



A CRIMINAL LAW REVIEW OF CYBERBULLYING AS A FORM OF DIGITAL CRIME

Giannini Oktobellini Henrik¹, Ardiyanti Aris², Lilis Suryani³, Sunardi Purwanda⁴, Phireri⁵

^{1,2,3,4,5} Faculty of Law, Institut Andi Sapada

Email: gianinih@gmail.com¹, ardiyanti.onleonn@gmail.com², lilisatjo@gmail.com³,
sunardipurwandaa@gmail.com⁴, chombenkphireri@gmail.com⁵

Received: 28/05/2026 | Revised: 30/06/2026 | Accepted: 28/07/2026 | Published: 29/07/2026

Abstract

This study aims to analyze the qualifications of cyberbullying as a criminal act within the digital crime family and examine the effectiveness of positive legal regulations in Indonesia in ensnaring perpetrators. The research method used is a normative one with a statute approach and a conceptual approach. The data used is secondary data sourced from primary and secondary legal materials, which are then analyzed qualitatively. The results of the study indicate that cyberbullying has fulfilled the elements of a digital crime (cybercrime) and is regulated in several regulations, particularly the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP). However, law enforcement still faces normative challenges, such as the interpretation of certain articles (rubber articles) and complex digital evidence. Regulation harmonization and a more specific formulation of crimes regarding cyberbullying are needed to provide legal certainty and optimal protection for victims.

Keywords: Cyberbullying Principles, Normative, ITE Law.

INTRODUCTION

Cyberbullying is an act of bullying carried out through electronic media, such as social media, instant messaging apps, online forums, or other digital platforms, with the aim of intimidating, humiliating, insulting, threatening, or psychologically harming another person. Unlike conventional bullying that occurs in person, cyberbullying has a broader reach, can occur at any time, and allows perpetrators to conceal their identities, making it more difficult to trace. This condition makes cyberbullying a serious problem that requires attention from various parties, including the government and law enforcement.¹

Case Example, First Case (Audrey) Pontianak City: the victim's name is Audrey (initials A or AU, full identity is kept secret because she is still a child) who is a junior high school student domiciled in Pontianak City, West Kalimantan which occurred on March 20, 2019 on Jalan Sulawesi and the Taman Akcaya area, Pontianak City, West Kalimantan. The chronology of Audrey's case began with a dispute that occurred via social media between the victim and several senior high school students. The dispute was triggered by mutual taunts and insinuations related to friendships and personal issues. The conflict that initially took place in the digital space then developed into a face-to-face meeting to resolve the dispute. On March 29, 2019, the victim went to the meeting location in the Jalan Sulawesi area, Pontianak. During the meeting, an argument occurred which then led to physical violence. Based on the results of the police investigation, the victim experienced actions in the form of hair pulling, pushing until she fell, and throwing sandals. After the incident at the first location, the victim moved to Akcaya Park, where another fight broke out with the other perpetrator.²

¹ Fiyanti, DAAR, Dewi, AASL, & Suryani, LP (2026). Legal Protection for Content Creators Due to Cyberbullying on Instagram Social Media. *Journal of Legal Analogy*, 8(1), 69-75.

² Haris Fdhil. (2019). Starting with Bullying on Social Media, Here's the Chronology of Audrey's Case. Detik News. https://news.detik.com/berita/d-4506079/berawal-dari-bully-di-medsos-begini-kronologi-kasus-audrey?utm_source

Several days after the incident, the victim's mother reported the incident to the Pontianak City Police. At the same time, information regarding the alleged assault on Audrey spread widely through social media with the hashtag #JusticeForAudrey, thus gaining national public attention. The viral nature of the case gave rise to various public opinions, comments, and the dissemination of information that was not entirely in accordance with the results of the investigation by law enforcement officers. During the investigation, the police questioned the victim, witnesses, and a number of students suspected of being involved. Based on the evidence obtained, the police named three children as suspects. The three were processed under Article 76C in conjunction with Article 80 paragraph (1) of Law Number 35 of 2014 concerning Child Protection, for alleged violence against children. Meanwhile, the results of the post-mortem showed that some of the information circulating on social media did not entirely correspond to the medical facts found by investigators.

The second case example is Titania Aurelie Nurhermansyah (Aurel Hermansyah), a singer, public figure, digital content creator, and entrepreneur in Jakarta. The incident occurred in 2024 (the case gained widespread attention after the birth of her second child). Legal research often uses this case as an illustration of the phenomenon of body shaming on social media. The chronology of the case is that Aurel Hermansyah became the target of body shaming after uploading various activities on social media after giving birth to her second child. In these posts, a number of social media users left comments containing mockery, insults, and negative assessments of the victim's changes in body shape and weight. These comments were posted through the comments section on digital platforms and repeated by many accounts, thus spreading widely in cyberspace. The victim later revealed that these comments caused psychological pressure and affected her emotional state. Aurel also displayed some of the comments she received as a form of education to the public about the negative impacts of body shaming. According to her, these actions not only attacked her physical appearance but also affected her self-confidence and comfort in carrying out activities as a breastfeeding mother.³

This phenomenon demonstrates that social media can be a vehicle for persistent insults to a person's body image. The dissemination of derogatory comments by numerous users in a relatively short period of time magnifies the psychological impact on the victim. Therefore, this act has characteristics of cyberbullying, particularly in the form of body shaming and cyber harassment, because it is carried out electronically with the aim or result of degrading a person's dignity and honor. The case study above serves as a benchmark for relevant evidence for the author's research. It proves that cyberbullying exists. I use normative data, not empirical data, but rather the above example to provide explanatory evidence.

