

# Indonesian Cyber Law from Verdict No. 1152/Pid.Sus/2020/PN.Tjk: Review of Indonesian Cyber Law

**Kusbianto<sup>1\*</sup> Azmiati, Z<sup>2</sup>.Andi, M<sup>3</sup>. and Andrian<sup>4</sup>**

*<sup>1,2,3,4</sup>Department of Law., Faculty of Law. Universitas Dharmawangsa Medan, Indonesia*  
[kusbianto\\_yanto@yahoo.co.id](mailto:kusbianto_yanto@yahoo.co.id) (Kusbianto)

## **Abstract**

Using a Normative Research Method of Law that focuses on the prevailing legal norms and the study of legal norms, this study aims to gather the data of cyber crimes in Indonesia. This research was carried out as a result of the increase in cyberspace activities due to the COVID-19 pandemic that hit the world in 2020. The lock down was initially resisted and fought against, however, as months went by, people began to adjust to this new lifestyle of social distancing and now they can easily operate and even speak out their minds from their various homes. This procedure was carried out by examining secondary data and making comparisons of law with regulations and other legal theories. Theoretically speaking, cyber laws were formulated to anticipate cyber crimes. Data collection was related to the Criminal Code which regulates the attack on the honor or the defamation of character of a person, and parallelizes to the contents of the electronic media used as evidence in acts of insult and defamation. Consequently, Indonesian law on Electronic Information and Transaction 2016, in article 27 paragraphs (3), needs to be immediately revised in order to interpret the law in accordance with the principles of legality, predictability, and transparency.

*Keywords: Human Rights, insult, private message, cyber crimes*

## **INTRODUCTION**

The lock down that was enforced due to the Covid-19 pandemic brought different reactions in its wake as people began to show various forms of intolerance. However, they often try to cover it up with excuses of reacting to humiliation and defamation, which are often seen as rubber articles. The virtual world came to the rescue by making it easy for them to have all forms of communication and exchange of information in everyday life. This move brought about an increase in Cyber crimes of all sorts and issues like insults and defamation of character were not left out. Insult and defamation are criminal acts that cannot be separated. The Criminal Code in Chapter XVI Book II with the title insult (beleediging) regulates several rules regarding defamation. The Criminal Code did not regulate a detailed explanation of defamation.

One important factor in the articles of defamation and / or defamation that is regulated in the Criminal Code is that there are elements that can be widely known. If Article 27 paragraph (3) of the ITE Law follows its new explanation which refers to the provisions stipulated in the Criminal Code, this element should also apply to the application of the article.

## **Definition of Evidence and Types of Evidence**

Evidence is an act carried out in an effort to ensure the search for and defend the truth, whether by judges, public prosecutors, defendants, or legal advisors, all of which are bound by procedural law as well as an assessment of the validity of evidence based on positive regulations in Indonesia.

Evidence is the core location of case examination at court proceedings. Evidence is a provision that contains guidelines and procedures regulated in legislation to prove or explain whether or not a criminal event has occurred. The theory of evidence that is generally adopted in the criminal justice system, including Indonesia, is known as negative *wettelijkbewijstheorie*. This is the basis for proving a judge's conviction that arises from negative evidence in law. The basis for this evidence is expressly stated in Article 183 of the Criminal Code: "A judge may not impose a sentence on a person unless with at least two valid pieces of evidence to show that he is convinced that a criminal act actually occurred and that the defendant is guilty of committing it" (Eddy, 2012).

Evidence in the criminal procedure law is regulated in Article 141 of the Criminal Procedure Code, namely: witness statements, expert statements, letters, instructions, and statements of defendants. The proving process in cyber crime cases is basically not different from proof in conventional criminal cases, but in cyber crime cases there are several things that are electronic in nature, which are the main things used as proof, including the existence of electronic information or electronic documents, legal provisions regarding the evidence of cyber crime cases. Regulated in Article 5 paragraph (1) and paragraph (2) Law Number 19 of 2016, which states that electronic information and / or documents are considered as valid evidence in the process of proving cyber crime cases and electronic evidence is also considered an extension of evidence enforced in the criminal procedural law in Indonesia, in this case the evidence contained in Article 184 of the Criminal Procedure Code (Hamdi & Suhaimi, 2013).

