JURNAL
POROS HUKUM
PADJADJARAN

P-ISSN: 2715-7202
E-ISSN: 2715-9418

Volume 7, Number 1, November 2025

Submission:
22/09/2025

Accepted:
25/11/2025

Published:
30/11/2025

DOI:
https://doi.org/10.23920/jphp.v7i1.2697

Link Publication:
https://jurnal.fh.unpad.ac.id/index.php/jphp/issue/archive

Publisher:
Magister of Laws
Universitas Padjadjaran

Legal Issues in Applying Criminal Law to Cyberbullying Offenses Through the Anonymous Messaging Application NGL.Link

Navaratu Annisa Devi[a], Dewi Mayaningsih[b], Fenny Fatriani[c]

ABSTRACT

Advances in information technology have led to the emergence of various forms of digital interaction, including the use of anonymous messaging applications such as NGL.Link. Despite its convenience, this platform has also given rise to the phenomenon of cyberbullying in the form of online insults or defamation. This study aims to analyze the application of Article 310 of the Criminal Code in conjunction with Article 27A of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions against perpetrators of cyberbullying through the anonymous messaging application NGL.Link. The research method used is normative juridical. Data was obtained through legislation and legal literature as primary data and interviews with legal experts as secondary data. The results of the study indicate that the application of Article 310 of the Criminal Code and Article 27A of the ITE Law faces legal obstacles, especially in proving the elements of "in public" and "dissemination of electronic information". The closed, personal, and anonymous nature of NGL.Link communication means that the publicity element required in both articles is not fulfilled, so that the perpetrator cannot be held criminally liable. This study concludes that there is a need for a more adaptive interpretation and update of cyber criminal law in order to ensure legal certainty and effective protection for victims of cyberbullying in anonymous digital spaces.

Keywords: cyberbullying; NGL.Link; criminal liability.

INTRODUCTION

The development of information and communication technology has brought significant changes to the patterns of social interaction within society. The presence of internet-based technology has provided enormous benefits, particularly in facilitating communication and the dissemination and exchange of information across various levels of society. The internet has opened up new horizons in social life by enabling the rapid, widespread, and unlimited flow of information. Based on data from We Are Social in the Global Digital Report, the number of internet users in Indonesia alone in January 2025 reached around 212 million people, with a penetration rate of 74.6% of

[a] State Islamic University of Sunan Gunung Djati Bandung. Jl. AH. Nasution No. 105, Cipadung Wetan, Kec. Cibiru, Kota Bandung, Jawa Barat. Indonesia. Correspondence email: navaratu14@gmail.com
[b] State Islamic University of Sunan Gunung Djati Bandung. Jl. AH. Nasution No. 105, Cipadung Wetan, Kec. Cibiru, Kota Bandung, Jawa Barat. Indonesia.
[c] State Islamic University of Sunan Gunung Djati Bandung. Jl. AH. Nasution No. 105, Cipadung Wetan, Kec. Cibiru, Kota Bandung, Jawa Barat. Indonesia.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

the total population of around 285 million. The growth of internet users in Indonesia from the previous year was around 8.7%, with an additional 17 million new users in the last year.[1]

Currently, information dissemination is largely carried out through internet-based media, one of which is social media, which makes it easier for people to access and share information. Digital media no longer functions solely as a means of communication, but has also become a new space for various acts that have the potential to violate the law, one of which is *cyberbullying*. *Cyberbullying* is an act of insulting, harassing, or attacking someone through electronic media and can have psychological and social impacts on the victim. In Indonesian, *"bully"* has the same meaning as oppression or persecution.[2] Based on a survey conducted by the Ministry of Women's Empowerment and Child Protection (KemenPPPA) in 2024, it was found that most victims of *cyberbullying* were aged between 18 and 25 years old. In addition, according to SAFEnet (Southeast Asia Freedom of Expression Network), the number of cases of Online Gender-Based Violence (KBGO) in Indonesia in the first quarter of 2024 increased by 118 cases compared to the previous year.[3] This shows that cyberbullies are beginning to exploit weaknesses in the virtual world to commit acts of violence.

The complexity of *cyberbullying* is increasing with the emergence of *anonymous* messaging apps, one of which is NGL.Link. This app uses the term "NGL," which comes from the informal expression "Not Gonna Lie." NGL.Link was introduced to the public in November 2021 and was developed by DeepMoji, an independent group of developers based in Venice Beach, California, United States. Users can share NGL.Link links on their social media profiles, particularly through the Instagram Story feature. From these links, other social media users can send *anonymous* messages, and the recipients can receive *anonymous* messages from other parties. Conceptually, NGL.Link is designed as a means of communication that encourages freedom of expression, providing a space for users to express their opinions, questions, or feelings honestly without having to reveal their personal identity. The anonymity system implemented allows for one-way or two-way communication without the sender's name being included. Although NGL.Link also has a paid feature called Who Sent This, where users can find out the sender's location. Thus, this application basically functions as a container

[1] We Are Social, 2025 "Special Report Digital 2025 Indonesia" https://wearesocial.com/id/blog/2025/02/digital-2025/ [accessed on August 06, 2025].
[2] Hatarto Pakpahan, "Criminal Law Aspects of Cyberbullying on Social Media." *Cakrawala Law Journal* 11, no. 3 (2020). https://doi.org/10.26905/idjch.v11i3.5718
[3]Ministry of Women's Empowerment and Child Protection, "Press Release Number B-219/SETMEN/HM.02.04/7/2024 Regarding the Protection of Women and Children in the Digital Space." https://www.kemenpppa.go.id/index.php/siaran-pers/gandeng-sejumlah pihak-kemen-pppa-dorong-aksi-bersama-lindungi-perempuan-dan-anak-dari-kekerasan-di-ranah-daring [accessed on August 06, 2025].

