets, while trickery is deceiving someone to get that person's secrets or personal data.
7. Exclusion, which is the deliberate removal of someone from an online group on any social network, is common in the general public, especially within friendships.

Indirect verbal abuse that affects the victim's emotional or psychological health is known as cyberbullying. This is one of the types of cyberbullying mentioned above.

C. Perpetrators and Victims in Cyberbullying Crimes

KCrimes emerge and thrive in society, and every crime has a perpetrator who fits the crime. As more and more people use the internet to communicate daily, crimes like cyberbullying have also emerged. Experts say there's no easy solution to addressing cyberbullying, and teenagers are often reluctant to tell their parents about online incidents for fear that their parents will restrict their access. As a result, cyberbullying

can be a significant challenge for teenagers because it can persist for a long time.

Cyberbullying consists of two people, namely:(Dwipayana et al., 2020)

1. A perpetrator is an individual who directly commits physical, verbal, or psychological violence against another person online. In this case, the perpetrator acts as the subject.
2. The victim is an individual who is the target or object of bullying carried out by the perpetrator in cases of cyberbullying.

A victim in cyberbullying is an individual who is the target of the bullying perpetrated by the perpetrator. In cyberbullying cases, the victim is usually a single person, unlike other cases where there are both a primary perpetrator and co-perpetrators. Cyberbullying can affect anyone, regardless of profession. This crime can be committed by various parties, including celebrities, students, politicians, and even government agencies.

D. Cyberbullying Media

With the advent of the internet, various communication platforms, such as email, blogs, Twitter, and Facebook, are now extremely popular. These platforms can be misused for criminal activity, blackmail, or threats. Because a person's identity is easily manipulated in the vast virtual world, it is difficult to identify who is involved. Therefore, it is easier to identify someone in the real world. Some media frequently used in cyberbullying cases include the following:(Dwipayana et al., 2020)

1. Instant Message (IM)

Instant Message involves a special account and email that allows users to send text messages or other messages to other people who have an ID on the site.

2. Chatroom

Chatrooms are websites that allow users, who may pretend to be someone else, to join group chats. Within these chats, cyberbullies can write intimidating remarks that can be read by other members of the group, making the victim feel isolated.

3. Trash Polling Site

Some cyberbullies create polls with topics that aim to damage someone's reputation.

4. Blog

A blog is a personal website often used as a journal or diary. The perpetrator has the freedom to post anything there, including information that could intimidate someone.

5. Bluetooth Bullying

By using an active Bluetooth connection, the perpetrator can send disturbing images or messages to someone.

6. Social Networking Sites

Cyberbullying perpetrators can take advantage of social media platforms that have various features to post statuses, comments, photos, and other content that is disturbing, intimidating, offensive, or damaging to someone's reputation.

7. Online game

Cyberbullying is also often found in online games played through computer game software connected to the internet, such as Nintendo, Xbox 360, and Playstation.

8. Mobile phone

Cyberbullying often involves using mobile phones to perpetrate its actions. Perpetrators can send harassing text messages, images, or ideas to the victim.

E. Cyberbullying According to Law No. 19 of 2016 concerning Electronic Information and Transactions

Indonesia is deeply involved in various global interactions as part of the global information community. Because cybercrime involves the use of advanced technology as its medium, criminalization policies in the information technology sector need to consider developments in cybercrime prevention efforts at both the regional and international levels to maintain consistency in its regulations.(Marwin, 2013). With the issuance and implementation of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions, a legal infrastructure is needed that supports the management, use, and utilization of information technology by taking into account the religious, social, and cultural values of Indonesian

society, as well as maintaining and strengthening national unity.

Before the enactment of the Electronic Information and Transactions Law, the Criminal Code already regulated legal relations related to crimes involving computers, which later evolved into cybercrime. Two main perspectives have developed regarding the handling of computer-related crimes, which are also indirectly related to cybercrime: (Marwin, 2013)

1. The Criminal Code is considered capable of addressing computer crimes. According to Mardjono Reksodiputro, a criminologist from the University of Indonesia, computer crime is not a new type of crime, and the Criminal Code is still capable of addressing it. Therefore, computer crimes should be included within the Criminal Code, rather than regulated in a separate law.
2. Computer-related crimes, also known as cybercrime, require specific regulations in the Criminal Code or a separate law governing computer-based crimes. According to J. Sudama Sastroandjojo, new provisions are needed to oversee computer-related crimes. These crimes must be handled specifically because they differ from other crimes in terms of method, environment, time, and location.

