

# Cyberbullying Crime Evidence System

Ratna Indayatun<sup>1</sup>, Evita Isretno Israhadi<sup>2</sup>  
{ratna.indayatun@gmail.com<sup>1</sup>, evita\_isretno@borobudur.ac.id<sup>2</sup>}

Universitas Borobudur, Jakarta, Indonesia<sup>1,2</sup>

**Abstract.** The purpose of this paper is to present how the system for proving cyberbullying has been done. Through a normative juridical approach, by utilizing literature studies to collect the data, and descriptive analysis as an analytical tool. It was found that the evidentiary system for cyberbullying was still based on the Criminal Procedure Code and Law Number 11 of 2008. Decisions regarding evidence, evidence, and electronic data are the authority of the judge.

**Keywords:** Children; Cyberbullying; Criminal; Evidence

## 1 Introduction

The internet makes originally conventional crimes, such as threats, theft, and hoax can now be carried out using online computer media with a minuscule risk of being caught by individuals and groups with higher losses for both the community and the country. In addition to creating new crimes accompanied by the development of internet technology, this can also be a means for various kinds of crimes through the internet network. Therefore, in computer crimes, it is possible to have formal offenses and material offenses. The legal offense referred to in the internet crime is the deed of someone entering someone else's computer without permission, while the substantial violation is an act that causes harm to other people.

The use of social and digital media is an integral part of everyday life. It found that 98 percent of users are teenagers and children. The impact of the high use of social media has led to increased crime targeting users in cyberspace. Crimes that often occur today in cyberspace are cyberbullying, that a form of intimidation by one or more people to corner, corner, and discredit others through the cyber world. This intimidation is not arbitrary as a result, not infrequently death is the end of cyberbullying.[1] The characteristics of cross-border activities in the digital world that are presently not expose to regional limits and conventional laws require responsive law since explicit articles in the Criminal Code were thought of as inadequate to answer legitimate issues that emerge regardless of exercises in the digital world. Articles in the Criminal Code applicable to cyberbullying are Article 310 and Article 311 of the Criminal Code and in light of Law Number 11 of 2008 concerning Information and Electronic Transactions Article 27 section (3).

Cyberbullying is another sort of wrongdoing when seen from the media utilized, in particular electronic media. This phenomenon requires special attention from law enforcers because of the increasingly massive interaction in the cyber world. The phenomenon of cyberbullying in Indonesian law is included in the definition of defamation or humiliation where the description is inadequate when viewed forms of cyberbullying that are more than

just defamation. In addition, the incomplete definition of cyberbullying can cause journalistic activities, which are guarantees of the right to freedom to disseminate opinions to the public, which can also be considered defamation for those who feel that their reputation has been defamed. Based on the description above, this paper wants to present the system of proof of *cyberbullying*.

## 2 Method

This paper uses a qualitative approach with normative juridical research methods.[2] Data were collected by studying literature originating from legislation, books, and literature related to the research topic. The collected data is then analyzed using descriptive analysis.[3]

## 3 Discussion

The act of bullying that had known at first was an act that intimidated someone weak by doing it directly using physical or verbal contact. However, the rapid development of information and communication technology causes someone to do bullying no longer directly, but by using information and communication technology facilities through applications that can be downloaded via smartphones such as Twitter, Instagram, Facebook, WhatsApp, and others. Bullying in cyberspace or often called Cyber has been prevalent in the past two years. Bullying is an action carried out by another person continuously or repeatedly. This action frequently leaves the victim physically and mentally helpless. Meanwhile, Willard, Director of the Center for Safe and Responsible Internet Use in America, defines it "as an act of defamation, content, discrimination, information content or content of a privacy nature with the intent to embarrass or can also be interpreted as an offensive comment, openly frankly explained." [4]

Apart from the word cyber, the term *bullying* is carried out in situations where there is a desire to hurt, make someone feel depressed and afraid, traumatized, depressed, and helpless. In summary, there are three forms of bullying, including first physical bullying, bullying, hitting, and kicking. Second, bullying in verbal form is hurting in speech, such as mocking, berating, gossiping, cursing, and yelling. Third, in psychical types such as ostracizing, intimidating, suppressing, discriminating, and ignoring. [5]

Bullying (Indonesia: Penindasan) is the utilization of power, dangers, or pressure to manhandle or scare others. This conduct can become constant and include an irregularity of social or actual power. It can incorporate verbal provocation or dangers, actual brutality or intimidation, and over and over coordinated against a particular casualty, maybe dependent on race, religion, sex, sexuality, or capacity. There are four kinds of mistreatment, specifically enthusiastic, physical, verbal, and digital. A harsh culture can grow anyplace as long as there is an association between individuals, beginning in schools, work environments, families, and the climate.[6]

As explained in Article 183 of the Criminal Procedure Code, it explicitly figured that "An adjudicator may not force a sentence on an individual except if with no less than two substantial bits of proof he acquires the conviction that a criminal demonstration has happened and that the respondent is at legitimate fault for carrying out it." [7] Thus, in Indonesian criminal procedural law expressly provides legality that in addition to being based on the element of judge's belief, proof with at least two valid pieces of evidence is very necessary to

support the component of error in criminal law to determine whether someone is proven to have committed a crime or no.