P-ISSN: 2715-7202
E-ISSN: 2715-9418

for *anonymous* messages from unknown parties, with the main target group being internet users ranging from teenagers to young adults.

Anonymous applications such as NGL actually have a positive side in the business world. For example, they can serve as a suggestion box in the business world. NGL can be used as a place for customers to provide reviews, criticism, and suggestions to companies.[4] However, there are also negative aspects if these anonymous apps are not used wisely, given that the anonymity system in these apps makes cyberbullies feel more free to express themselves, including in making negative comments. Of course, this has a detrimental impact on the recipient, especially when the messages received contain irresponsible comments that cause distress and insecurity.

As a real example, *cyberbullying* happened to a female student at Pasundan University, majoring in International Relations, with the initials MR. Around 2021, the student with the initials MR shared her NGL.Link link on her Instagram story. After the link was shared, MR immediately received a number of taunts, insults, and threats through the *anonymous* messaging app NGL.Link. At the time, MR tried to find out who sent the messages using the "Who Sent This" feature. However, this feature only displayed the type of phone used by the sender. This meant that MR could not determine exactly who sent the *anonymous* messages because the information provided by the feature was very limited, making it relatively difficult to guess the sender's identity.

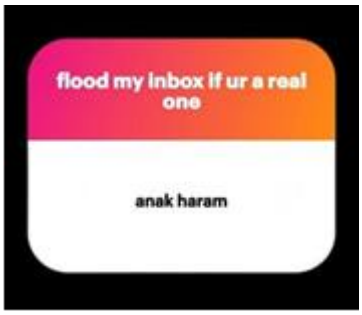

Figure 1.1 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

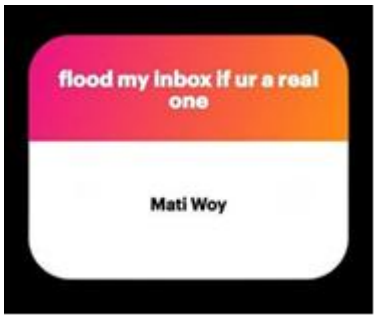

Figure 1.2 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

[4] Salisa Rizky Permata, "Reasons for Using the NGL App – Anonymous Q&A." https://digilib.unila.ac.id/74347/ [accessed on August 10, 2025].

P-ISSN: 2715-7202
E-ISSN: 2715-9418

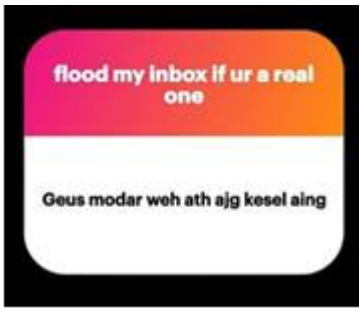

Figure 1.3 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

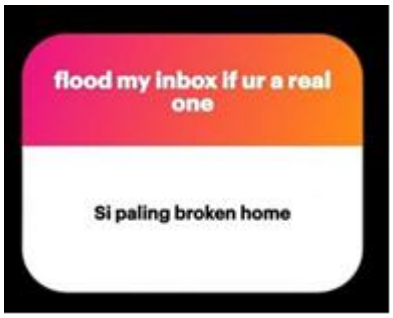

Figure 1.4 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

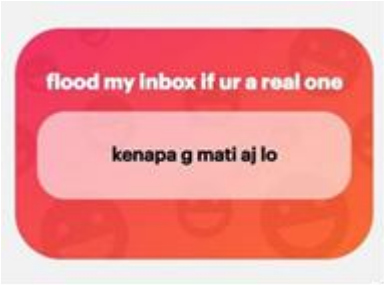

Figure 1.5 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

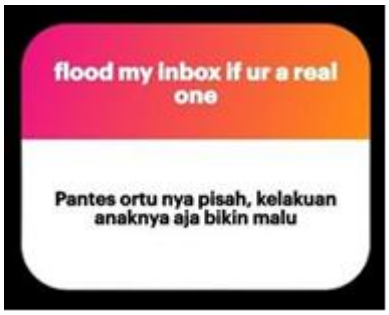

Figure 1.6 Example of *Cyberbullying* on the NGL.Link Application
Source: Researcher Processed Data, 2025

The images above are empirical evidence of *cyberbullying* against a female student with the initials MR. These actions have the potential to lead to misuse of the NGL.Link application by individuals who use the application as a means of *cyberbullying*. Legally, *cyberbullying* can be analyzed through a normative approach by referring to applicable laws and regulations. Generally, *cyberbullying* cases fall under the category of criminal offenses regulated in Article 310 of the Criminal Code (KUHP). The following is the text of Article 310 of the Criminal Code (KUHP) based on Constitutional Court Decision No. 78/PUU-XXI/2023:

(1) *"Anyone who intentionally attacks the honor or reputation of another person by making an accusation verbally, with the clear intention of making it known to the public, shall be punished for defamation with a maximum imprisonment of nine months or a maximum fine of four thousand five hundred rupiah.*
(2) *If this is done in writing or through images that are broadcast, displayed, or posted in public, then it is punishable as written defamation with a maximum imprisonment of 1 year and 4 months or a maximum fine of Rp 4.5 million.*

P-ISSN: 2715-7202
E-ISSN: 2715-9418

(3) *Neither slander nor libel shall exist as far as the principal obviously has acted in the general interest or for a necessary defence."*[5]

Article 310 of the Criminal Code (KUHP) regulates verbal and written defamation and libel. In the KUHP, the criminal act of defamation is regulated as a complaint offense. Because it is classified as a complaint offense, prosecution of this act requires a prior complaint from the victim as the party who has directly suffered harm.[6]

The meaning of the phrase "*in public*" in Article 310 of the Criminal Code is interpreted to mean that statements that are insulting or defamatory are conveyed in such a way that they can be known by the wider community, not just by the person being insulted.[7] This element presupposes publicity, namely the possibility that third parties (other than the victim and perpetrator) are aware of the content of the insult. Meanwhile, in cases of *cyberbullying* carried out through *anonymous* messaging applications such as NGL.Link, the NGL system is anonymous and closed *(one-to-one)*, meaning that messages are sent directly to the recipient and cannot be accessed by the public. This means that there is no element of dissemination of information to the general public, because the content of the message is only known to the victim *(recipient)* and the NGL system server *(not the general public)*. Therefore, the element of "*in public*" becomes debatable because, from a technical standpoint, the message cannot be seen or known by the general public; only the recipient of the message can see the content of the message.