Based on the pros and cons of opinion, Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is the first law that regulates information technology and electronic transactions. This law is a very important legal product because it builds the foundation for the use of information technology and electronic transactions. Law No. 19 of 2016 concerning Information and Electronic Transactions then replaced Law No. 11 of 2008. The ITE Law has been a topic of debate since its inception, especially regarding the criminalization of Article 27 paragraph 4 which states, "Any person who intentionally and without the right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain blackmail and/or

threats." The changes were made with the following considerations:

- a. Law No. 11 of 2008 concerning Electronic Information and Transactions needs to be amended to create justice, order, and legal certainty, as well as to guarantee respect for individual rights and freedoms. This amendment is also intended to meet demands for justice in accordance with considerations of security and public order in a democratic society.
- b. Law on Amendments to Law no. 11 of 2008 concerning ITE needs to be made for the reasons mentioned in point a.

The social code stipulated in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions regulates acts that disrupt and disseminate electronic information. Articles 27 to 37 of the ITE Law stipulate penalties for violators of these provisions. Both individuals and companies can be involved in information and electronic transaction crimes recognized in Law No. 19 of 2016. A total of 19 criminal offenses are regulated in articles 27 to 30 and articles 45 to 51.

Cybercrime, especially crimes involving computer programs, is difficult to detect. Nevertheless, the issue of proof is a crucial element in cybercrime cases. (Nurdin et al., nd). Proof is a requirement that ensures a judge has the confidence to make a decision. Judges are prohibited from making unilateral decisions without the support of at least two valid pieces of evidence. This is regulated in Article 183 of the Criminal Procedure Code:

"A judge is not permitted to sentence a person unless, with at least two valid pieces of evidence, he or she is convinced that a crime has actually occurred and that the defendant is guilty of committing it."

The types of valid evidence that can be used as a basis for a judge's decision are limited by Article 184 of the Criminal Procedure Code. Since the enactment of the Electronic Information and Transactions (ITE) Law, anyone committing legal action domestically or internationally that impacts Indonesian law and harms Indonesia's

interests can use electronic evidence. Although the ITE Law only covers insults, defamation, threats, and blackmail, cyberbullying also includes flaming, harassment, impersonation, outing, trickery, exclusion, and cyberstalking.

If we consider the definition of cyberbullying, which includes verbal threats of violence, such actions need to be criminalized. In general, Article 369 paragraph (1) of the Criminal Code regulates the criminal act of threats as follows:

"Anyone who, with the intention of unlawfully benefiting himself or another person, by threatening to slander, slander in writing or to reveal a secret, forces someone to give something that is partly or wholly his or another person's property, or creates a debt or cancels a debt, is threatened with a maximum prison sentence of four years."

The aforementioned threatening actions and methods are known as defamation through threats to disclose secrets. In "threats to disclose secrets," secrets refer to conditions or events related to the person being coerced, which should not be known to others or the general public. However, threats to disclose or conceal these secrets can cause the person to feel anxious, worried, or afraid. Article 310 of the Criminal Code defines defamation in a similar way. Meanwhile, paragraph 4 of Article 27 regulates the dangers arising from internet media, which reads:

"Any person who intentionally and without authority distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing blackmail and/or threats."

Under Article 29 of the ITE Law, which specifically regulates threats of violence, the threats listed in Article 27 paragraph 4 are not threats of violence. In other words, they do not include "acts of violence" against the party being threatened.

F. Punishment for Cyberbullying according to Law No. 19 of 2016 concerning ITE

Law Number 19 of 2016 concerning Electronic Information and Transactions only covers

elements of insults, defamation, threats, and extortion, without explicitly addressing cyberbullying. Article 29 of the ITE Law, which focuses on verbal threats of violence, stipulates the following penalties for cyberbullying:

"Any person who intentionally and without permission sends electronic information and/or electronic documents containing threats of violence or attempts to intimidate individuals."

As explained in Article 45B, this article also includes criminal penalties, namely:

"Any individual who intentionally and without authority sends electronic information and/or electronic documents containing threats of violence or attempts to intimidate individuals."

The threats (including those involving physical violence, fear, and/or material loss) must be directed personally, as stipulated in Article 29 in conjunction with Article 45B. Threats to reveal secrets or defame a person's reputation are also included in the category of threats mentioned in the article. Although corporations can be involved, the explanation in Article 29 does not provide further information regarding the definition of an individual, which refers to a natural person. Because only humans can feel fear, the perpetrator of this crime can only be held criminally responsible if the victim is an individual.

