

THE EXISTENCE OF ELECTRONIC EVIDENCE IN VERIFICATION LAW SYSTEM IN INDONESIA FROM THE JUDGE'S PERSPECTIVE

Dedy Muchti Nugroho, SH, M.Hum
Prof., Dr., Setiono, SH., MS
Prof., Dr., Adi Sulistiyono, SH., MH
Sebelas Maret University

Abstract: To find out the verification of civil case and criminal case in Republic of Indonesia's Law No.11 of 2008 about Information and Electronic Transaction. Conclusions: (1) in civil case using electronic evidence, the evidence that is legitimate and can be revealed in the verification process is determined based on Article 5 clause (1) and (2) of Law Number 11 of 2008 about Information and Electronic Information confirming that information and or electronic document can be considered as a legitimate evidence in verification process particularly in civil case using electronic evidence, the evidence is the expansion of evidence as regulated and enacted in the civil case law corresponding to the provision of Article 1866 BW. (2) The verification of crime should ensure that the existing electronic document came from electronic system meeting the requirement based on the legislation and after the enactment of ITE Law, there is an addition of evidence and the recognition of electronic document as a legitimate evidence determining that electronic document or its print out is the legitimate evidence that can be used before the trial as long as the information contained within it can be accessed, displayed, and ensured for its completeness and accountable for thereby informing a condition. In addition, the position of electronic document is equalized to the document prepared on a piece of paper as mentioned in General Explanation of ITE Law.

A. Introduction

The crime in information technology sector or called cybercrime or computer-related crime occurs more widely in Indonesia. Cybercrime is human activity in the cyber space making computer target of crime (e.g. illegal access, site hacking, illegal interception) and human activity using computer as the target of crime (e.g. credit falsification, pornography via internet). The provision

of penal code governing the crime in information technology area is commonly called cybercrime law.

Many factors result in the increased number of cybercrimes in Indonesia including rudimentary provision of cybercrime law, law enforcer's less optimal ability of dealing with cybercrime and society's low awareness of cybercrime eradication.

One important factor making the cybercrime eradication failed in Indonesia is inadequate understanding on cybercrime, the types of cybercrime, the danger of cybercrime, punishment threat for the cybercrime perpetrator and cybercrime law enforcing mechanism. Adequate understanding on cybercrime will encourage everyone to choose any way to avoid cybercrime. The perfect understanding on cybercrime for will help the law enforcer deal with cybercrime repressively through applying the penal code in information technology sector.

Republic of Indonesia's Law Number 11 of 2008 about Information and Electronic Information began to be proposed to the Legislative Assembly (DPR RI) on May 17, 2006 and was ratified since its enactment date of April 21, 2008 consisting of 13 (thirteen) chapters and 54 (fifty four) articles so that in juridical view, the cybercrime case occurring should be trialed based on Information and Electronic Transaction Law as long as its crime elements met the provision of a crime as mentioned in the law, but in fact many cases that should be trialed based on Information and Electronic Transaction Law processed in criminal judicature based on the law other than Information and Electronic Transaction Law by the law enforcer.

Considering this phenomenon, there should be a research on the application of Information and Electronic Transaction Law to the verification of civil and criminal cases.

Verification, according to Subekti¹, is the attempt of convincing the judge concerning the actual law between the parties in the case. In this case, between evidences and the crime indicted. In constructing this legal relation, each party uses evidence to verify their proposition suggested. For that reason, the judge is reasonable to accept the parties' propositions (public prosecutor or the indicted) without limited by the use of evidence as long as the proposition meets the principles of logics.

B. Problem Statement

1. How is the Republic of Indonesia's Law Number 11 of 2008 about Information and Electronic Transaction applied to the verification of civil case?
2. How is the Republic of Indonesia's Law Number 11 of 2008 about Information and Electronic Transaction applied to the verification of criminal case?

C. Discussion

¹Subekti, *Hukum Pembuktian*, Jakarta : Pradnya Paramita, 1983, pp. 7-8.

1. The Legal Power of Electronic Evidence Based on Civil Procedural Law and Law Number 11 of 2008 about Information and Electronic Transaction

Speaking of electronically verification is inseparable from the electronic evidence itself. The electronically verification process is the one involving many things related to information technology such as information and or electronic document in civil case using electronic evidence being investigated based on the provision of verification as governed in the Civil Procedural Law and other Legislations such as Republic of Indonesia's Law Number 11 of 2008.