Meanwhile, Article 27A of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions explicitly stipulates that:

> "*Any person who intentionally attacks the honor or reputation of another person by accusing them of something, with the intention of making it known to the public in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System*".[8]

However, the EIT Law itself does not specifically address *cyberbullying*. The EIT Law does regulate defamation and libel through electronic media, but the definition of acts that constitute *cyberbullying* is still not detailed. In the EIT Law, the element of "*in public*" is not explicitly mentioned, but is interpreted as inherent in the element of

[5] Kitab Undang-Undang Hukum Pidana (KUHP), Article 310.
[6] M. Yusuf dan R.R. Mulyadi, "Law Enforcement on Social Media Abuse for Bullying in the Perspective of the Electronic Information and Transaction Law and Islamic Criminal Law." *Wasatiyah: Law Journal* 4, no. 2 (2023). https://doi.org/10.70338/wasatiyah.v4i2.141
[7] Jennifer Angelina, Elfrida Ratnawati, Dhany Rahmawan, Novina Sri Indirahati, dan Simona Bustani, "Review of Defamation Cases Based on the Criminal Code with Legal Certainty." *Ensiklopedia of Journal* 7, no. 2 (2025). https://doi.org/10.57235/jalakotek.v2i1.4648
[8] Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions, Article 27A.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

"*distributing, transmitting, or making electronic information accessible*". This means that any act of sending, uploading, or disseminating content electronically is legally considered to have been done "*in public*", because electronic systems are open and potentially accessible to the public. However, in the context of NGL.Link, the element of "*dissemination of electronic information*" in Article 27A of the EIT Law is also debatable, because the NGL system is closed and personal, there is no public access to messages, and there is no publication as referred to in the element of electronic defamation. This has led to a debate between those who say that the element of "*dissemination*" is fulfilled because sending messages through an electronic system is still considered "*distributing*" or "*transmitting*" electronic data, as this act uses digital media to send information even if it is only received by one person. However, there is also an opinion that the element of "*dissemination*" is not fulfilled because there is no publication to the general public, but rather closed communication between the sender and the recipient.

Based on the above explanation, the application of these two articles creates a legal gap, particularly in proving the element of "*in public*" in Article 310 of the Criminal Code and the element of "distributing/transmitting" in Article 27A of the EIT Law. Although the provisions of Article 310 of the Criminal Code and Article 27A of the EIT Law regulate defamation and insult through electronic media, their application in practice still leaves significant legal issues, particularly in the context of *cyberbullying* through anonymous messaging applications such as NGL.Link. The characteristics of communication that are closed, personal, and anonymous raise doubts about the fulfillment of the element of "*in public*" as referred to in Article 310 of the Criminal Code, as well as the element of "*distributing/transmitting*" in Article 27A of the EIT Law. This condition shows the tension between the construction of conventional criminal law norms and the reality of rapidly developing digital communication technology.

A number of previous studies have examined *cyberbullying* crimes using the approach of Article 310 of the Criminal Code and Article 27A of the EIT Law, including research by Haulah Nu'ma Salsabila Sholihah entitled "*Cyberbullying Crimes on the TikTok Platform Based on Article 27A of the 2024 EIT Law concerning the Second Amendment to Law -Law Number 11 of 2008 concerning EIT*", as well as an article by Ayu Indah Poncowati entitled "*Criminal Liability for Perpetrators of Cyberbullying: A Review of the Criminal Code and EIT Law in Indonesian Positive Law*". Unlike these studies, this research offers something new by focusing on the phenomenon of *cyberbullying* through the *anonymous* messaging app NGL.Link, which has the characteristics of closed *(one-to-one)* and anonymity-based communication.

The anonymity system in *anonymous* messaging applications complicates the process of proving the identity of perpetrators, thereby directly impacting the

P-ISSN: 2715-7202
E-ISSN: 2715-9418

application of criminal sanctions and criminal liability for *cyberbullying* perpetrators. The ambiguity in interpreting the elements of the offense and the mechanism of criminal liability raises its own set of problems in fulfilling the elements of the offense of defamation, and has the potential to create legal uncertainty and inconsistency in law enforcement in *cyberbullying* cases. Therefore, a comprehensive legal study is needed to analyze the application of criminal elements and the application of criminal sanctions against cyberbullies through *anonymous* messaging applications (NGL.Link) based on Article 310 of the Criminal Code in conjunction with Article 27A of the EIT Law, in order to provide legal certainty and clarity in the enforcement of criminal law.

RESEARCH METHODS

A normative legal method was used in this study, which highlights an in-depth analysis of various legal aspects, including legal rules, laws, regulations, and court decisions.[9] Through this approach, the author seeks to analyze the extent to which the application of Article 310 of the Criminal Code in conjunction with Article 27A of Law No. 1 of 2024 concerning EIT has been effective, consistent, and reflective of the principle of legal certainty in its interpretation and application. The legal materials used consist of primary legal materials, namely legislation (such as Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning EIT and Article 310 of the Criminal Code), secondary legal materials, namely the results of direct interviews with legal experts, and tertiary legal materials, books, journals, legal articles, and data taken from online media and used as reference materials related to the research. The data analysis technique uses a descriptive analytical method to interpret legal norms, theories, and research results to find the suitability of the application of articles to the phenomena being studied.