First, the investigator's role is to carry out a series of actions to search for and collect evidence to clarify a crime and find the perpetrator. In cyberbullying cases, investigators not only receive reports from victims but also identify the accounts or devices used by the perpetrators, secure electronic evidence such as screenshots, conversation recordings, social media posts, and coordinate with digital forensic experts if necessary. Given that perpetrators often use anonymous accounts, investigators are required to have technical skills in tracing electronic evidence so that the perpetrator's identity can be legally proven. Second, the prosecutor's role is that after the investigation is declared complete, the case file is transferred to the public prosecutor for research and preparation of an indictment. In cyberbullying cases, prosecutors are responsible for ensuring that all elements of the crime as stipulated in the Criminal Code, the ITE Law, and other relevant regulations have been fulfilled based on valid evidence. In addition to proving the defendant's guilt in court, prosecutors also play a role in filing proportionate criminal charges, taking into account the level of the perpetrator's culpability, the impact on the victim, and the purpose of the punishment.⁴

Third, the role of the judge is that they have the authority to examine, try, and decide cases independently based on the facts of the trial and the provisions of the laws and regulations. In cyberbullying cases, the judge assesses the validity of electronic evidence, proves that the elements of the crime have been fulfilled, and determines whether or not the perpetrator is criminally liable. The judge's decision is not only oriented towards imposing sanctions but must also consider aspects of victim protection, the public's sense of justice, and legal certainty in accordance with the principles of criminal law.⁵

³ Nafilah Sri Sagita. (2024). Regarding the Body Shaming Experienced by Aurel Hermansyah, This is How Serious the Impact Is. Detik Health. <https://health.detik.com/berita-detikhealth/d-7129035/soal-body-shaming-yang-dialami-aurel-hermansyah-seserius-ini-dampaknya>

⁴ Handayani, A., Hidayat, S., & Saputra, DN (2025). Law enforcement against online gambling practices in the digital era: A case study of cyber crime in Indonesia. Al-Zayn: Journal of Social Sciences & Law, 3(2), 207-215.

⁵ Balla, H., Jumardin, J., Kasim, A., & Pappa, AK (2024). The Role of Locus and Tempus Delicti in Determining Court Competence in Cybercrime Cases. Amsir Litigation Journal, 11(4), 390-395.

The author argues that this study explains how the results of the review of previous research, it is known that studies on cyberbullying have been carried out in cyberspace, but most still focus on victim protection, proof of criminal acts, or the application of provisions in certain regulations. There is still limited research that examines cyberbullying comprehensively as a form of digital crime by examining the basis of criminalization, elements of criminal acts, criminal liability, and the effectiveness of legal regulations in dealing with the development of information technology. Therefore, this study is directed to fill this gap through a legal analysis of cyberbullying as a form of digital crime in using the Indonesian legal system. This study aims to fill this gap through the author's analysis of the position of cyberbullying as a criminal act, the basis of its criminalization, the criminal liability of the perpetrator, and the effectiveness of criminal law regulations in dealing with cyberbullying as a form of digital crime.

The development of information and communication technology in the digital era has brought significant changes to people's lives. Advances in the internet and social media have made it easier to communicate, obtain information, and carry out various daily activities .⁶ However, while this research provides significant benefits, these technological advances have also given rise to various new forms of crime that utilize digital means, known as cybercrime. One increasingly prevalent form of digital crime is cyberbullying.

Although bullying and cyberbullying are often similar in terms of form and technique in the crime, both have many differences. Unlike traditional bullying, cyberbullying allows perpetrators to hide their identity behind a computer to commit their crimes. This anonymity makes it easier for perpetrators to attack victims without having to see the victim's physical response. Where perpetrators commit this crime without knowing whether the victim has a mental or psychological illness that can cause someone's sanity or mental disorders. The influence of distance that technological devices have on today's youth often makes them say and do things that are more cruel than what usually happens in traditional face-to-face bullying situations. As for cyber phenomena in society, namely cyberbullying, the spread of hoaxes, hate speech, online fraud, hacking, theft of personal data, phishing, distribution of pornography and many more.

Criminal law plays a crucial role in maintaining order and protecting society from various forms of harmful behavior. In the context of cyberbullying, this study explains that criminal law serves as a means of protecting victims and as a deterrent to perpetrators. However, the application of criminal law to cyberbullying still faces various obstacles, including obtaining evidence, identifying perpetrators, and interpreting the elements of crimes committed through electronic media.⁷

Based on this description, cyberbullying can be explained as a phenomenon strongly relevant to the development of information technology and criminal law. The increasing number of cyberbullying cases demonstrates the need for an in-depth legal study of how Indonesian criminal law regulates, addresses, and protects victims of cyberbullying as a form of digital crime. Therefore, this study was conducted under the title "Criminal Law Review of Cyberbullying as a Form of Digital Crime."

The phenomenon of cyberbullying in Indonesia is increasing along with the growing number of internet and social media users. Victims of cyberbullying are not only children and adolescents, but also adults, public figures, and the general public. The resulting impacts are not only psychological harm, such as stress, depression, fear, loss of self-confidence, and even suicidal thoughts, but can also affect the victim's social and economic life.⁸ Therefore, cyberbullying can no longer be viewed as merely deviant behavior in the digital space, but as an act that has the potential to become a criminal offense. Cyberbullying differs from conventional bullying because it has a wider reach and greater impact. While direct bullying is usually limited to a specific place and time, cyberbullying can occur anytime and anywhere as long as the victim has access to a digital device. Furthermore, information or content used to perpetrate cyberbullying can spread quickly to the wider community, magnifying the psychological impact experienced by victims.