Electronically verifying process should be supported by a variety of electronic evidence as well, in this case by keeping considering the provision of legitimate evidence in Article 1866 BW. In the civil case using electronic evidence, the evidence mentioned in article 1866 BW is the legitimate evidence as long as it is obtained through lawful process. In civil case using electronic evidence, the legal evidence can be suggested in the verification process based on Article 5 clauses (1) and (2) of Law Number 11 of 2008 about Information and Electronic Transaction confirming that

information and or electronic document can be considered as legitimate evidence in the verification process particularly in civic case using electronic evidence. The evidence is the expansion of the one as governed and enacted in procedural law particularly civil procedural law, consistent with the provision of Article 1866 BW.

In the civil case using electronic evidence, the evidence used is the one produced and containing information technology. Information and or electronic document can be considered as electronic evidence. In addition to be determined as the expansion of evidence in the procedural law enacted based on the Article 5 clause (2) of Law Number 11 of 2008 about Information and Electronic Transaction, the evidence can be interpreted extensively so that the intended information or electronic document has the same legal power as the one in ordinary criminal case as governed in Article 1866 BW. The evidence in the form of information and or electronic document can be considered as a supposition as a legitimate evidence as governed in Article 1866 BW. It is because the supposition evidence is considered as

legitimate when it is obtained from the Judge's knowledge.

When information and or electronic document is considered as the letter evidence as governed in Article 1866 BW either directly or through extensive law interpretation, information and or electronic document is the supposition evidence, so that the validity of electronic evidence can be seen clearly and it can be proposed as the evidence in the process of verifying the civil case using electronic evidence, so that the verification process conducted in this civil case with electronic evidence has the same legal power as the one in ordinary criminal case as governed in Article 1866 BW *juncto* Article 5 clauses (1) and (2) Number 11 of 2008 about Information and Electronic Transaction.

Other evidences such as witness information and expert opinion are important evidence in the electronically verifying process in civil case using electronic evidence although it is not the product of or does not contain information technology element. The article 163 HIR of Indonesian civil procedural law mentions the principle of "*everyone proposing something should verify it*".

At a glance, this principle seems to be very easy but in practice it is very difficult to determine appropriately who should be imposed with an obligation to verify something. As the criterion, it can be suggested that not only one party is obliged to verify but also it should be considered the casuistically according to the concrete condition and the verification should be imposed to the less incriminated party.

Considering the provision of Article 1 number 1 of ITE Law, electronic transaction is defined as a lawful deed conducted by and using computer and/or other electronic media. In the attempt of conducting electronic transaction, the parties always uses electronic document as their foundation to make legal relations. Related to the presence of electronic transaction using electronic document, in ITE Law there is a principle determining that everyone stating the right, confirming the existing right or rejecting others' right (the similar principle existing in article 163 HIR *juncto* Article 1865 BW) based on the presence of electronic information and/or electronic document should ensure that electronic information and/or electronic

document existing derives from the electronic system complying with the precondition based on legislation.

The precondition determined in ITE Law is the one pertaining to the presence of electronic transaction and/or electronic document in which the subject or the system should be certified by:

Firstly, credibility certification institution that will undertake administrative function including registration and physical authentication on business performer, development and management of credibility certificate and preparing the suspended certificate list as determined in Article 10 of ITE Law.

Secondly, the organizer of electronic certification undertaking administrative function that may involve registration and physical authentication on the applicant, the development and management of public lock or private lock, the management of electronic certificate and suspended certificate list, as mentioned in Articles 13 and 14 of ITE Law.

2. The validity of Electronic Document Verification Based on ITE Law

In the enactment of ITE Law, there is a new regulation on electronic

document evidence. Considering the provision of Article 5 clause 1 of ITE Law, it is mentioned that electronic information and or electronic document and or its print out is the legitimate legal evidence. Furthermore, Article 5 clause 2 of ITE Law mentions that electronic information or electronic document as intended in clause 1 is the expansion of legal evidence and corresponding to the procedural law enacted in Indonesia. Thus, ITE Law has determined that electronic document and or its print out are the legitimate evidence and the expansion of legitimate evidence according to the procedural law enacted in Indonesia so that they can be used as evidence before the trial.

Then, Article 5 clause 3 of ITE Law mentions that electronic information and or electronic document is stated as legitimate when it uses electronic system corresponding to the provision existing in ITE Law. Thus, the use of electronic document as the legitimate evidence when using an electronic system corresponding to the provision as mentioned in Article 6 of ITE Law stating that electronic document is considered as legitimate as long as the information included can be accessed, displayed, ensured for its

completeness and accountable for thereby informing a condition. In addition, it is the electronic document, the position of which can be equalized with the document made on a piece of paper as mentioned in the General Explanation of ITE Law. This provision is an exception as intended in Article 5 clause 4 of ITE Law mentioning that several types of electronic document cannot be the legitimate evidence when they are related to its preparation, in which letter, according to the law, should be prepared in written form and letter as well as its document, according to the law, should be prepared in notary deed form or in the deed made by the deed preparing officials.