## **Definition of Electronic Evidence and Types of Electronic Evidence**

Material arrangements regarding electronic evidence have been regulated in several special laws such as Law No. 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering; however the formal rules do not yet exist, although in practice judges in deciding cases of money laundering have paid attention to the existence of this electronic evidence. Technological developments, which are often misused and which have become the media and means used in the crime of money laundering, need serious handling, including in the case of the proof. Multiple interpretations resulting from the meaning of elements can be accessed, displayed, guaranteed, and their integrities can be accounted for based on Article 6 of Law Number 19 of 2016 concerning Electronic Information and Transactions can affect the judge's conviction in assessing the validity of an electronic evidence instrument.

According to O.C. Kaligis, there is no positive law in Indonesia that regulates in detail; comprehensively and uniformly regarding the validity of electronic evidence which can guarantee its integrity, thus causing disagreements in the trial process from expert statements regarding the guarantee of the integrity of electronic evidence (Kaligis, 2012). This is because the evidence really determines the guilt or innocence of a person.

Electronic evidence is evidence obtained from a crime using technological equipment to direct a

criminal event in the form of electronic data both inside the technology device itself, for example on a computer, hard disk / floppy disk, memory card, sim card or that is the result of a print out, or has undergone processing through a certain technological device such as a computer or in other forms in the form of a path from an activity using technology (Kartika, 2019).

Judge Mohammed Chawki of the Computer Crime Research Center classified electronic evidence into three categories, as follows:

### 1. Real Evidence

Real Evidence or Physical Evidence is evidence consisting of tangible / tangible objects that can be seen and touched. "Real evidence is also direct evidence in the form of automatic recordings generated by the computer itself by running software and receipts from information obtained from other devices, for example computer log files (Kartika, 2019).

Edmon Makarim presents electronic evidence as a valid and stand-alone evidence, of course, guarantees must be given that a data recording is carried out in accordance with applicable procedures (calibrated and programmed) in such a way that the print out results of a data can be accepted in proving a case.

### 2. Testamentary Evidence

Testamentary Evidence is also known as Hearsay Evidence, while testimony from witnesses and expert witness is information from an expert that can be given during the trial, based on individual experiences and observations. "The role of expert testimony is in accordance with our laws and regulations, namely Law no. 8 of 1981 Criminal Code. The expert's statement is considered as evidence that has the power of proof if the information given is based on specific expertise in his / her field and in the form of information "according to his knowledge" purely "(Harahap, 2012). The position of an expert in clarifying criminal acts that occur and in explaining or explaining electronic evidence is very important in giving judges the confidence to decide cases of cyber crime.

### 3. Circumstantial Evidence

This is detailed evidence obtained based on utterances or observations of actual events that encourage someone to support a conclusion, but not to prove it. Circumstantial evidence or derived evidence is a combination of real evidence and hearsay evidence"(Kartika, 2019).

Until now, there are several laws that partially regulate the existence of electronic evidence (Kartika, 2019), namely:

1. Law Number 8 of 1997 Concerning Company Documents, from Article 12 of Law no. 8/1997, which states that company documents can be transferred to microfilm, and in the next article it is stated that the new company documents have the power as evidence after the transfer process is carried out which is then followed by the legalization process. Only after this process will the company documents be declared as valid evidence.
2. Law Number 2 of 2001 concerning Amendments to Law Number 31 of 1999 concerning Eradication of Corruption Crimes. Based on the Criminal Procedure Code, evidence of evidence can only be obtained from the testimony of witnesses, letters and statements of the

defendant. However, according to Law no. 20 of 2001, evidence of guidance can also be obtained from other evidence in the form of information uttered, sent, received, or stored electronically by means of an optical device or something similar but not limited to electronic data interchange, electronic mail(e-mail), telegram, telex, facsimile, and from documents, namely any recorded data or information that can be issued with or without the assistance of a facility, whether it is written on paper, any physical object other than paper, or that is recorded electronically, which in the form of writings, sounds, pictures, maps, designs, photographs, letters, signs, numbers, or perforations that have meaning.