From a criminal law perspective, cyberbullying is related to several acts regulated by Indonesian law, such as insults, defamation, threats, the dissemination of hateful information, and other acts that attack a person's honor. Regulations regarding these acts can be found in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as well as in Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code). However, to date there are no provisions that specifically

⁶ Anisah, A., Nazib, F., & Putri, CM (2024). Cyberbullying and how to overcome it from an Islamic perspective. *Journal of Islamic Religious Education*, 3(1), 201-212.

⁷ Kurniawan, K., Mannan, K., & Darwis, M. (2024). Dissecting the Anatomy of Organized Crime: A Study of Criminal Conspiracy Decisions in the Digital Era. *Amsir Litigation Journal*, 226-232.

⁸ Najwa, FR (2024). Legal analysis of cybersecurity challenges: A case study of cyber law enforcement in Indonesia. *AL-BAHTS: Journal of Social, Political, and Legal Sciences*, 1(2), 8-16.

regulate cyberbullying as a separate crime.⁹ The lack of specific regulations regarding cyberbullying creates various problems in law enforcement practices. Law enforcement officials often have to classify cyberbullying acts into several articles that share similar elements, such as insults, defamation, or hate speech. Furthermore, the cross-border nature of digital crimes, the use of anonymous accounts, and the complexity of electronic evidence present unique challenges in the law enforcement process against cyberbullying perpetrators. This situation necessitates an examination of the extent to which positive criminal law in Indonesia has been able to accommodate and provide legal protection for victims of cyberbullying.

Based on this, an in-depth legal study is needed regarding the regulation of cyberbullying within the Indonesian criminal justice system. This study is crucial to understand how the provisions of the New Criminal Code and the Electronic Information and Transactions Law can be applied to cyberbullying, as well as to identify the various legal obstacles that arise in their enforcement. Using a normative approach, this research will examine various laws and regulations, legal doctrines, and criminal law concepts related to cyberbullying as a form of digital crime.

From a criminological perspective, cyberbullying is a form of social deviance that arises from changes in societal interaction patterns in the digital era. Easy internet access, low legal awareness, weak social control, and a culture of irresponsible social media use are factors that encourage cyberbullying. Therefore, addressing cyberbullying requires not only a criminal law approach but also educational, preventive, and social approaches.

¹⁰The core of the problem:

1. There are no specific regulations regarding cyberbullying in Indonesian criminal law.
2. Cyberbullying regulations are still scattered throughout several provisions of the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE).
3. The difficulty of proving and tracking perpetrators in the digital space.
4. Low digital literacy and legal awareness among the public.
5. Legal protection for victims of cyberbullying is not yet optimal.
6. Technological development is faster than legal development.

This research is important because it aims to analyze the extent to which existing criminal law provisions in Indonesia have been able to accommodate cyberbullying as a form of digital crime. Furthermore, this research also aims to identify weaknesses in existing legal regulations, thereby providing recommendations for legislators and law enforcement officials in realizing a more effective, just, and legal system that provides legal certainty. This research contributes to the development of criminal law, particularly as it relates to the development of digital crime and cyber law. The results of this research are expected to serve as considerations for the government, law enforcement officials, the public, and social media users in increasing legal awareness and preventing cyberbullying. Thus, this research not only has theoretical value but also provides tangible benefits for the formation of legal policies and the protection of community rights in the digital era.

METHOD

The type of research used is normative research. Normative legal research is also called doctrinal legal research, library research, or documentary study. It is called doctrinal legal research because it is conducted solely on written regulations or other materials. Normative research uses a theoretical-rational method with a deductive logical reasoning model (drawing conclusions from the general to the specific).¹¹ The approach used in this paper is the Statutory Approach, which is an approach carried out by examining all laws and regulations related to the legal issue being handled. Conceptual in legal research is a method that starts from the doctrines, thoughts, and views of legal experts to build legal arguments. This approach analyzes basic concepts to answer legal issues when laws and regulations do not.¹²

⁹ Sari, UIP (2021). Law Enforcement Policy in Cyber Crime Handling Efforts Carried Out by Virtual Police in Indonesia. *Journal of Studia Legalia*, 2(01), 58-77.

¹⁰ Ersya, MP (2017). Legal Issues in Tackling Cyber Crime in Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.

¹¹ Juliardi, B., Runtuwuwu, YB, Musthofa, MH, TL, AD, Asriyani, A., Hazmi, RM, ... & Samara, MR (2023). *Legal Research Methods*. Padang: Gita Lentera.

¹² Syarif, M., Ramadhani, R., Graha, MAW, Yanuarita, T., Muhtar, MH, Asmah, N., Syahril, MAF, ... & Jannah, M. (2023). *Legal Research Methods*. Padang: Get Press Indonesia.

RESULTS AND DISCUSSION

A. Legal Regulations Regarding Cyberbullying in the Indonesian Criminal Law System

Cyberbullying is an act committed intentionally by utilizing information technology, electronic systems, or digital media as a means to insult, defame, intimidate, threaten, harass, or otherwise attack a person's honor and dignity. This act is essentially a manifestation of the development of digital crime (cybercrime), the object and modus operandi of which are carried out through cyberspace. Although the terminology of cyberbullying has not been explicitly regulated in Indonesian law, the substance of the act has been accommodated through various criminal law provisions, particularly regarding insults, defamation, threats, and the dissemination of information that incites hatred or hostility through electronic media.¹³

According to the author's understanding, cyberbullying cannot be viewed solely as deviant behavior in the use of social media, but rather as an act that has the potential to give rise to criminal liability if it meets the elements of a criminal act as stipulated in the laws and regulations. The element of intent (*dolus*), the existence of an unlawful act, the use of electronic media as a means, and the occurrence of harm to the honor, good name, or psychological condition of the victim are indicators that determine whether an action can be qualified as a criminal act. Therefore, cyberbullying has characteristics as a form of digital crime that requires law enforcement through the application of provisions in Law Number 1 of 2023 concerning the Criminal Code and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.¹⁴

Conventional bullying and cyberbullying are fundamentally similar: both are acts intended to harm, intimidate, or demean another person. The differences lie in the medium used, the nature of the act, and the resulting legal consequences. Conventional bullying occurs directly through physical or verbal contact in a specific location, while cyberbullying occurs through electronic media or cyberspace, making its reach broader and its impact more difficult to stop.