The practice that develops is that the modus operandi of crimes in the field of Cyber Crime is not only carried out with sophisticated tools, but this crime is complicated to determine quickly and simply who is the perpetrator of the crime when the legal instruments in criminal law enforcement still have many limitations. It can be felt that if the crime committed by law enforcement officers is not ready or even unable (technological stutter) to investigate the perpetrators of cyberbullying or because this crime was committed by involving various actors from a country, each country has its legal sovereignty.

This legal phenomenon in efforts to overcome cyberbullying also appears to have obstacles, particularly when it is associated with the evidentiary system according to Indonesian criminal law, because as in Article 184 of the Criminal Procedure Code, which means of evidence legally cannot be applied as a basis for proof only if the crime has intended in the context of a crime. "Cyber Crimes" clearly the evidence does not match (not classified) the formulation of evidence as required according to the Criminal Procedure Code. Thus, it is appropriate that the system of proof and evidence as in the Criminal Procedure Code needs to be improved or updated following the legal reality that is developing at this time, especially concerning cyberbullying.

As for Law Number 19 of 2016, Amendments to Law Number 11 of 2008 on Information and Electronic Transactions related to cyberbullying crimes only regulated regarding defamation/insult, defamation/spreading false news,[7] spreading hatred and enmity are stipulated in Chapter VII regarding prohibited acts, namely:

- a. Article 27 paragraph (1) reads: "Every person intentionally and without rights distributes nor transmits nor makes accessible Electronic Information nor Electronic Documents that have contents that violate decency."
- b. Article 27 Paragraph (3) reads: "Every person intentionally and without rights distributes nor transmits nor makes accessible Electronic Information nor Electronic Documents that contain insults nor defamation."
- c. Article 27 Paragraph (4) reads: "Every person intentionally and without rights distributes nor transmits nor makes accessible Electronic Information nor Electronic Documents containing extortion nor threats."
- d. Article 29 reads: "Every person intentionally and without rights sends Electronic Information nor Electronic Documents containing threats of violence or intimidation aimed at personally."

The criminal provisions of the articles above regarding cyberbullying are regulated in Chapter XI of Criminal Provisions in Law Number 19 of 2016 Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions that are: [7]

- a. Article 45 Paragraph (1) peruses: "Each and every individual who deliberately and without privileges appropriates nor sends nor makes available Electronic Information or Electronic Documents containing the substance as alluded to in Article 27 section (1) will be rebuffed with detainment for a limit of 6 (six) a long time nor a greatest fine of Rp. 1,000,000,000.00 (one billion rupiah).
- b. Article 45 Paragraph (3) peruses: "Each and every individual who deliberately and without privileges appropriates nor sends nor makes available Electronic Information nor Electronic Documents containing the substance as alluded to in Article 27 section (3) will be rebuffed with detainment for a limit of 4 (four) a long time nor a greatest fine of Rp. 750,000,000.00 (700 and fifty million rupiahs) (the arrangement alluded to in this section is a grievance offense).

- c. Article 45 section (4) peruses: "each and every individual who intentionally and without privileges circulates nor communicates nor makes open Electronic Information or Electronic Documents containing the substance as alluded to in Article 27 (4) will be rebuffed with detainment a limit of 6 (six) a long time nor a greatest fine of Rp. 1,000,000,000.00 (one billion rupiah)."
- d. Article 45 B, peruses: "Each and every individual who deliberately and without privileges sends Electronic Information nor Electronic records containing dangers of brutality or terrorizing that are shown especially as alluded to in Article 29 will be rebuffed with detainment for a limit of 4 (four) a long time. ) a long time nor a most extreme fine of Rp. 750,000,000.00 (700 and fifty million rupiah)."."

Other regulations contained in the Draft Draft Law on the Criminal Code 2000, where this concept changed from 2008, have regulated electronic evidence, namely: In Book I (General Provisions), Provisions on evidence are made [1]:

- a. The definition of "goods" (Article 174/178) includes intangible objects in the form of data and computer programs, telephone or telecommunications services, or computer services.
- b. The definition of "key" (Article 178/182) includes a secret code, a computer entry key, a magnetic card, a signal that has been programmed to open something.

The key referred to in the article is a password or key to enter into an existing system or virtual space. The definition of "entry" according to Agus Raharjo here is to enter the global information network system called the internet and then enter a site or website which includes servers and computers, included in site management. So there are two meanings of entry, namely ingoing the internet and entering the Site.[8] The description of "telephone network" (Article 191/195) includes computer networks or computer communication systems.

With the increase in electronic activity, proof that can be utilized legitimately should likewise incorporate data or electronic reports to work with the applying law. Likewise, the printout of the archive or data should likewise be lawfully legitimate. To work with the execution of the utilization of electronic proof (either in electronic structure or on paper), electronic proof can allude as an augmentation of evidence.