3. Law No.15 of 2003 concerning the Stipulation of Government Regulation in Lieu of Law Number 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism. The Article of the Terrorism Law regulates that evidence for investigating criminal acts of terrorism includes, among other things, other evidence in the form of information uttered, sent, received, or stored electronically with an optical device or something similar to this.
4. Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons. In Article 29 of the Law on the Eradication of the Crime of Trafficking in Persons, the regulation regarding electronic evidence is clearer than the previous law. However, it has not yet reached the increasingly diverse development of electronic evidence.
5. Law Number 8 of 2010 concerning Money Laundering. Law Number 8 of 2010 concerning Money Laundering also regulates electronic evidence; this can be seen in Article 73. In this Law, the law of proof is not only used as evidence specified in the Criminal Procedure Code. Also, the use of electronic evidence is permitted, so that electronic evidence can exist. The law only states that it is permissible to use, namely other evidence in the form of information uttered, sent, received, or stored electronically by means of an optical device or the like. This regulation has not yet been able to accommodate electronic evidence.
6. Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Electronic Information and Transactions. With the promulgation of Law Number 19 of 2016 concerning Electronic Information and Transactions, we can provide a basis for the use of electronic evidence, with the existence of this ITE Law, electronic evidence can become valid evidence which is an extension of the Criminal Procedure Code, so that electronic evidence is valid in Justice. The electronic evidence is regulated in Article 5 of the Law of Electronic Information and Transactions (ITE). Article 5 relates to electronic documents as valid legal evidence in court. The new ITE Law follows a Constitutional Court decision which states that electronic documents obtained through wiretapping (interception) without court permission are invalid as evidence.

In previous case that involved Syamsul Arifin who is chairman of AKLI (Asosiasi Kontraktor Listrik dan Mekanikal Indonesia) 2009-2013. He was reported by Napoli Situmorang with SMS contains the following text:

“Lu sama tololnya dg Maulidin, Lu nggak bisa memahami putusan pengadilan & SK DPP AKLI

yang konsiderannya Putusan Inkracht ya?

Lu tolol Napoli, musdalub AKLI itu harus diselenggarakan oleh DPD-AKLI yang syah dan Peserta

Musdalub AKLI harus Anggota AKLI..

Lu tolol Napoli, Pemberhentian Ketum DPD-AKLI harus melalui musdalub yang syah bukan dengan SK Bodong dari DPD-AKLI apalagi dr oknum mantan Ku & Sekjen DPP-AKLI..

Lu tolol Napoli, pembekuan DPD-AKLI tidak dikenal di AD-ART AKLI..

Lu goblok Napoli, pemulihan Anggota AKLI tdk bisa dilakukan DPP-AKLI apalagi oleh oknum mantan KU & Sekjen DPP-AKLI krn berhak menerima atau menolak anggota AKLI itu DPDP-AKLI

Lu idiot Napoli, mauludin cs yang tolol itu menggugat DPD-AKLI yang memecat mrk, lu tolol Napoli, dg gugatan tsb berarti dan tidak terbukti mrk mengakui sdh dipecat oleh AKLI..

Lu bodoh Napoli, putusan PNTK yang inkracht itu adalah Hukum dg Hirarki tertinggi.

Ngomong apa lu Napoli tolol dg reporter..

Sarjana Tolol lu!!

Baca dulu AD-ART AKLI, pahami dulu”

To which roughly translate as:

“You are the same stupid Mauludin, You can’t comprehend law verdict from court & SK DPP AKLI

which consider as Putusan Inkracht huh?

Napoli you are stupid, musdalub AKLI must be held by legitimate DPD-AKLI and the attendee of Musdalub AKLI must be a member of AKLI..

You idiot Napoli, the dismissal of the chairman of the DPD-AKLI must go through a valid Musdalub not by a Bodong (Not legitimate) SK from DPD-AKLI especially from my former personnel & Secretary General of DPP-AKLI..

You idiot Napoli, DPD-AKLI pembekuan (freeze) is not recognized in AKLI's AD-ART..

You are an idiot Napoli, the recovery of AKLI members cannot be done by DPP-AKLI especially by my former personnel & Secretary General of DPP-AKLI because the right to accept or reject AKLI members is on DPDP-AKLI

You dumb Napoli, mauludin (and associate) that dumb sue DPD-AKLI that fired them, you dumb

Napoli, with the sue had it means and it is not proven they acknowledge that they are fired by AKLI..