Aspect	Conventional Bullying	Cyberbullying
Media	Done in a way direct (face to face) face).	Done via electronic media , internet, or social media .
Form Deeds	Violence physical , insults verbal , extortion , intimidation direct .	Insults , defamation , threats , spread Photo or video, speech hatred , harassment through digital platforms.
Range	Limited to location and time certain .	Accessible When just and reach out public wide without territorial boundaries.
Identity of the Perpetrator	Generally known by the victim.	The perpetrator can use identity false or anonymous so that difficult identified .
Impact	Characteristic direct towards the victim at the time incident .	Impact psychological more prolonged Because digital content can Keep going scattered and difficult deleted .
Proof	Depend on witnesses and goods proof conventional .	Use tool proof electronics , such as catch screens , digital recordings , metadata, and traces electronics .
Legal basis	Criminal Code and provisions criminal general if fulfil element action criminal .	Criminal Code, Law Number 1 of 2023 concerning the Criminal Code, and Law Number 1 of 2024 concerning Change Second on the ITE Law.

Legally, cyberbullying is not yet regulated as a separate crime in Indonesian law. However, various forms of cyberbullying can be prosecuted under several criminal provisions, both in Law Number 1 of 2023 concerning the Criminal Code and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Efforts to prevent and protect victims are as follows:

¹³ Hutabarat, SA, Praja, SJ, Suhariyanto, D., Paminto, SR, Kusumastuti, D., Fajrina, RM, ... & Abas, M. (2023). CYBER-LAW: Quo Vadis Regulation of the ITE Law in the Industrial Revolution 4.0 Towards the Era of Society 5.0. Jambi: Sonpedia Publishing Indonesia.

¹⁴ Vide Law Number 1 of 2024 concerning Change Second on Constitution Number 11 of 2008 concerning Electronic Information and Transactions .

a) Preventive

Cyberbullying prevention is carried out through increasing digital literacy to raise public awareness of the responsible, ethical, and legal use of information technology. Schools have a preventive role through character education, promoting digital media ethics, and monitoring students' internet use. Parents play a role in supervising, assisting, and guiding their children's digital activities to prevent cyberbullying. Digital platforms are obligated to provide reporting systems, moderate violating content, and take swift action against accounts or posts containing elements of cyberbullying.

b) Repressive

The government, through the Ministry of Communication and Digital (Komdigi), has the authority to terminate access or block content containing elements of cyberbullying to protect users and create a safe digital space.

c) Restorative

The cases of Audrey and Aurel Hermansyah showed contrasting outcomes. Mediation in Audrey's case failed because diversion failed to reach an agreement, and public opinion was already formed before the medical facts were revealed. In Aurel's case, however, mediation was successful because the perpetrator publicly apologized, removed the defamatory content, and the report was withdrawn.

Article 27 paragraph (3) of the Electronic Information and Transactions Law, stipulates that any person who intentionally and without authority carries out the act of distributing, transmitting, or making accessible Electronic Information and/or Electronic Documents containing elements of insult or defamation, may be held criminally liable in accordance with the provisions of statutory regulations.¹⁵ The provisions of Article 27 paragraph (4) of the Electronic Information and Transactions Law, provide a legal basis for acts carried out intentionally and without authority in the form of distribution, transmission, or actions that cause Electronic Information and/or Electronic Documents containing blackmail or threats to be accessed by other parties. In the context of cyberbullying, this provision is relevant to prosecute perpetrators who use electronic media as a means of intimidating, threatening, or blackmailing victims, thereby causing fear, psychological pressure, or other losses.¹⁶

The provisions of Article 29 of the Electronic Information and Transactions Law (ITE Law) provide a legal basis for any act carried out intentionally and without authority in the form of sending Electronic Information and/or Electronic Documents containing threats of violence or intimidation to certain individuals. In the context of cyberbullying, this norm is relevant to the actions of perpetrators who use electronic media to threaten, frighten, or intimidate victims personally, thereby causing fear, psychological pressure, and disturbing the victim's sense of security.

The characteristics of cyberbullying are as follows:

a) Done repeatedly (repeated behavior)

Cyberbullying generally doesn't happen just once, but rather continuously or repeatedly, causing long-term psychological distress for the victim. The intensity of the repeated acts indicates a pattern of intentional intimidation.

b) There is an intention to harm

Cyberbullying is carried out with an element of intent (*dolus*), namely the perpetrator's desire to embarrass, intimidate, demean, threaten, or cause suffering to the victim through digital media.

c) Using electronic media

Cyberbullying is carried out using information technology tools, such as social media, instant messaging apps, email, online forums, online games, or other digital platforms. The use of electronic media is the main difference between cyberbullying and conventional bullying.

In practice, victims of cyberbullying often experience psychological disorders in the form of stress, anxiety, depression, decreased self-confidence, and even the desire to end their lives. These impacts indicate that cyberbullying is no longer just an ethical issue in the use of social media, but has developed into a form of digital crime that threatens human rights, especially the right to honor, security, and legal protection. The problem in this study is the existence of bullying actions carried out through electronic media that have the potential to violate a person's rights and dignity and cause psychological and social harm. In addition, the development of digital technology makes this form of crime increasingly easy to commit, while public understanding of the legal

¹⁵Vide Article 27 paragraph (3) of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

¹⁶ Vide Article 29 of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

consequences of cyberbullying is still relatively low. Article 433 paragraph (1) of the Criminal Code stipulates that anyone who attacks the honor or good name of another person by accusing something to be made public shall be punished for defamation with a maximum imprisonment of 9 months or a maximum fine of Rp. 10,000,000.00 (Category II). According to the author's understanding, the elements that must be fulfilled include the existence of a legal subject, the act of attacking honor or good name, accusations regarding a particular act, and the intention for the accusation to become public knowledge.