DISCUSSION

Application of Criminal Elements in *Cyberbullying* Offenses Committed Through Anonymous Messaging Applications (NGL.Link)

The legal provisions that most closely resemble the basis for analyzing cyberbullying committed through *anonymous* messaging applications, such as that experienced by a female student with the initials MR, are the articles governing defamation or libel. This is because the substance of the act relates to an attack on the victim's honor and reputation. Defamation is regulated in the Criminal Code and also in the Information and Electronic Transactions Law. In the Criminal Code, it is regulated

[9] Dr. Jonaedi Efendi, S.H.I., M.H, dan Prof. Dr. Johnny Ibrahim, S.H., S.E., M.M., *Legal Research Methods: Normative and Empirical*. (Depok: Prenadamedia Group, 2016), p. 132.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

in Chapter XVI on Defamation, contained in Articles 310 to 321 of the Criminal Code. The main rule is in Article 310 of the Criminal Code, which states:

(1) "Anyone who intentionally attacks the honor or reputation of another person by making an accusation verbally, with the clear intention of making it known to the public, shall be punished for defamation with a maximum imprisonment of nine months or a maximum fine of four thousand five hundred rupiah.
(2) If this is done in writing or through images that are broadcast, displayed, or posted in public, then it is punishable as written defamation with a maximum imprisonment of 1 year and 4 months or a maximum fine of Rp 4.5 million.
(3) Neither slander nor libel shall exist as far as the principal obviously has acted in the general interest or for a necessary defence."

Article 310 of the Criminal Code essentially contains several elements of a crime that must be fulfilled, namely:

1) **Anyone,** the word "anyone" means that the perpetrator includes all people. The legal subject of the criminal act of defamation is general and not limited to certain groups. This element includes every person as a legal subject capable of acting, both Indonesian citizens and foreign nationals, as long as the act is committed within Indonesian jurisdiction or has legal consequences in Indonesia.
2) **Intentionally,** shows that there was intent *(opzet)* on the part of the perpetrator in committing defamation. For example, when writing the tweet, it was indeed intended to make the recipient feel sad, offended, and the like. Moeljatno argues that intent has two main aspects, namely the will *(willens)* to commit the act and knowledge *(wetens)* of the consequences of the act. The perpetrator does not have to explicitly intend to damage the victim's honor or reputation, but it is sufficient if the perpetrator knows and realizes that their actions have the potential to cause such consequences.
3) **Attacking someone's honor or reputation,** related to the protection of a person's personal dignity. An act is considered to be an attack on honor or reputation if the statement made can demean the dignity of the victim or lower the public's opinion of them. Defamation does not have to be conveyed in the form of harsh insults, but can take the form of sarcasm or derogatory statements that substantially damage the victim's image and dignity. Therefore, the assessment of this element is not only based on the form of

P-ISSN: 2715-7202
E-ISSN: 2715-9418

language used, but also on the impact and meaning of the statement on the victim's honor.

4) **By accusing someone of something,** this element indicates that defamation must be carried out through accusations of a specific act, circumstance, or characteristic directed at the victim. The accusation does not have to be a fact that is objectively proven to be untrue, but rather it is sufficient if the accusation has the potential to cause a negative perception of the victim in the eyes of others.
5) **With the intention of making it known to the public,** emphasizes the perpetrator's intention or desire for the accusation to be known to the general public. This element requires publicity, meaning that the statement or accusation is conveyed in a space that allows people other than the victim to know the content of the accusation. Thus, this element is fulfilled if the statement is conveyed in a public place, through print media, or other means that allow many people to know about it.[10]

Based on an analysis of the elements of Article 310 of the Criminal Code in relation to the characteristics of communication on the *anonymous* messaging app NGL.Link, it can be concluded that the acts of *cyberbullying* that occurred did not fully meet the elements of the criminal offense of defamation. The elements of *"anyone"* and *"intentionally"* can basically be fulfilled because the perpetrator is a legally competent subject who consciously sends messages that are insulting in nature, while substantively the content of the message can also be classified as an act that attacks the honor or reputation of the victim and contains elements of accusation against something. However, the element of *"with the intention of making it known to the public"* is not fulfilled because the NGL.Link communication system is closed, personal, and one-to-one, so that messages can only be accessed by the recipient without publication or access by third parties or the general public. The failure to fulfill the element of publicity means that cyberbullying through NGL.Link cannot be classified as a criminal act of defamation under Article 310 of the Criminal Code.

However, when examined using Article 315 of the Criminal Code concerning minor defamation, the characteristics of *cyberbullying* through the *anonymous* messaging application NGL.Link are indeed closer to the construction of the offense regulated in that article. Article 315 of the Criminal Code does not require the element of *"public knowledge"* or publicity as stipulated in Article 310 of the Criminal Code, but is sufficient

[10] R. Soesilo, *Criminal Code (KUHP) and Complete Commentary on Each Article*. (Bogor: Politeia, 2016). p. 226-229.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

if the insult is made directly to the victim, either verbally or in writing.[11] In the context of NGL.Link, messages with insulting content are conveyed personally and directly to the victim through electronic means, thereby substantially fulfilling the elements of minor defamation as referred to in Article 315 of the Criminal Code.

Although Article 315 of the Criminal Code can normatively be used as an alternative in prosecuting *cyberbullying* through anonymous messaging applications, its application still faces serious obstacles, especially in proving the identity of the perpetrator due to the anonymity system inherent in digital platforms. Furthermore, the nature of Article 315 of the Criminal Code as a complaint-based offense with relatively light criminal penalties and its formulation based on the context of conventional defamation demonstrates its limitations in addressing the complexity of crimes in the digital space. This condition confirms that the use of Article 315 of the Criminal Code is only a temporary solution and is not yet ideal. This actually confirms the existence of a legal gap in cyber criminal law, because acts that occur in the digital space are ultimately forced into conventional crime formulations that have not been designed for the context of information technology.