Based on Article 28 of Law Number 8 of 2011 concerning Information and Electronic Transactions [9] :

- a. Everyone deliberately and without privileges gets out bogus and deluding word that outcomes in shopper misfortunes in Electronic Transactions.
- b. Everyone deliberately and without privileges scatters data pointed toward making contempt or aggression explicit people nor local gatherings dependent on nationality, religion, race, and between bunch (SARA).

Based on Article 29 of Law Number 8 of 2011 concerning Information and Electronic Transactions [9] :

- a. Everyone purposefully and without freedoms sends Electronic Information nor Electronic Documents that contain dangers of savagery or terrorizing focused on actually. The utilization of Article 27 can't be isolated from Article 45 section (1) of the ITE Law which peruses:
- b. Everyone who satisfies the components as alluded to in Article 27 passage (1), section (2), passage (3), or passage (4) will be condemned to a most extreme detainment of 6 (six) a long time nor a greatest fine of Rp. 1,000,000. .000,00 (one billion rupiah).

Thus, Indonesian criminal procedural law expressly provides legality that in addition to being based on the element of judge's belief, proof with at least two valid pieces of evidence is very necessary to support the component of error in criminal law to determine whether someone is proven to have committed a crime or no. Then the practice developed, that the

modus operandi of offense in the field of Cyber Crime is not only carried out with sophisticated tools, but this crime is complicated to determine quickly and simply who is the perpetrator of the crime when the legal instruments in criminal law enforcement still have many limitations. It can be felt if the crime committed by law enforcement officers is not ready or even unable (technological stutter) to investigate the perpetrators of cyberbullying or because this crime was committed by involving various actors from a country, each country has its legal sovereignty.

This legal phenomenon in efforts to overcome cyberbullying also appears to have obstacles, particularly when it is associated with the evidentiary system according to Indonesian criminal law, because as in Article 184 of the Criminal Procedure Code, which means of evidence legally cannot be applied as a basis for proof if the crime is committed in the context of a crime. "Cyber Crimes" clearly the evidence does not match (not classified) the formulation of evidence as required according to the Criminal Procedure Code. Thus, it is appropriate that the system of proof and evidence as in the Criminal Procedure Code needs to be improved or updated following the legal reality that is developing at this time, especially concerning cyberbullying.

#### 4 Conclusion

Guideline of the Crime of Cyberbullying, under the watchful eye of the order of Law Number 11 of 2008 concerning Information and Electronic Transactions, there were a few legal arrangements identifying with the utilization and abuse of data innovation directed in the Criminal Code and a few laws outside the Criminal Code. Nonetheless, the definition strategy for the wrongdoing of Cyberbullying, both as far as criminalization, kinds of criminal assents, detailing of criminal approvals, subjects, and capabilities of criminal deeds is unique and as of not long ago has not been managed expressly and plainly against the wrongdoing. The system of proof against criminal acts, Cyberbullying, which is still according to the Criminal Procedure Code, legally does not regulate provisions regarding evidence and electronic data, is contrary to the provisions of Law Number 11 of 2008 that has acknowledged, evidence-based on evidence and electronic data. However, considering the legal system in Indonesia in terms of evidence, a judge is given the authority to decide a case even though the provisions are still unclear.

#### References

- [1] S. Kalo, "Kebijakan Kriminal Penanggulangan Cyber Bullying Terhadap Anak Sebagai Korban [*Cyber Bullying Criminal Policy Against Children as Victims*]," *USU Law J.*, vol. 5, no. 2, p. 34, 2017.
- [2] M. H. Dr. johnny ibrahim,SH., *Teori & Metodologi Penelitian Hukum Normatif [Normative Legal Research Theory & Methodology]*. 2006.
- [3] I. M. P. Diantha, "Normative Legal Research Methodology," *Teor. Metodol. Penelit. a.*, 2017.
- [4] Student Reports of Bullying, "Results From the 2001 School Crime Supplement to the National Crime Victimization Survey, US National Center for Education Statistics & Cambridgeshire.gov.uk." Cambridge University Press, USA, 2001.
- [5] Sartana and N. Afriyeni, "Perilaku Perundungan Maya (Cyberbullying) Pada Remaja

Awal [*Cyberbullying Behavior in Early Adolescents*],” *Insight J. Psikol.*, vol. 1, no. 1, 2017.

- [6] A. S. Sudarwanto, “Cyberbullying Kejahatan Dunia Maya yang ‘Terlupakan’ (Wacana Kritis Cyber Crimedi Negara Berkembang) [*Cyberbullying ‘Forgotten’ Cyber Crime (Critical Discourse on Cyber Crime in Developing Countries)*].,” *J. Huk. Pro Justitia*, vol. 27, no. 1, 2009.
- [7] “ Law Number 19 of 2016 Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.” .
- [8] A. Raharjo, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi [Cyber Crime Understanding and Prevention of Technological Crime]*. Bandung: PT Citra Aditya Bakti, 2002.
- [9] “ Law Number 8 of 2011 concerning Information and Electronic Transactions.” .