In addition, Article 434 paragraph (1) of the Criminal Code regulates the crime of slander if the perpetrator cannot prove the truth of the accusation and the accusation is contrary to what he knows, with the threat of a maximum prison sentence of 3 years or a maximum fine of IDR 200,000,000.00 (Category IV). Article 435 emphasizes that a person cannot be punished for slander if a court decision with permanent legal force states that the accusation is true.¹⁷ Article 436 and Article 437 of the Criminal Code provide protection against minor insults. In the context of cyberbullying, this provision is relevant to the use of harsh words, ridicule, or verbal harassment through electronic media that can harm the victim's honor. The perpetrator can be punished with a maximum prison sentence of 6 months or a maximum fine of IDR 10,000,000.00 (Category II). Article 438 of the Criminal Code provides protection against the submission of untrue suspicions or accusations that can damage a person's honor and good name. In addition, Article 263 of the Criminal Code regulates the prohibition of openly inciting others to commit criminal acts, violence, or violations of the law, which in the digital space can take the form of provocation via electronic media.¹⁸

Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence also provides protection against sexually charged cyberbullying. Article 5 regulates non-physical sexual harassment through speech, writing, images, or digital communication that causes the victim to feel embarrassed, humiliated, or suffer psychologically. Article 14 paragraph (1) regulates Electronic-Based Sexual Violence (KSBE), including the recording of sexually charged images without consent, sending unwanted sexual content, and stalking via electronic media for sexual purposes. Furthermore, Article 1 paragraph (1) of the Criminal Code emphasizes the principle of legality, namely that no act can be punished except based on criminal provisions that existed before the act was committed. Thus, these various provisions form the basis for legal protection for victims of cyberbullying. Cyberbullying itself has various forms that have developed along with advances in information technology, but basically all aim to attack the honor, dignity, sense of security, and psychological condition of the victim through electronic media.¹⁹

Furthermore, in this study, the author assesses that cyberbullying has various forms that have developed along with advances in information technology. Each form has different characteristics, but essentially all aim to attack the honor, dignity, sense of security, and psychological condition of the victim through electronic media. Flaming is the act of sending messages or comments containing harsh words, insults, or curses through social media, discussion forums, messaging applications, or other digital platforms with the aim of embarrassing or degrading the victim. Harassment (online harassment) is the continuous sending of messages containing insults, threats, harassment, or intimidation that causes prolonged psychological stress. Doxing is the act of obtaining, disclosing, or disseminating someone's personal data without their consent via the internet to intimidate or embarrass the victim. Cyberstalking is the act of continuously monitoring, following, contacting, or intimidating someone through electronic media so that the victim feels afraid or threatened.

Another form of harassment is the distribution of memes or videos that are harassing, namely creating, editing, or distributing memes, photos, or videos intended to embarrass or degrade someone. Furthermore, there is hate speech containing insults, incitement, or hatred against a person or group based on ethnicity, religion, race, intergroup relations (SARA), gender, disability, or other specific characteristics. If these actions meet the requirements of the law, they can be subject to criminal sanctions.²⁰

The development of information and communication technology has transformed the pattern of social interaction from conventional communication to digital communication via the internet. The presence of social media, instant messaging applications, online forums, and video sharing services makes it easier to communicate without being limited by space and time. However, this development has also given rise to various new forms of crime known as cybercrime, one of which is cyberbullying. Research confirms that the impact of cyberbullying on

¹⁷ Vide Article 434 (1) of the Law Number 1 of 2023 concerning the Criminal Code .

¹⁸ Vide sections 346 and 347 of the Act Number 1 of 2023 concerning the Criminal Code .

¹⁹ Rafika Nur, Amriyanto, Handar Subhandi Bakhtiar, Sunardi Purwanda . (2023). System Justice Criminal Law . Gorontalo: Cahaya Arsh Publisher & Printing.

²⁰ Ode Abdurachman, Henny Saidan,... & Achmad Yusuf. (2026). Cyber Law 4.0: Regulation , Security , and Digital Ethics. Jambi: Nawala Gama Education.

mental health is consistent over the long term, so that prevention programs, effective interventions, and strengthening of legal regulations are needed to provide optimal protection for children and adolescents. Manifestations of cyberbullying in the form of intimidation and insults through social media and instant messaging platforms have developed into a form of digital crime because it utilizes electronic systems as a means of committing unlawful acts.

Article 29 of Law Number 1 of 2024 stipulates that anyone who intentionally and without authority sends electronic information or electronic documents containing threats of violence and intimidation delivered in person may be subject to sanctions. Unlike conventional bullying, cyberbullying has more complex characteristics because the perpetrator does not have to meet the victim in person and often uses anonymous or fake identities, making it easier to repeatedly insult, threaten, and harass. This research will also explain how to deal with cyberbullying.²¹

1. Improving digital literacy
2. Instilling social media ethics
3. Strengthening parental supervision
4. The role of schools in preventing cyberbullying
5. Family planning as a form of prevention
6. Do not respond to the perpetrator's actions
7. Storing digital evidence
8. Reporting content to digital platforms
9. Psychological assistance to victims
10. Collaboration between government, society, and digital platform providers

Furthermore, information published through digital media can spread very quickly to thousands, even millions, of internet users in a short time, resulting in a far greater impact on victims than traditional bullying. Once content is shared online, it is extremely difficult to completely erase its digital footprint, as it is stored on various servers and other users' devices. Therefore, cyberbullying not only attacks a person's dignity at the time of the act, but also leaves lasting psychological impacts due to the existence of these digital footprints.