Meanwhile, Article 27A of Law Number 1 of 2024 concerning Electronic Information and Transactions reads as follows:

> "Any person who intentionally attacks the honor or reputation of another person by accusing them of something, with the intention of making it known to the public in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System."

Article 27A of the EIT Law requires the fulfillment of several elements of a crime, namely:

1) **Any person,** referring to Article 1 point 21 of the EIT Law, it states, "A person is an individual, whether an Indonesian citizen, a foreign citizen, or a legal entity." Thus, the element of *"any person"* indicates a broad and unlimited scope of legal subjects. In the context of criminal acts committed through electronic media, the element of "*any person*" is not only understood physically as an individual, but also includes the digital identity attached to a person, such as social media accounts or accounts on internet-based applications. These accounts are considered to be the legal representation of the perpetrator behind them, so that any act committed through a social media account or messaging application can still be classified as an act of a

[11] Eparius Laia, "Application of Article 315 of the Criminal Code to Perpetrators of Minor Defamation (Study of Decision Number 33/Pid.C/2022/PN Pdg)." *Ekasakti Legal Science Journal* 1, no. 3 (2024). https://doi.org/10.60034/5y0kp121

P-ISSN: 2715-7202
E-ISSN: 2715-9418

legal subject as long as it can be proven that there was control and intent on the part of the person operating it. Thus, any individual who has the capacity to act and uses electronic means, including digital media and internet-based applications, can be held legally responsible if they fulfill the elements of a criminal offense.

2) **Intentionally,** intent is understood as the perpetrator's will and knowledge of their actions and the consequences thereof. Moeljatno explains that intent *(opzet)* contains two main elements, namely the will to commit the act and the awareness or knowledge of the consequences of the act..[12] In the context of Article 27A of the EIT Law, the element of intent does not necessarily mean that the perpetrator explicitly desires the legal consequences to occur, but rather it is sufficient if the perpetrator knows and realizes that their actions have the potential to attack the honor or reputation of another party. This is in line with the doctrine of dolus eventualis, which is a form of intent where the perpetrator is aware of the possibility of prohibited consequences arising, but still carries out the act.[13] Thus, someone who consciously sends messages that are insulting or demeaning to the victim through electronic media, including *anonymous* messaging applications, can be considered to have fulfilled the element of *"intentionally"*, even if the perpetrator argues that their actions were merely a joke or did not intend to cause harm.
3) **Attacks the honor or reputation of another person by accusing them of something,** honor *(eer)* relates to a person's self-esteem, while reputation *(goede naam)* relates to society's assessment of a person's dignity and reputation.[14] The element of attacking honor or reputation can be fulfilled if the electronic information conveyed contains accusations that are insulting, degrading, or stigmatizing to the victim, either explicitly or implicitly. Insults do not have to be conveyed in the form of rude words or curses, but can also take the form of sarcasm, insinuations, or disparaging statements that substantially diminish the victim's dignity. Thus, acts that attack honor or reputation are acts that can demean the victim's personal dignity or lower society's opinion of them. Furthermore, the phrase *"by accusing someone of something"* indicates that defamation or libel must be carried out through accusations of a particular act, circumstance, or characteristic that is demeaning and directed at the victim. The accusation does not have to be a

[12] E.Y. Kanter, S.H., dan S.R. Sianturi, *Op.cit.* p. 166.
[13] Prof. Sudarto, S.H, *Criminal Law I Revised Edition.* (Semarang: Yayasan Sudarto, 2018). p. 89-91.
[14] R. Soesilo, *Op.cit.*, p. 226.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

statement of fact that is proven to be untrue, but rather a statement that has the potential to create a negative perception of the victim in the eyes of others.

4) **With the intention of making it known to the public in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System,** this element requires that the act of defamation or libel be intended for public knowledge through the use of electronic information or electronic documents that are processed, sent, or disseminated through electronic systems. Based on Article 1 points 1 and 4 of the EIT Law, electronic information and/or electronic documents include any electronic data or records, including images, sounds, text, or other forms, which can be viewed, displayed, or heard through electronic devices.[15] However, the element of "*with the intention of making it known to the public*" cannot be automatically interpreted as fulfilled simply because the act was carried out through an electronic system. This is because this element is often associated with the act of "*distributing, transmitting, or making electronic information accessible*", which conceptually has the potential for open access. However, this potential must be assessed concretely based on the characteristics of the electronic system used, whether it is open *(public)* or closed *(private)*.

Based on an analysis of the elements of Article 27A of the EIT Law and in relation to the characteristics of the communication system in the anonymous messaging application NGL. Link, it can be concluded that the elements of "*every person*" and "*intentionally*" can in principle be fulfilled because the perpetrator is a legal subject capable of acting and consciously uses electronic means to send messages that are insulting in nature, while in substance the content of the message can also be qualified as an act that attacks honor or reputation by accusing someone of something. However, the crucial element in Article 27A of the EIT Law, namely "*with the intention that it be made public in the form of Electronic Information and/or Electronic Documents*", is not fulfilled because the NGL.Link communication mechanism is closed, personal, and only accessible to the recipient of the message, without any process of distribution, transmission, or creation of access for the public or third parties. The absence of the elements of publicity and public accessibility means that *cyberbullying* through NGL.Link cannot be classified as an electronic defamation offense under Article 27A of the EIT Law.

[15] Law Number 11 of 2008 Concerning Electronic Information and Transactions, Article 1 Number 1 and Number 4.

P-ISSN: 2715-7202
E-ISSN: 2715-9418

Thus, from the analysis of the elements of Article 310 of the Criminal Code and Article 27A of the EIT Law, it can be understood that the fulfillment of the elements of the offense is greatly influenced by the characteristics of the media used. Although *cyberbullying* substantially fulfills the element of attacking honor or reputation, the applicability of the element *"with the intention of making it known to the public"* cannot be separated from the nature of the electronic communication system used, whether it is open or closed. The element of publicity remains a requirement for fulfilling the elements of both articles.