G. Cyberbullying in the Perspective of Islamic Criminal Law

Many civilizations around the world have enacted laws to protect human honor. However, due to a lack of a deep understanding of human nature, these laws are imperfect. Human honor and rights are less protected by these laws than by ethical norms in Islam. Cyberbullying is an act that violates human honor, as threats and intimidation can damage reputations, which is reflected in components of cyberbullying, such as threatening messages and insults directed at someone on a continuous basis.(Aksin & Aini, 2022).

To maintain social harmony, it is crucial to protect this honor. Furthermore, insulting honor or defaming a person's good name can lead to

hatred, division, and a loss of mutual cooperation. Therefore, Islam teaches that anything that damages another person's honor is a sin, and a believer should avoid it, such as insulting or accusing someone they dislike, having negative thoughts, spying, and inappropriately speaking about others.

According to Al-Ghazali, insulting, mocking, ridiculing, and mentioning disgrace is haram, which is sometimes done through imitation, actions, or words.(Tuah et al., 2023)Islam strictly forbids acts such as insulting, ridiculing, criticizing, having bad thoughts (su'udzon), or defaming others, especially fellow Muslims, as explained in Surah al-Hujurat verse 11. This is because the person who insults is not always better than the person who is insulted. Insulting others means insulting oneself, because such actions can damage one's honor and dignity.

Abdul Rahman al-Maliki classifies pollution into three categories, namely:(Rizqi & Wati, 2024)

- a. Al-Dzammu is the mention of a certain thing directed at someone in the form of subtle sarcasm that can trigger anger.
- b. Al-Qadhu is everything related to reputation and self-esteem without linking it to certain things.
- c. al-Tahqir is any word that is insulting or indicates abuse

H. Analysis of Islamic Criminal Law on Cyberbullying in Law No. 19 of 2016 concerning ITE

Because punishment ('uqubah) is prescribed in Islam as a way to repay actions that violate sharia with the aim of maintaining order and the interests of society and protecting personal interests.(Sari, 2023)Cyberbullying is considered a criminal offense or the death penalty according to the following requirements. Although Law No. 19 of 2016 concerning Information and Electronic Transactions regulates cyberbullying, there is no text regulating it from the Quran or Hadith. Because ta'zir punishment does not have a text explained in the Quran or Hadith, Islamic criminal law explains that an act of sin that is not subject to had or expiation is a sinful act in the form of

threats or intimidation that harms the victim.(Ali, 2007).

1. Material elements (al-rukhn al-maddiy), actions carried out intentionally to threaten and intimidate the victim by repeatedly sending text messages or images published in cyberspace.
2. Moral elements (al-rukhn 'adabiy), the perpetrator of cyberbullying is an individual who is legally competent (mukalaf) because he has the ability to utilize technology.

Cyberbullying is a type of crime committed via the internet. Because computers and the internet were not yet available during the time of the Prophet Muhammad (peace be upon him), cybercrime falls under the category of ta'zir crimes. Therefore, there are no verses or hadith specifically regulating cybercrimes, such as online harassment. In Islamic criminal law, imprisonment can be used as a primary or additional punishment in ta'zir cases, when the primary punishment of flogging does not deter the convict.(Aksin & Aini, 2022).

Islamic criminal law scholars have differing views regarding the length of prison sentences in the Islamic criminal law system. Some argue that the sentence should last two or three months, while others argue that the duration is left entirely to the judge's discretion. Life imprisonment is given for very serious crimes, such as murder, which do not qualify for qishas sanctions. However, prison sentences that are limited until the defendant repents have educational purposes, as is currently implemented in Correctional Institutions (Lapas), which grant remissions to inmates who show signs of repentance and a commitment not to repeat the crime. Scholars believe that a person has repented if there is a positive change in their actions and behavior, because true repentance comes from the heart and is not always physically visible. Therefore, ulil amri or the government has the authority to implement ta'zir punishments, as regulated in Article 29 and Article 45 paragraph (3) of Law Number 19 of 2016 concerning Information and Electronic Transactions. The crime of

cyberbullying is also included in the category of ta'zir crimes.

IV. CONCLUSION AND SUGGESTIONS

A. Conclusion

Under Law Number 19 of 2016 concerning Electronic Information and Transactions, cyberbullying perpetrators will be subject to sanctions in accordance with Article 29 and Article 45B if they intentionally and without authorization send Electronic Documents and/or Electronic Information containing threats of violence or intimidation directed at a person. These threats include physical violence, psychological violence, and/or material loss. Perpetrators can be sentenced to a maximum of four years in prison and/or a fine of no more than IDR 750,000,000.