You are stupid Napoli, verdict of PNTK that inkracht are the highest Law Hierarchy.

What even did you say to the reporter Dumb Napoli..

Dumb Scholar!!

Read AD-ART AKLI first, understand it first”

The report document show that Syamsul Arifin was reported of insult and defamation which the police force of Lampung processed by following the assumption of Pasal 27 ayat (3) jo. Pasal 45 ayat (1)

UU ITE dan/atau Pasal 310 KUHP. By the end of it, Syamsul Arifin was charged with alternative charges, having committed a criminal act: First, Article 27 paragraph (3) jo. Article 45 paragraph (1) of the ITE Law; or Second, Article 310 paragraph (2) of the Criminal Code; or Third, Article 335 paragraph (1) of the Criminal Code.

The existence of Article 27 paragraph (3) of the Electronic Information and Transactions (ITE) Law, whose essence and detailed meaning is still being debated, has the potential to clog information channels, and create a generation that is weak and easily offended. This situation unconsciously creates a condition where there is competition and everyone is competing over who can be offended first.

This becomes a more complex problem when the degree of distraction between individuals is reasonably varied and no standardized unit can be applied to it. It is fitting that if you want to fight for freedom of opinion like what has been fought for in the 1998 era, then all parties must be prepared to face the consequences that will come with it, namely the right to be offended.

### **Research purposes**

The purpose of this research is to examine how legal arrangements for criminal acts of defamation are carried out through electronic messages in cyber law.

### **Research methods**

This study used a Case study method followed by Normative Research Method of Law that focuses on analyzing a defined problem consisting in a real situation and uses real information as methodical tool with the prevailing legal norms and the study of legal norms as references. This procedure was carried out by examining the case of Syamsul Arifin with secondary data and making comparisons of law with regulations and other legal theories. Data analysis was carried out qualitatively with a prescriptive model, which is to provide arguments for the results of the research that has been carried out, to provide prescriptive (assessment) about right or wrong or what should be according to the law regarding the facts or events of the research results.

## DISCUSSION

In Syamsul Arifin case there are several law that are used as charge, first is Pasal 27 ayat (3) UU ITE, to which formulation shown that there are several important elements that can be see more carefully and attached to Article 310/311 of KUHP.

In the Criminal Code, insult is regulated in Chapter XVI starting from Article 310 to Article 321. Meanwhile, in the Draft Criminal Code; the offense for insult is regulated in Chapter XIX, starting from Article 540 to Article 550. The offense regulated in both of them does not have a significant difference. The similarities that they have are that they contain almost the same prohibited acts, namely: an offense against defamation, an offense for slander and false suspicion as well as an offense for a person who has died. Various offenses can be made verbally while other offenses can be made in writing. Insult and / or defamation is explicitly regulated in Article 310 paragraph (1) of the Criminal Code where the formulation of the article contains several important elements, namely (<https://business-law.binus.ac.id>):

- a. Intentionally
- b. Attacking the honor or defamation of character of others
- c. Accused of committing a certain act, and
- d. With a real intention so that it is known by the public.

(Diskusinya lebih baik pada analisa kasus Siber yang sdh masuk ranah hukum)

If we refer to the elements of Article 310 above, defamation can be interpreted as a material offense. Material offense is an offense that can be punished if prohibited consequences have arisen. Insult and / or defamation does not have a specific definition by the Criminal Code but defamation itself comes from the word "*cemar*" which according to the Big Indonesian Dictionary (KBBI) is defined as tarnished, dirty, or despicable. Pollution is defined as the act of polluting or defiling. Honor is defined as good character or self-respect. The meaning given by KBBI is clear that an act of defamation means a series of actions that cause damage to one's self-esteem, dirty one's dignity or defames one's character, and those actions are committed against the law or against ethics.

This defamation offense should not be immediately punishable if the prohibited effect cannot be proven in court, the result can be in the form of material loss or non-material loss and the type of loss must be assessed or measured. The loss must also be proven as a result of an act of defamation. Other aspects that also need to be proven are "attack" and "honor". These two elements become difficult to prove because attack does not necessarily mean to attack with weapons, but with words. However, the words that are used are difficult to measure, because they could be criticisms or complaints or words that contain truth. Therefore, it is difficult to distinguish between attacking, criticizing and complaining.