According to Mrs. Aini Lathifah Nazhara, S.H., a prosecutor at the Bandung District Attorney's Office, the use of Article 310 of the Criminal Code in *cyberbullying* cases through *anonymous* messaging applications such as NGL.Link cannot be applied because the nature of the act is electronic and private. She explained that the element of *"public knowledge"* as implied in Article 310 of the Criminal Code is not fulfilled because messages sent through NGL.Link can only be accessed by the recipient and are not disseminated to the general public. Furthermore, Ms. Aini explained that Article 27A of the Electronic Information and Transactions Law (EIT Law) also cannot be applied in the context of the NGL.Link application because the element of *"dissemination of electronic information"* is not fulfilled. The NGL.Link system is *one-to-one* and can only be received by one party, namely the message recipient, and the message is not published, cannot be accessed by other users, and is also not intended for public consumption, thus preventing the distribution or transmission of information to the public. Thus, this element emphasizes that the mere use of an electronic system is not sufficient to prove the intention of publicity, but rather the intention to disseminate to the public must be proven. Therefore, neither Article 310 of the Criminal Code nor Article 27A of the EIT Law fulfill the elements of a crime to prosecute perpetrators of cyberbullying through such *anonymous* messaging applications.

In line with these findings, interviews with Dr. Ahmad Jamaludin, S.H., M.H., a legal practitioner and academic, show that normatively, the application of Article 27A of the EIT Law requires the element of *"dissemination"* or *"transmission"* that can be accessed by other parties. If the insult is made personally and privately, then the elements of Article 27A of the EIT Law are not fulfilled. However, according to him, in certain contexts, personal insults can still be analyzed using Article 310 of the Criminal Code, as long as the elements of attacking a person's honor or dignity can be proven. Nevertheless, Mr. Jamal also emphasized that both the old and new Criminal Codes are still unable to effectively address *cyberbullying* through anonymous messaging applications such as NGL.Link. The element of *"public knowledge"* remains a key

P-ISSN: 2715-7202
E-ISSN: 2715-9418

requirement in defamation cases, so that cases that are private and closed tend not to fulfill the elements of the offense.

From the perspective of criminal theory *(delic)*, this legal vacuum is evident in the absence of the objective elements of a crime, even though *cyberbullying* has substantially attacked the honor and dignity of the victim. Criminal offense theory asserts that all elements of a criminal offense must be cumulatively fulfilled, and failure to prove even one element, particularly the element of publicity, means that the act cannot be classified as a criminal offense. This shows that the construction of defamation offenses, which is still oriented towards the concept of conventional public space, is not yet fully adaptive to the reality of digital space, which is private and *anonymous*, thus creating a legal loophole in the handling of *cyberbullying*.

In line with this, the legal loophole leads to a legal vacuum in the regulation and enforcement of *cyberbullying* crimes committed through *anonymous* messaging applications such as NGL.Link. The element of *"in public"* in Article 310 of the Criminal Code and the element of *"dissemination of electronic information"* in Article 27A of the EIT Law require public access, while on NGL.Link messages are only received by one party without publication. The incompatibility between legal norms and the characteristics of digital media creates legal uncertainty for both victims and law enforcement officials. Although Article 310 of the Criminal Code and Article 27A of Law Number 1 of 2024 concerning Electronic Information and Transactions regulate defamation and libel, both provisions are still oriented towards the concept of open publicity. Existing criminal norms do not explicitly accommodate closed and *anonymous* forms of electronic communication that enable *cyberbullying* without publication to the general public.

Application of Criminal Sanctions Against Perpetrators of *Cyberbullying* Through Anonymous Messaging Applications Based on Article 310 of the Criminal Code in Conjunction with Article 27A of the Electronic Information and Transactions Law

In the context of *cyberbullying* carried out through *anonymous* messaging applications, the characteristics of the NGL.Link communication system, which is closed, personal, and based on anonymity, raise serious issues in the application of criminal sanctions. The closed and personal nature of the NGL.Link communication system makes it difficult to prove the element of *"in public"* in Article 310 of the Criminal Code and the element of *"dissemination of electronic information"* in Article 27A of the EIT Law. As a result, acts that substantially fulfill the elements of attacking a person's honor and dignity cannot be classified as criminal acts, so that the perpetrator cannot be held criminally liable, even though the victim suffers real psychological and social losses. This ultimately creates legal uncertainty for victims, due to the absence of a clear legal basis

P-ISSN: 2715-7202
E-ISSN: 2715-9418

for prosecuting perpetrators criminally. On the other hand, law enforcement officials also face normative limitations in determining the appropriate article to apply, which has the potential to cause inconsistencies in the handling of cyberbullying cases through private and *anonymous* digital media.

The issue becomes even more complex when linked to the principle of *geen straf zonder schuld*, which is a fundamental principle in criminal law. This principle emphasizes that a person can only be punished if it is proven that they have committed an act that is prohibited by law and that the act was committed with fault *(schuld)*, either in the form of intent *(dolus)* or negligence *(culpa)*.[16] In line with this view, Moeljatno also emphasized that a person cannot be convicted if there is no evidence of wrongdoing on the part of the perpetrator, because criminal punishment can only be imposed for acts that constitute a criminal offense and are committed with culpable fault.[17] Roeslan Saleh also argued that criminal liability requires an intrinsic connection between the perpetrator and the act, so that without fault, punishment cannot be legally justified.[18]

In cases of *cyberbullying* through anonymous messaging applications, the principle of *geen straf zonder schuld* (no punishment without guilt) highlights the limitations of positive criminal law. The absence of the elements of a crime in Article 310 of the Criminal Code and Article 27A of the Electronic Information and Transactions Law means that no criminal act has been committed in legal terms, so the perpetrator's guilt cannot be further assessed. The difficulty of proving the element of *"in public"* in Article 310 of the Criminal Code and the element of *"dissemination of electronic information"* in Article 27A of the EIT Law means that the perpetrator's actions cannot be formally classified as a criminal offense. When the elements of the offense are not fulfilled, then legally there is no criminal act that can be attributed to the perpetrator, so that criminal liability is dropped. This shows that the principle of *geen straf zonder schuld* cannot be separated from the fulfillment of the elements of the offense as a whole, because guilt can only be assessed if a criminal act has been proven first. Furthermore, the anonymity of perpetrators on the NGL.Link application makes it difficult to prove the identity and intent of the perpetrator, which are important parts of the element of fault *(schuld)*.