Considering the provision in the Article 5 clause 4 of ITE Law, when the parties want to enter into a formal agreement, the agreement will be considered as illegitimate until it is poured into written form manually in the form of either privately made deed (*akta bawah tangan*) or authentic deed. The examples of formal agreement are, among others, peace agreement, vide Article 1851 BW; Grant Agreement, vide Article 1682 BW; and trade agreement with land object, and trading deed of a plot of land, vide

Government Regulation No. 24 of 1997 about Land Registration.

In the attempt of preparing an agreement or electronic transaction poured into electronic document, the validity of such electronic document should contains electronic signature; it is consistent with the regulation concerning the most important element in preparing a deed as governed in Article 1867 BW juncto Article 1874 BW and the preconditions of legitimate agreement as governed in Article 1320 BW. Furthermore, it is mentioned that electronic signature has legitimate legal power and legal consequence as long as it meets the preconditions as mentioned in the Article 11 of ITE:

1. Data of electronic signature preparation is related to only the signed;
2. Data of electronic signature preparation during electronic signing process is under the authority of the signed only;
3. Any change in Electronic Signature occurring after the signing time can be known;
4. Any change in Electronic Information related to the Electronic signature after the signing time can be known;

5. There is a certain way used to identify who the signed is;
6. There is a certain way to show that the signed has agreed the corresponding electronic information.

Furthermore in Article 12 clause 2 of ITE Law it mentioned that everyone involved in Electronic signature is obliged to protect the security of Electronic Signature used. The presence of the electronically signing is related to general preconditions of evidence authenticity. Those preconditions include firstly, the material authenticity; it is the clarity of subjective and objective condition, particularity, competency, clear time and place, confidentiality, traceability, data completeness guaranty or information security, the copy should be as same as the original one, copy of deed. Secondly, formal authenticity, it is consistent with the form specified by law, including certain media and format, reading, whether or not the evidence has been read; time inclusion, whether or not time security has been written correctly (time-stamping), document and its substance security, and whether or not the historical data on the deed document has been obvious; log or notary-journal (notary

protocol) maintenance, whether or not it has been maintained well.

In judicature practice, the judges' attitude in viewing some evidence of electronic document is varied, some argue that electronic document evidence is the legitimate evidence and as supplement to conventional evidence in Procedural Law and some other argue that electronic document serves as supporting evidence should support other evidence to increase the judge's conviction. Thus, referring to the first argument, electronic document can be equated with the privately-made deed evidence, in which the privately-made evidence is recognized by the parties as having formal and material verifying power, but not having verification power to outside unless it is registered to public employees. Having formal authentication power is defined as what poured into the deed is indeed expressed by the parties corresponding to the actual condition, however, in practice in Cirebon District Court environment, there are some judges arguing that electronic document can be equated with letter evidence, when electronic document, for example in the form of *Facebook* can be downloaded and printed. But

electronic document can be equated with the supposition when the electronic document is in e-mail form that has been supported by 2 (two) other evidences. Such the argument has been included into the verdict by the Judge Chamber of Cirebon District Court's verdict over the love scandal using Short Message Service (SMS) as evidence that is then transformed into printout that is in turn considered as letter evidence. Similarly, in other case, when a husband catches his wife sending email to other man with undue content, the judge considers this email as an evidence of supposition.

In the case of labor dispute in Industrial Relation Court (*Pengadilan Hubungan Industri = PHI*), Surabaya, East Java with Register Number: 28/G/2010/PHI.Sby, one party used electronic document evidence in the form of broadcast in *Metrotvnews.com* and the judge considered the electronic document as supposition, in which its verification power should remain to be supported by 2 (two) witnesses who saw directly the incidences as same as those in the broadcast of *Metrotvnews.com*. Meanwhile, in Sidoarjo District Court, there are some judges arguing that electronic document evidence remains to be

categorized into letter evidence and the position of electronic document in a civil case trialing cannot stand alone but should be supported by other evidence. In principle, as long as there is a relationship to other supporting evidence, the electronic document is reasonable to use, and in examining the electronic document evidence, expert witness can be employed, but in practice in Sidoarjo District Court, some judges stated that no case is trialed with electronic document as evidence.