In order to make it easier to interpret the offense of insulting and / or defamation as regulated in Article 310, several criminal law scientists, including E. Utrecht van Bemmelen, Moeljatno, ToeslanSaleh and AdamiChazawi, provided various interpretations that were summarized in table 1 as follows:

Table1.

*The Definition of the Elements of Article 310 Criminal Code*

No.	The Content of the Article 310 Criminal Code	The Definition
1.	Intentionally	"Intentionally" is the first element of error and the second element of error is in the word "with intention". The "deliberate" mental attitude refers to action attacking people's honor or defamation of character (deeds and objects of action).
2.	Attacking honor or people's defamation of character	The act of attacking (aanranden), is not physical, because what is being attacked (the object) is not physical but a feeling of respect and feelings about people's defamation of character. The objects that are attacked are a sense or feeling of self-worth regarding respect (eer), and a sense or feeling of self-worth regarding people's defamation of character (goedennaam).
3.	Accusing a certain action	By using words or sentences through speech, by accusing a certain action. So what the maker accuses must be an act certain, and not other things, for example, referring to someone with disrespectful words, such as stupid, lazy, dog and so on.
4.	Public Knowledge	The mental attitude "intent" refers to the "public knowledge" element of what action the person is accused of.

The article 310 paragraph (2) has the addition content of writing or picture which has been shown to the public. The content can be summarized as follows:

Table 2.

*The Definition of Elements of Article 310 paragraph (2) Criminal Code*

No.	The Content	The Definition
1.	Writing or Picture	<p>Writing is the result of writing either by hand or by any means of equipment in the form of a series of words or sentences in any language whose contents contain certain meanings, or attacking the honor and defamation of character of a person on a paper or other object which is writable in nature, for example: paper, boards, fabrics and more.</p> <p>Drawings or paintings are imitations of objects made by hand scribbling through writing tools such as pencils, brushes and paints, with any tools on paper or other objects that can be drawn or written in nature. This image should contain a meaning that defames the character or honor of a certain person (the addressee).</p>
2.	Broadcast, Shown and Affixed	<p>Broadcast (verspreiden), the meaning is that the writing or image is made in large enough numbers, which can be printed or reproduced, then distributed in any way. For example, being traded, sent to various parties, or distributed to anyone (public). Therefore, verspreiden can also be translated as spreading. The method of disseminating so many writings or pictures to the general public has been the intent of the spreader so that the contents of the writing or the meaning in the broadcast images, which are insulting in nature, are known to the public.</p> <p>To be shown (ten toongesteld) is to show writings or pictures whose content or meaning is offensive to the public, so that the public will know about it. Shown can happen in person at the time of showing in general to a lot of people, but it can also be indirect. For example, placing an insulting banner on a highway, done at night when no one can see when it was placed.</p> <p>Affixed (aanslag), refers to a writing or image, that is attached to other objects that can be affixed, for example boards, building walls, trees and so on.</p>

Insult in the Criminal Code can be classified into 5 types, namely insulting, slander, minor insults, slander complaints and false suspicions. However, if we look at the application of cases of insults and / or defamation committed through electronic media, they often link articles 310 and 311 of the

Criminal Code (Komarudin, 2016). In Indonesia, the term “defamation offense” is not a judicial term (legal term) because it is not explicitly stated in the Criminal Code, but it is a term that has developed in the academic world (academic term) and in the society (social term).

The Decision of the Constitutional Court Number 50 / PUU-VI / 2008 strengthens the link between the ITE Law and Articles 310 and 311 of the Criminal Code where item 3.17 of the decision stated that the interpretation of the norms contained in Article 27 paragraph (3) of the ITE Law regarding insulting and / or defamation of people’s character, cannot be separated from the criminal law norms contained in Chapter XVI concerning Defamation as contained in Article 310 and Article 311 of the Criminal Code. According to ICJR senior researcher AnggaraSuwahju quoted by gresnews.com, an SMS (private message via other electronic media) sent to a person does not qualify in public as one of the important conditions in the crime of humiliation. In line with the Court's decision Article 27 paragraph 3 of the ITE Law must be read in line with Article 310 of the Criminal Code and Article 311 of the Criminal Code.