According to Sudarto, criminal liability can only be imposed on perpetrators who can be proven to have committed a criminal act with a certain level of awareness and

[16] Ahda Muttaqin, Elmina A. Herysta, Faisal, dan Pratama Putra Sadewa. "Analysis of the Principle of No Punishment Without Guilt in Criminal Liability for Fraud Through Mystical Rituals." *University of Bengkulu Law Journal* 8, no. 1 (2023).
[17] Dr. Agus Rusianto, S.H., *Criminal Acts & Criminal Liability: A Critical Review Through Consistency Between Principles, Theory, and Application*. (Jakarta: Kencana, 2016), p. 20.
[18] *Ibid.*

P-ISSN: 2715-7202
E-ISSN: 2715-9418

intent.[19] If the identity and intent of the perpetrator cannot be proven, then criminal sanctions cannot be imposed even though the act is morally and socially reprehensible.[20] This situation indicates that the application of criminal sanctions against perpetrators of *cyberbullying* through *anonymous* messaging applications has not been effective. Criminal law, which is still oriented towards the conventional concepts of publicity and information disclosure, has not been able to fully cover forms of electronic communication that are closed and *anonymous*. As a result, the function of criminal law as a means of protecting society and exercising social control has been weakened, potentially leading to impunity for cyberbullies.

In addition, in the context of *anonymous* identities in applications such as NGL.Link, a digital forensics approach is needed to bridge the limitations of proving criminal elements and criminal liability. Although the NGL.Link system is designed based on anonymity and closed *(one-to-one)* communication, this anonymity is not absolute because every activity in an electronic system essentially leaves a digital trace. These traces include IP addresses, access logs, message metadata, delivery times, and device information, which can be technically analyzed to identify the parties controlling *anonymous* accounts. The provisions in Article 43 paragraph 5 letter i of Law Number 19 of 2016 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions form the normative basis and provide scope for investigators to request and obtain electronic data from Electronic System Operators, including platforms whose servers are located outside the territory of Indonesia.[21]

In the context of foreign platforms not based in Indonesia, such as NGL.Link, the Indonesian National Police (POLRI) can submit a Law Enforcement Request or official request to service providers (such as technology companies, social media, internet service providers/ISPs, or institutions) through the *Mutual Legal Assistance* (MLA) mechanism to obtain data, information, or take certain actions in the context of law enforcement.[22] Therefore, requests for data such as IP addresses and account information can be submitted as long as such actions have legal consequences in Indonesia.

Thus, the issue of *cyberbullying* through *anonymous* messaging applications not only highlights the limitations of criminal norms oriented towards publicity, but also emphasizes the importance of integrating the interpretation of cyber criminal law with

[19] Lulu Salsabila dan Alfian Azhari, *"Criminal Liability". JUSTITIA: Journal of Justice, Law Studies, and Politic* 1, no. 01 (2025).
[20] Sudarto, *Op. Cit*, p. 88.
[21] Muhammad Singgih Imam Wibowo, "Technical and Legal Obstacles in the Investigation of Cybercrimes in Indonesia." *Rewang Rencang: Lex Generalis Law Journal* 5, no. 7 (2024).
[22] Andrew Moniaga, Max Sepang, dan Harly Stanly Muaja. "Investigation to Reveal Electronic Information and Electronic Transaction Crimes." *Lex Administratum* 11, no. 2 (2023).

P-ISSN: 2715-7202
E-ISSN: 2715-9418

digital forensics capabilities. This approach shows that the effectiveness of law enforcement against *cyberbullying* does not solely depend on regulatory updates, but also on the optimization of investigators' authority and the professional and proportional use of electronic evidence technology, so that the application of criminal sanctions continues to guarantee legal certainty, justice for victims, and the effectiveness of criminal accountability in the digital age.

CONCLUSION

Based on the results of the study, it was concluded that the application of Article 310 of the Criminal Code in conjunction with Article 27A of Law Number 1 of 2024 concerning Electronic Information and Transactions against perpetrators of *cyberbullying* through the *anonymous* messaging application NGL.Link cannot yet be effectively implemented. This is due to the characteristics of the NGL.Link communication system, which is closed, personal, and *anonymous*, making it difficult to fulfill the element of "*in public*" in Article 310 of the Criminal Code and the element of "*distributing and/or transmitting*" in Article 27A of the EIT Law. Although *cyberbullying* substantially attacks the honor and reputation of the victim, legally speaking, such acts do not always fulfill the elements of a crime as required by applicable criminal provisions.

In addition, the application of criminal sanctions against perpetrators of *cyberbullying* through *anonymous* messaging applications also faces serious obstacles in terms of criminal liability. The principle of *geen straf zonder schuld* emphasizes that criminal punishment can only be imposed if the criminal act and the perpetrator's guilt can be legally proven. In the context of *anonymous* applications such as NGL.Link, the absence of the elements of a crime means that criminal liability cannot be imposed, so no criminal sanctions can be imposed on the perpetrator. This condition has implications for the weakening of the function of criminal law as a means of legal protection for victims and social control over perpetrators.