To date, the Criminal Code (KUHP) has not yet regulated cyberbullying as a separate crime. However, various forms of cyberbullying can be classified as criminal acts of insult, defamation, slander, or threats through electronic media. The only difference lies in the medium used, namely digital media. According to Adnan and Putriyani, legal protection for victims of cyberbullying is not sufficient through criminal law enforcement alone, but also through preventive, educational, and assistance efforts for victims. This opinion is in line with Article 59A of Law Number 35 of 2014 concerning Child Protection, which regulates physical, psychological, and social rehabilitation and psychosocial assistance for child victims of crime.

The 2024 National Survey of Life Experiences of Children and Adolescents (SNPHAR) showed that 14.49% of boys and 13.78% of girls aged 13–17 had experienced cyberbullying. The Ministry of Communication and Digital also stated that approximately 48% of Indonesian children had experienced cyberbullying. Dewi, Nahak, and Widyantara stated that cyberbullying is a new type of crime using electronic means, which in Indonesia is categorized as defamation. However, the Criminal Code still has limitations because it is formulated based on conventional crime concepts, so it does not fully accommodate the characteristics of cyberbullying through digital media.

Cyberbullying regulations can be found in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. The ITE Law serves as the primary legal basis for handling cyberbullying because it regulates insults, defamation, threats of violence, the dissemination of information that attacks a person's honor, and the dissemination of unlawful content. In the author's understanding, law enforcement officers use the ITE Law more often than the Criminal Code when cyberbullying is carried out through social media, messaging applications, online forums, or other digital platforms. However, the ITE Law does not provide a specific definition of cyberbullying, so law enforcement still has to link it Based on Simons' theory of criminal acts, a crime must fulfill the elements of an act, be unlawful, be done wrongfully, and be subject to criminal penalties. These elements are reflected in Article 12, Article 1 paragraph (1), and Article 64 of Law Number 1 of 2023 concerning the Criminal Code. Thus, cyberbullying can be punished if it fulfills the elements of a criminal act through Articles 433–442 of the Criminal Code and Article 27A in conjunction with Article 45 paragraph (4) and Article 29 in conjunction with Article 45B of the ITE Law. However, the absence of specific regulations means that

²¹Vide Article 29 of Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

legal certainty is not optimal because law enforcement officers still have to interpret the various criminal provisions that are scattered with relevant articles.²²

B Implementation of Criminal Provisions Against Cyberbullying Perpetrators Based on the Criminal Code and the ITE Law

Cyberbullying is a form of crime that has emerged as a consequence of the rapid advancement of information and communication technology. The development of the internet has provided many benefits to people's lives, such as facilitating access to information, accelerating communication, and expanding social interaction. However, on the other hand, this progress has also given rise to various forms of digital media abuse, one of which is cyberbullying. Unlike conventional bullying, which occurs in person, cyberbullying is carried out through electronic media, such as social media, instant messaging applications, online forums, and other digital platforms. These acts can include insults, defamation, spreading slander, threats, the unauthorized distribution of photos or videos, hate speech, and even the dissemination of personal information intended to embarrass the victim.²³

From a criminal law perspective, an act can only be punished if it meets the elements of a crime as stipulated in statutory regulations. This principle is known as the principle of legality, as stipulated in the Criminal Code, which emphasizes that no act can be punished except based on the provisions of previously applicable statutory regulations. Therefore, even though the term cyberbullying is not explicitly mentioned in the Criminal Code or the ITE Law, law enforcement officials can still prosecute perpetrators as long as their actions meet the elements of certain crimes.

Criminal provisions under the Criminal Code (KUHP) generally apply to cyberbullying perpetrators if the act involves insults, defamation, slander, threats, or coercion. The new Criminal Code, as stipulated in Law Number 1 of 2023, further systematically regulates various forms of insults to a person's honor or reputation.²⁴ Insults are defined as any act that attacks a person's honor or reputation with the intent of making it known to others. In cyberbullying, insults are often perpetrated through social media posts, comments on digital platforms, or the distribution of images or videos intended to demean the victim.

Besides insults, cyberbullying can also take the form of defamation. Defamation occurs when someone spreads accusations or information that attacks another person's honor, thereby harming the victim's reputation. In the context of digital media, defamation has a far broader impact than direct insults because information published online can be easily disseminated, stored, and accessed by the public for extended periods. Therefore, the psychological and social impacts experienced by victims are often more severe.

If the perpetrator makes an accusation they know to be false with the intention of defaming the victim, their actions can be classified as slander. The element of intent is crucial in proving this crime. The public prosecutor must prove that the perpetrator knew the information they spread was false but nevertheless disseminated it to the public via electronic media.

Cyberbullying can also manifest in the form of online threats of violence or intimidation. These threats can take the form of text messages, emails, or social media posts containing threats to the safety of the victim's life, property, or family. Under certain circumstances, these threats can cause serious fear, disrupting the victim's activities and psychological well-being. Such actions can be subject to criminal provisions regarding threats as stipulated in the Criminal Code if all elements of the crime are met. Although the Criminal Code can be used to ensnare various forms of cyberbullying, developments in information technology have led to the emergence of more specific regulations through the Electronic Information and Transactions (ITE) Law. This law serves as the primary legal basis for law enforcement against various crimes that use electronic systems as a means of implementation. The existence of the ITE Law provides legal certainty by more specifically regulating the distribution of unlawful electronic information.