Acts of insulting and / or defamation in the ITE Law do not get a special classification but are unified when compared to the Criminal Code which classifies insults into 5 types. In further regulation in Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) especially in Article 27 paragraph (3), these acts refer to:

"Anyone who knowingly and without right distributes and / or transmits and / or causes to be accessible Electronic Information and / or Electronic Documents that have content of defamation and / or defamation".

The link between the ITE Law and the Criminal Code was strengthened again in Law no.19 of 2016 concerning Electronic Information and Transactions (ITE), which does not change the contents of Article 27 but adds changes to the explanation of paragraph (1), paragraph (3), and paragraph (4) especially in paragraph (3) where it stated that:

"The provisions in this paragraph refer to the provisions of defamation and / or slander which are regulated in the Criminal Code (KUHP)".

The last ITE Law also adds several definitions or basic interpretations of the elements of Article 27 paragraph (3), which are contained in the amendment to the explanation of Article 27 a yat (1), paragraph (3) and paragraph (4), and are shown in table 3 as follows:

Table 3.

*The Definition of the Elements of Article 27 Paragraph (3) Electronic Information and Transactions Law*

No.	The Content of the Article	The Definition based on the Law of Electronic Information and Transactions
1.	Intentionally and without Rights	<p>“Intentionally” is the first element of error and the second element of error is in the word “with intention”. The mental attitude “deliberately” refers to the act of attacking the honor or defamation of character of a person (actions and objects of action).</p> <p>“Without rights” means being carried out against the rights or against the provisions of the prevailing laws and regulations.</p>
2.	Distributing, Transmitting and Making it accessible	<p>Distributing means sending and / or distributing Electronic Information and / or Electronic Documents to many people or various parties through Electronic Systems.</p> <p>Transmitting, means sending Electronic Information and / or Electronic Documents addressed to one other party through an Electronic System.</p> <p>Making it accessible means all actions other than distributing and transmitting through Electronic Systems that cause Electronic Information and / or Electronic Documents to be known by other parties or the public.</p>
3.	Electronic Information and / or Electronic Document	<p>Electronic Information, the meaning of which is one or a set of electronic data, including but not limited to writing, voice, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail), telegram, telex, telecopy or the like, processed letters, signs, numbers, Access Codes, symbols, or perforations which have meaning, or which can be understood by those who are able to understand them (Article 1 Point 1 of the ITE Law).</p> <p>Electronic Document, the meaning is any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or the like, which can be seen, displayed, and / or heard through a computer or electronic system, including but not limited to writing, sound, pictures, maps, designs, photographs or the like, letters, signs, numbers, access codes,</p>

		symbols or perforations that have meaning or can be understood by those who are able to understand them (Article 1 Point 4 of the ITE Law).
4.	Contain elements of criminal acts of insulting and / or defamation	There are contents that contain elements of criminal acts of insulting and / or defamation, the provisions of which refer to the provisions of defamation and / or slander regulated in the Criminal Code.

Apart from the debate about Article 27 paragraph (3) it is a formal or material offense because there is no clear and firm regulation on it. Democratic requirements are the basis for legality to determine whether or not there is an act of defamation or insult. Democratic requirements do not allow or justify the existence of punishment for statements that are not spoken or written in public, so that "private correspondence" or "private conversation" is not allowed to be the subject or object of punishment.

Apart from democratic requirements, it is necessary to understand that there are requirements for publicity. This is because the offense of defamation / defamation will always be based on the element "with the intention to be known by the public", and the publication requirements in relation to the element "with the intention of being known by the public" are what can determine whether an act fulfills the formulation of the offense or whether it does not (Komarudin, 2016).

The constitutional basis which becomes the reference for the concept of protection of human rights in the judiciary in Indonesia is contained in the formulation of Article 28G paragraph (1) of the 1945 Constitution which contains the value of the right to privacy guaranteed in Article 12 UDHR and Article 17 ICCPR where this formulation becomes the constitutional basis for guaranteed right to privacy. Article 28G paragraph (1) of the 1945 Constitution stated that:

"Every person has the right to the protection of himself, his family, honor, dignity and property under his control, and the right to a sense of security and protection from the threat of fear to do or not do something which is a human right".