Thus, this study shows that there is a legal vacuum and inconsistency between the construction of criminal law norms that are still oriented towards the concept of conventional publicity and the reality of digital communication, which is private and *anonymous*. The problem of *cyberbullying* through *anonymous* messaging applications not only highlights the limitations of criminal norms, but also emphasizes the importance of optimizing the authority of investigators and the professional and proportional use of digital forensics. Therefore, it is necessary to update and interpret cyber criminal law in a manner that is more adaptive to developments in information technology, particularly in accommodating forms of *cyberbullying* through closed electronic communication systems. The integration of the interpretation of cyber criminal law and the technical

P-ISSN: 2715-7202
E-ISSN: 2715-9418

capabilities of electronic evidence is also key to ensuring legal certainty, justice for victims, and the effectiveness of criminal law enforcement in the digital age.

REFERENCES

Books

Dr. Agus Rusianto, S.H., M.H. *Tindak Pidana & Pertanggungjawaban Pidana: Tinjauan Kritis Melalui Konsistensi Antara Asas, Teori, Dan Penerapannya*. Jakarta: Kencana, 2016.

Dr. Jonaedi Efendi, S.H.I., M.H, dan Prof. Dr. Johnny Ibrahim, S.H., S.E., M.M., M.Hum. *Penelitian Hukum: Normatif Dan Empiris*. Depok: Prenadamedia Group, 2016.

E.Y. Kanter, S.H., dan S.R. Sianturi, S.H. *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya.* Jakarta: Storia Grafika, 2012.

Prof. Sudarto, S.H. *Hukum Pidana I Edisi Revisi*. Semarang: Yayasan Sudarto, 2018.

R. Soesilo. *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*. Bogor: Politeia, 2016.

Journals

Ahda Muttaqin, Elmina A. Herysta, Faisal, dan Pratama Putra Sadewa. "Analysis of the Principle of No Punishment Without Guilt in Criminal Liability for Fraud Through Mystical Rituals." *University of Bengkulu Law Journal* 8, no. 1 (2023).

Andrew Moniaga, Max Sepang, dan Harly Stanly Muaja. "Investigations to Uncover Electronic Information and Electronic Transaction Crimes." *Lex Administratum* 11, no. 2 (2023).

Ayu Indah Poncowati, Laura Ayu Azzahra, dan Putra Adhi Pratama. "Criminal Liability for Perpetrators of Cyberbullying: A Review of the Criminal Code and Electronic Information and Transactions Law in Indonesian Positive Law." *Causa: Jurnal Hukum Dan Kewarganegaraan* 14, no. 10 (2025).

Eparius Laia. "Application of Article 315 of the Criminal Code to Perpetrators of Minor Defamation (Study of Decision Number 33/Pid.C/2022/PN Pdg)." *Ekasakti Legal Science Journal* 1, no. 3 (2024). https://doi.org/10.60034/5y0kp121

Hatarto Pakpahan. "Criminal Law Aspects of Cyberbullying on Social Media." *Jurnal Cakrawala Hukum* 11, no. 3 (2020). https://doi.org/10.26905/idjch.v11i3.5718

Jennifer Angelina, Elfrida Ratnawati, Dhany Rahmawan, Novina Sri Indirahati, Simona Bustani. "Review of Defamation Cases Based on the Criminal Code with Legal Certainty." *Ensiklopedia of Journal* 7, no. 2 (2025). https://doi.org/10.57235/jalakotek.v2i1.4648

P-ISSN: 2715-7202
E-ISSN: 2715-9418

Lulu Salsabila dan Alfian Azhari. "Criminal Liability." *JUSTITIA: Journal of Justice, Law Studies, and Politic* 1, no. 01 (2025).

M. Yusuf dan R.R. Mulyadi. "Law Enforcement on Social Media Abuse for Bullying in the Perspective of the Electronic Information and Transaction Law and Islamic Criminal Law." *Wasatiyah: Jurnal Hukum* 4, no. 2 (2023). https://doi.org/10.70338/wasatiyah.v4i2.141

Muhammad Singgih Imam Wibowo, Akhmad Munawar dan Hidayatullah. "Technical and Legal Obstacles in the Investigation of Cybercrimes in Indonesia." *Rewang Rencang: Jurnal Hukum Lex Generalis* 5, no. 7 (2024).

Saut B. Siregar, Mahmud Ekaputra, dan Windi Trisna. "Imposition of Criminal Sanctions Against Perpetrators of Cyberbullying Based on Law Number 19 of 2016 Concerning Electronic Information and Transactions (Study of Decision Number 3745/Pid.Sus/2019/PN-Mdn)." *Jurnal Media Pencerahan Bangsa* 3, no. 2 (2019).

Legislations

Kitab Undang-Undang Hukum Pidana (KUHP).

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 11 of 2008 on Electronic Information and Transactions.

Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions.

Other Sources

Haulah Nu'ma Salsabila Sholihah. "Cyberbullying Crimes on the TikTok Platform Based on Article 27A of the 2024 ITE Law Concerning the Second Amendment to Law Number 11 of 2008." Faculty of Sharia & Law, Univesity Islam Negeri Sunan Gunung Djati Bandung, 2025. https://digilib.uinsgd.ac.id/110580/.

Ministry of Women's Empowerment and Child Protection. "Press Release Number B-219/SETMEN/HM.02.04/7/2024 Regarding the Protection of Women and Children in the Digital Space," 2024. https://www.kemenpppa.go.id/index.php/siaran-pers/gandeng-sejumlah-pihak-kemen-pppa-dorong-aksi-bersama-lindungi-perempuan-dan-anak-dari-kekerasan-di-ranah-daring.

Salisa Rizky Permata. "Reasons for Using the NGL App – Anonymous Q&A." Faculty of Social and Political Science University of Lampung, 2023. https://digilib.unila.ac.id/74347/.

We Are Social. "Special Report Digital 2025 Indonesia," 2025. https://wearesocial.com/id/blog/2025/02/digital-2025/.