One of the provisions most frequently applied to cyberbullying perpetrators is the prohibition on distributing, transmitting, or making accessible electronic information containing insulting or defamatory content. This provision aims to protect a person's honor from attacks carried out through electronic media. In practice, law enforcement officials must prove that the perpetrator intentionally disseminated electronic information to another party and that the information contained insulting or defamatory content.

²² Sirait, TM, & SH, M. (2024). *Cyber Law in Theory and Its Development (Cyber Crime, Data Privacy, E-Commerce)*. Sleman: Deepublish.

²³ Sakti, APSAP (2024). Criminal Law Policy In Implementing, the Value of Justice and Legal Certainty in the Scope of Cyber Law. *Das Sollen : Journal of Contemporary Studies of Law and Society*, 2(02).

²⁴ Elvi Susanti Syam. (2024). *Criminal Procedure Law*. Makassar: De La. Macca.

Amendments to the ITE Law through Law Number 1 of 2024 clarify several provisions that previously often gave rise to differing interpretations. These changes are aimed at providing a more balanced protection between freedom of expression and the honor, dignity, and rights of every person. Therefore, not every criticism or opinion expressed through electronic media can be immediately categorized as a crime. Law enforcement must consider the context, purpose of the communication, the public interest, and the presence of intent in the perpetrator's actions.²⁵

Cyberbullying can also be carried out through the spread of false news that harms the victim. For example, a perpetrator spreads false information about someone's personal life, causing hatred, social exclusion, or economic loss. If the dissemination of such information meets the elements of a crime stipulated in the Electronic Information and Transactions Law (UU ITE) or the Criminal Code, the perpetrator can be held criminally liable. Furthermore, the dissemination of personal data without the victim's consent can also have legal consequences if it is done with the intention of humiliating or intimidating the victim.²⁶

Another form of cyberbullying is hate speech directed at a particular individual or group based on ethnicity, religion, race, intergroup relations, gender, or other identities. Under certain circumstances, hate speech not only harms a specific individual but can also disrupt public order and trigger social conflict. Therefore, if such actions meet the elements of a criminal offense as stipulated in laws and regulations, the perpetrator may be subject to criminal sanctions. In the law enforcement process, evidence plays a crucial role. Unlike conventional crimes, cyberbullying requires electronic evidence as one of the primary means of proof. This evidence can include screenshots, recordings of electronic conversations, emails, social media posts, video recordings, metadata, or the results of digital forensic examinations. Based on applicable criminal procedure law and the provisions of the ITE Law, electronic information and electronic documents are valid evidence as long as they are obtained in accordance with legal procedures.

In addition to proving a criminal act, law enforcement officials must also establish the perpetrator's identity. In practice, cyberbullying perpetrators often use anonymous accounts, fake identities, or virtual networks, complicating the investigation process. Therefore, investigators require the assistance of digital forensic experts to trace IP addresses, electronic devices used, digital activity history, and the relationship between social media accounts and the perpetrator's identity. The results of these examinations are then used as evidence in court proceedings.

Criminal liability for cyberbullying perpetrators is essentially based on fault, whether intentional or negligent, according to the applicable criminal law. In most cyberbullying cases, intent is the primary element that must be proven. The perpetrator is deemed to have known that their actions could demean, humiliate, threaten, or defame the victim, but still committed the act. Intention can be proven through the content of conversations, communication patterns, frequency of actions, and the perpetrator's purpose in disseminating information. Judges also consider various aggravating and mitigating circumstances when sentencing. Aggravating factors include repeated acts, involving multiple accounts, causing severe trauma to the victim, causing the victim to lose their job, drop out of school, suffer mental health problems, or even encourage the victim to commit acts that endanger themselves. Conversely, mitigating circumstances can include the perpetrator's confession, remorse, reconciliation with the victim, prior conviction, and efforts to recover losses.

In some cases, resolution through a restorative justice approach is also being considered, particularly when the impact is not too severe and the parties are willing to resolve the case through amicable settlement. This approach aims to restore the relationship between the perpetrator and the victim without diminishing the function of criminal law as a means of protecting society. However, the application of restorative justice must be selective, taking into account the interests of the victim, the level of culpability of the perpetrator, and the resulting social impact. If cyberbullying results in serious harm or is carried out systematically, resolution through the criminal justice process remains the more appropriate option.²⁷

The application of criminal provisions to cyberbullying perpetrators also faces several obstacles. First, there is still a perception that mutual insults on social media are part of freedom of expression. However, freedom of expression is not an absolute right, as it requires respect for the rights and dignity of others. Second, low digital literacy levels mean that many people do not understand the difference between legitimate criticism and insults or

²⁵ Vide Law Number 1 of 2024 concerning change second regarding Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

²⁶ Sihotang, M., & Hoessein, ZA (2025). Transformation political law in strengthening Cyber law regulations in Indonesia. *Jurnal Syntax Admiration*, 6(1), 586-596.

²⁷ Handayani, A., Hidayat, S., & Saputra, DN (2025). Enforcement law to practice Online gambling in the digital age: A case study Cyber crime in Indonesia. *Al-Zayn: Journal Knowledge Social & Law*, 3(2), 207-215.

defamation. Third, rapid technological developments often outpace regulatory developments and the ability of law enforcement to uncover cybercrimes. Furthermore, the characteristics of social media, which allow information to spread widely in a short time, make the impact of cyberbullying more complex than traditional bullying. Once information is published, it can be copied, shared, or saved by other users, making restoring the victim's reputation even more difficult. Therefore, law enforcement must be balanced with preventative efforts through digital literacy education, improving social media ethics, and strengthening oversight of digital platform use.