Again quoting the Constitutional Court Decision Number 50 / PUU-VI / 2008 concerning the Case Review of Law Number 11 of 2008 concerning Information and Electronic Transactions, the Constitutional Court provides a translation of Article 12 UDHR and Article 17 ICCPR. In this translation, the word "privacy" is translated as "personal affairs / personal problems" and it is stated as follows (<http://www.hukumonline.com>):

Article 12 UDHR:

*"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interferences or attacks"*.

Translation in Constitutional Courts Decision (<http://www.hukumonline.com>):

No one may be arbitrarily disturbed in his personal affairs, family, household, or correspondence, nor are others permitted to violate his honor and reputation. Everyone has the right to legal protection against disturbances or violations like this ". Article 17 ICCPR (<http://www.hukumonline.com>):

1. *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation"*.
2. *"Everyone has the right to the protection of the law against such interference or attacks"*.

Like the general character or nature of human rights that are not divided, interrelated and dependent on one another (indivisible, interrelated and interdependent), the right to privacy is closely related to the right to freedom of speech. The right to privacy and the right to free speech are mutually supportive. To provide protection of right to privacy means providing protection for the right to freedom of speech (Eoin, 2008).

For example, in a democratic society, it is important to maintain privacy in communication between people, the concern that there is monitoring of members of the public from irresponsible parties will result in the lack of freedom of opinion. This situation can result in voiceless constructive ideas in democratic life (Eoin, 2008). This means that the right to privacy guarantees protection from the threat of fear to do or not do something that is a human right.

In addition to mutually reinforcing linkages, the presence of the right to privacy must also be interpreted as a balancing of the right to freedom of opinion. The purpose of balancing is that the right to reputation which is part of the right to privacy must be the limit of the right to freedom of opinion. The concept of balancing is expressly stated in Article 28J paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that in exercising one's human rights, a person's human rights will be limited by the rights of others. Regarding the right to freedom of opinion, the right to the reputation of others becomes the limit for every citizen in exercising his right to express his opinion (Giri, 2011).

According to Indonesian Language Dictionary or KBBI's interpretation, the meaning is deeds done so as to cause defamation of character. Example: "Its reputation in the badminton arena is known worldwide". Reputation can also be defined as a picture of mind, which is a picture that is in someone's mind (<https://id.wikipedia.org>). According to Oxford Advanced Learner's Dictionary 1995, Reputation is the opinion that people in general have about what somebody or something is like. The translation is, reputation is what some people generally think about what or how a person is characterized. So it is clear that in determining whether an act is classified as a criminal act of humiliation and / or defamation, the act must be committed with the intention of being publicly known.

Following back to the Syamsul Arifin case it is also stated that similar case also have been decided by the Bantul District Court in case No 196/Pid.Sus/2016/PN.Btl which in essence the Judge handed down a waiver decision on the allegation insults committed by a defendant who is not proven to have committed insults by "intentional with intent or purpose" but according to the judge's intentional what the defendant did was intentional with the possibility of knowing (opzet bij mogelijkheidbewustzijn), in his consideration the Bantul District Court Judge stated that:

"Considering, that based on the description of the considerations, the Assembly is of the opinion that the actions

The defendant included intentional possibility (*opzet bij mogelijkheidbewustzijn*), namely the defendant posted a status on Facebook with the intention of expressing a complaint.

his rants and criticisms are likely to offend others and it turns out that status

has offended witness Diah Sarastuty alias Ayas, but the Assembly is of the opinion that the actions the defendant posted a status on facebook not containing insults, defamation or slander."

Above decision also help proven that in order to decide that Syamsul Arifin was caught under wrong article the more suitable article was Pasal 315 KUHP to which then it also need to be proven further more because "tolol" which is indeed a rude word but is not an accusation of an action.

Syamsul Arifin at 14 December 2020 was later decided to be innocent and set free after been through several process of suing that the case have been passed by 7 years but it is forced to be continued or repeated.