Article 29 of the Law regulates sanctions for acts of cyberbullying, including threats of violence or intimidation directed at individuals. The penalties can include imprisonment of up to four years and/or a fine of up to Rp 750,000,000. Cyberbullying crimes meet the elements of ta'zir crimes, the punishment for which is not explicitly stipulated in sharia but is left to the discretion of the ulil amri (rulers). The type and extent of ta'zir sanctions must be determined carefully, based on the guidance of the text for the public interest.

B. Suggestion

From an Islamic criminal law perspective, cyberbullying is viewed as a violation of a person's honor and dignity, which contradicts Islamic teachings on maintaining individual dignity. Addressing this issue requires strengthening understanding of social media ethics by instilling Islamic values to raise public awareness of the negative impacts of online insults and harassment. A restorative approach is also a solution, where mediation and reconciliation between the perpetrator and victim can help restore relationships and encourage forgiveness. Furthermore, applying appropriate sanctions commensurate with the severity of the offense and the resulting impact can be both a preventative and educational measure. Strong

regulations on digital communication ethics are also needed to prevent various forms of online harassment. With these principles, Islamic criminal law can provide guidance for dealing with cyberbullying more effectively and fairly.

REFERENCE LISTAN

- Aksin, N., & Aini, F. N. Q. (2022). Cyber Bullying dalam Persepektif Islam. *Jurnal Informatika Upgris*, 8(1), 135–141.
- Ali, Z. (2007). *Hukum Pidana Islam*. Sinar Grafika.
- Dwipayana, N. L. A. M., Setiyono, S., & Pakpahan, H. (2020). Cyberbullying di media sosial. *Bhirawa Law Journal*, 1(2), 63–70.
- Febriyantoro, M. T., & Arisandi, D. (2018). Pemanfaatan digital marketing bagi usaha mikro, kecil dan menengah pada era masyarakat ekonomi ASEAN. *JMD: Jurnal Riset Manajemen & Bisnis Dewantara*, 1(2), 61–76.
- Guntara, B., & Herry, A. S. (2022). Hak kebebasan berpendapat di media sosial dalam perspektif hak asasi manusia. *Jurnal Pendidikan Dan Konseling (JPDK)*, 4(6), 6945–6961.
- Imani, F. A., Kusmawati, A., & Tohari, M. A. (2021). Pencegahan kasus cyberbullying bagi remaja pengguna sosial media. *KHIDMAT SOSIAL: Journal of Social Work and Social Services*, 2(1), 74–83.
- Indrayani, S. A., & Johansari, C. A. (2019). Cyberbullying use on teenage artists and its implications on increasing awareness of bullying. *Litera*, 18(2), 275–296.
- Jonaedi Efendi, S. H. I., Johnny Ibrahim, S. H., & Se, M. M. (2018). *Metode penelitian hukum: normatif dan empiris*. Prenada Media.
- Marwin, M. (2013). Penanggulangan Cyber Crime Melalui Penal Policy. *ASAS*, 5(1).
- Nurdin¹, M. K., Rivaldi, C. A., Rahmadani, N., Zahra⁴, H. A., Rayhan, A., & Herang⁵, P. (n.d.). *PERAN HUKUM TELEMATIKA DALAM PENYELESAIAN KASUS CYBERCRIME THE ROLE OF TELEMATICS LAW IN SOLVING CYBERCRIME CASES*.

- Ramli, T. S., Ramli, A. M., Permata, R. R., Wahyuningsih, T., & Mutiara, D. (2020). Aspek Hukum Atas Konten Hak Cipta Dikaitkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Legislasi Indonesia*, 17(1), 65.
- Rizqi, R., & Wati, S. S. (2024). Pencemaran Nama Baik dalam Tinjauan Hukum Islam. *Siyasah Jurnal Hukum Tatanegara*, 4(1), 80–90.
- Sari, S. M. (2023). *Fiqih Jinayah (Pengantar Memahami Hukum Pidana Islam)*. PT. Sonpedia Publishing Indonesia.
- Tuah, M. S., Yusuf, M., & Nurfadliyati, N. (2023). Sarkasme dalam Literatur Tafsir. *Qudwah Qur'aniyah: Jurnal Studi Al-Qur'an Dan Tafsir*, 1(2), 1–11.
- Yunus, H. M. (2014). Pemikiran Yusuf Qardawi Tentang Penyelesaian Masalah Fiqh Kontemporer. *An-Nida'*, 39(2), 215–231.