From the explanation above, the application of criminal provisions against cyberbullying perpetrators in Indonesia does not depend on the existence of specific regulations regarding cyberbullying as a separate crime. Various forms of cyberbullying can be prosecuted through provisions regarding insults, defamation, slander, threats, hate speech, and misuse of electronic information as regulated in the Criminal Code and the ITE Law. The application of these two legal instruments is carried out in a complementary manner according to the characteristics of the actions committed by the perpetrator. The success of law enforcement depends heavily on the ability of law enforcement officials to prove the elements of the crime, utilize electronic evidence, and balance protection of freedom of expression with protection of the honor, dignity, and rights of every citizen. With consistent law enforcement and supported by increased public legal awareness, cyberbullying is expected to be minimized so that the digital space becomes safer, healthier, and more responsible.

CONCLUSION

Legal provisions regarding cyberbullying in the Indonesian criminal justice system have not yet been regulated as a stand-alone crime. However, various forms of cyberbullying can be prosecuted through provisions in Law Number 1 of 2023 concerning the Criminal Code (KUHP) and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). These provisions cover criminal offenses such as insults, defamation, threats, the dissemination of hateful information, and other acts that attack a person's honor through electronic media. However, the absence of specific regulations regarding cyberbullying has resulted in a lack of legal certainty in its enforcement.

The application of criminal provisions against perpetrators of cyberbullying is carried out by adjusting the character of the actions carried out with the elements of criminal acts that have been regulated in the criminal code (KUHP) and the law on information and electronic transactions (UU ITE). Criminal responsibility can be imposed on the perpetrator if the elements of an unlawful act, error, ability to be responsible, and the existence of valid electronic evidence are met.

SUGGESTION

Recommend to lawmakers (DPR and Government) to formulate specific articles or offenses regarding *cyberbullying in future revisions to cyber law regulations*, instead of relying solely on composite articles (such as articles on defamation, insults, or threats). And also encourage the Police and Prosecutors to improve the technical capacity of investigators/prosecutors and expand the availability of *digital forensics facilities* down to the regional/resort police level (Polda/Polres).

REFERENCES

- Anisah, A., Nazib, F., & Putri, C. M. (2024). Perundungan dunia maya (cyberbullying) dan cara mengatasi perspektif Islam. *Jurnal Pendidikan Agama Islam*, 3(1), 201-212.
- Balla, H., Jumardin, J., Kasim, A., & Pappa, A. K. (2024). Peran Locus dan Tempus Delicti dalam Menentukan Kompetensi Pengadilan pada Kasus Kejahatan Siber. *Jurnal Litigasi Amsir*, 11(4), 390-395.
- Elvi Susanti Syam. (2024). *Hukum Acara Pidana*. Makassar: De La. Macca.
- Fiyanti, D. A. A. R., Dewi, A. A. S. L., & Suryani, L. P. (2026). Perlindungan Hukum Terhadap Content Creator Akibat Cyberbullying Pada Sosial Media Instagram. *Jurnal Analogi Hukum*, 8(1), 69-75.
- Handayani, A., Hidayat, S., & Saputra, D. N. (2025). Penegakan hukum terhadap praktik judi online di era digital: Studi kasus cyber crime di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(2), 207-215.
- Haris Fdhil. (2019). Berawal dari Bully di Medsos, Begini Kronologi Kasus Audrey. *Detik News*. https://news.detik.com/berita/d-4506079/berawal-dari-bully-di-medsos-begini-kronologi-kasus-audrey?utm_source
- Hutabarat, S. A., Praja, S. J., Suhariyanto, D., Paminto, S. R., Kusumastuti, D., Fajrina, R. M., ... & Abas, M. (2023). *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. Jambi: Sonpedia Publishing Indonesia.

- Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.
- Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). *Metode Penelitian Hukum*. Padang: Gita Lentera.
- Kurniawan, K., Mannan, K., & Darwis, M. (2024). Membedah Anatomi Kejahatan Terorganisir: Studi Putusan Permufakatan Jahat di Era Digital. *Jurnal Litigasi Amsir*, 226-232.
- Nafilah Sri Sagita. (2024). Soal Body Shaming yang Dialami Aurel Hermansyah, Seseius Ini Dampaknya. *Detik Health*. <https://health.detik.com/berita-detikhealth/d-7129035/soal-body-shaming-yang-dialami-aurel-hermansyah-seserius-ini-dampaknya>
- Najwa, F. R. (2024). Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, 1(2), 8-16.
- Ode Abdurachman, Henny Saida,...& Achmad Yusuf. (2026). *Cyber Law 4.0: Regulasi, Keamanan, dan Etika Digital*. Jambi: Nawala Gama Education.
- Rafika Nur, Amriyanto, Handar Subhandi Bakhtiar, Sunardi Purwanda. (2023). *Sistem Peradilan Pidana*. Gorontalo: Cahaya Arsh Publisher & Printing.
- Sakti, A. P. S. A. P. (2024). Kebijakan Hukum Pidana Dalam Mengimplementasikan, Nilai Keadilan, dan Kepastian Hukum Dalam Ruang Lingkup Cyber Law. *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, 2(02).
- Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Journal of Studia Legalia*, 2(01), 58-77.
- Sihotang, M., & Hoessein, Z. A. (2025). Transformasi politik hukum dalam penguatan regulasi cyber law di Indonesia. *Jurnal Syntax Admiration*, 6(1), 586-596.
- Sirait, T. M., & SH, M. (2024). *Cyber Law dalam Teori dan Perkembangannya (Cyber Crime, Privacy Data, E-Commerce)*. Sleman: Deepublish.
- Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., Syahril, M. A.F., ... & Jannah, M. (2023). *Metode Penelitian Hukum*. Padang: Get Press Indonesia.

Statutes, Laws and Regulations

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).