## CONCLUSIONS

Indonesia adheres to a *wettelijk* and negative proof system where in carrying out their obligations, judges can perform *rechtsvinding* which is limited by the principles and regulations of the law. Therefore, in deciding a case or making legal findings, Judges must read the law properly. The insult and / or defamation regulated in the ITE Law refers to the definition provided by the Criminal Code so that Article 27 paragraph (3) naturally inherits elements of Article 310 of the Criminal Code as the basis for the criteria for determining criminal acts of insult and / or defamation. Unfortunately, this arrangement is not explained in detail and firmly like the explanation in the explanation of Article 27 paragraph (1) of the ITE Law.

The protection of human rights in Indonesia is contained in the Indonesian constitution, the right to privacy, the right to freedom of expression, the right to freedom of opinion, and others are guaranteed by the constitution. Protection of human rights in Indonesia is guaranteed from the start of the investigation process to the final stage of court decisions. Judging from the democratic requirements that do not allow or justify the existence of punishment for statements that are not spoken or written in public, therefore "private correspondence" or "private conversation" is not allowed to be the subject or object of punishment and publicity requirements for acts of insult and / defamation. However, even when the action is being carried out with the intention to be made known to the public, it is still not fulfilled if the media is used only in private messages. Therefore, according to the authors' positive legal analysis in Indonesia, proving criminal acts of insult and / or defamation as proven by means of private message evidence with electronic media is illegal according to law and if left unchecked can result in weak mentality in the Indonesian society where people compete over who was first offended and who was not. Also, there are many available solutions in the application of communication via the electronic media.

## **SUGGESTIONS**

Based on the above conclusions, the researchers propose the following suggestions:

1. There needs to be a revision of the ITE Law Article 27 paragraph (3) along with an explanation so that the article is stated firmly and clearly and does not appear to be a "rubber article". This is important so that in the future there will be no more criminalization or abuse of these articles.
2. The community must be wiser in communicating and dealing with it. Efforts to respond to parties who disturb or offend in electronic media can be taken positively if it is in the form of criticism. But if it is dropped, efforts can be made to delete messages or delete conversations or even block or blacklist actions if it is deemed necessary. Democracy in its implementation and safeguards require existing people to have a strong mentality and to be flexible enough to overlook minor offences since it is difficult to distinguish between words that attack, criticize and complain.
3. In the context of handling criminal cases, the state must follow the guidelines for criminal law and the elements of the article of defamation and / or defamation where the state does not interfere in personal matters, except for exceptions that are expressly stated in the constitution and laws and regulations. The state of Indonesia as a rule of law should always maintain the meaning contained therein, where a state of law is "a legal system in which rules are clear, well understood, and fairly enforced" and follows the principles of legality, predictability and transparency.

## REFERENCES

- Eddy, O. (2012). *Theory & Law of Evidence*. Jakarta: Erlangga.
- Eoin C. (2008). The Concept of a Right to Privacy”, in Eoin Carolan, Hilary Delany (ed). *The Right to Privacy: A Doctrinal and Comparative Analysis* (pp. 25). Thompson Round Hall. England.
- Giri A. T. (2011). *Identifying the Traces of Particularity in Indonesia Freedom of Expression*. South East Asia Human Rights Conference.
- Hamdi, S., & Suhaimi, M. (2013). Electronic Evidence in a Criminal Evidence System. *Journal of Legal Studies*, 1(4), 53-58
- Harahap, M.Y. (2012). *Discussion of Problems and Application of KUHP: Court Trial Examination, Appeal, Cassation, and Review*. Jakarta: SinarGrafika.
- Kaligis, O.C. (2012). *Application of Law Number 11 of 2008 concerning Electronic Information and Transactions in Practice*. Jakarta: YarsifWatampone.
- Kartika, P. P. (2019). Electronic Data As Legal Evidence In Proving the Crime of Laundering Money. *Indonesian Journal of Criminal Law*, 1 (1), 33-46.
- Komarudin, A. (2016). *Reconsidering Article 27 paragraph (3) of the ITE Law in Court Decisions: Consideration of Court Decisions Related to the Use of Article 27 paragraph (3) of Law No. 11 of 2008 concerning Electronic Information and Transactions in Indonesia*. Jakarta: YarsifWatampone.
- Mansur, D.M.A. & Gultom, E. (2005). *Cyber Law-Law Aspect Information and Technology*. RefikaAditama, Bandung.