In the attempt of using electronic document, it should be understood that ITE Law prohibits actions/conducts as governed in the provision of Article 27-37 mentioning that when there is a misuse of information technology, particularly electronic document, harmful to others, any lawsuit can be filed civilly or criminally as specified in Articles 38, 39, and 45-52 of ITE Law.

The provision of ITE Law governing many cybercrime and other laws governing specifically any form of cybercrime (e.g., Telecommunication Law, Pornography Law) cannot be applied without the presence of Civil Code because the law beyond Penal Code qualifies the crime

only and threatens the perpetrator of crime and special definition (e.g. definition of electronic document, telecommunication) while the general definition should refer to the Penal Code as general rule.

Some cases have occurred, for example, the online gambling case as governed in ITE Law. The criminal provision threatening the perpetrator of crime is Article 27 clause (2) reading “Everyone deliberately and without entitlement distributing, transmitting or allowing the access to Information or Electronic Document containing gambling” is threatened with the punishment as mentioned in Article 45 clause (1) that everyone fulfilling the elements as intended in article 27 clauses (1), (2), and (3) or (4) with imprisonment maximally 6 (six) years and fine maximally IDR 1,000,000,000 (one billion rupiah).

In applying ITE law, in fact, there are many related legal provisions because ITE law applies special law beyond Penal Code governing the crime and its consequence, so general provision to apply ITE law should refer to the general law, Penal Code, to

apply its criminal procedural process or formal criminal law.²

Considering the case, the explanation about the criminal elements of gambling is that the elements of everyone and without entitlement should refer to Book I of Penal Code, while the definition of the elements of distributing, transmitting, or allowing the access to information or electronic document refer to ITE Law. Meanwhile, the definition of whoever in Article 27 clause (2) of ITE Law can be defined not only as individual (human being) but also corporation, and the definition of gambling content element refers to Book II of Penal Code, in Article 303 and 303 bis.

D. Conclusion

1. In civil case using electronic evidence, the evidence mentioned in article 1866 BW is the legally legitimate evidence as long as it is obtained through a lawful process. in civil case using electronic evidence, the evidence that is legitimate and can be revealed in the verification process is determined based on Article 5 clause (1) and (2) of

²Widodo, Hukum Pidana di Bidang Teknologi Informasi *Cybercrime Law: Telaah Teoritik dan Bedah Kasus*, Aswaja Pressindo, Yogyakarta, 2013, p.141.

Law Number 11 of 2008 about Information and Electronic Information confirming that information and or electronic document can be considered as a legitimate evidence in verification process particularly in civil case using electronic evidence. The evidence is the expansion of evidence as regulated and enacted in the civil case law corresponding to the provision of Article 1866 BW.

2. That the regulation on the verification principle included in Article 163 of HIR jo Article 1865 BW determining that everyone stating as being entitled with an object or pointing to an event to confirm his/her right, or denying others' right, he/she should verify it, seems to keep being enacted and unchanged after the enactment of ITE Law, but it emphasizes that the parties should ensure that the existing electronic document derives from the electronic system electronic system complying with the precondition based on legislation and after the enactment of ITE law, there is an addition of evidence and the recognition of electronic document as a legitimate evidence determining that electronic document or its print out is the legitimate evidence that can be used

before the trial as long as the information contained within it can be accessed, displayed, and ensured for its completeness and accountable for thereby informing a condition. In addition, the position of electronic document is equalized to the document prepared on a piece of paper as mentioned in General Explanation of ITE Law.

E. Recommendation

Considering the conclusions above, the following recommendations can be given:

1. There should be an attempt of understanding among the society, particularly the law enforcers, on the importance of verification principle in relation to the development of electronic document use.
2. There should be an attempt of understanding among the society, particularly the judges, on having the shared idea about the verification power of electronic document evidence after the enactment of Republic of Indonesia's Law Number 11 of 2008 about Information and Electronic Transaction (ITE Law).

REFERENCES

R. Subekti, Pokok-Pokok Hukum Perdata,
Jakarta: P.T. Intermasa, 2005, Cet.
XXXII.

Sudikno Mertokusumo, Hukum Acara
Perdata Indonesia Edisi Ke 7,
Yogyakarta: Liberty, 2006, Cet. I.

Munir Fuady, *Teori Hukum Pembuktian
(Pidana dan Perdata)*, PT. Citra
Aditya Bakti, Bandung, 2006.

M. Yahya Harahap, *Hukum Acara Perdata
: Tentang Gugatan, Persidangan,
Penyitaan, Pembuktian dan Putusan
Pengadilan*, Sinar Grafika, Jakarta,
2005.

M. Yahya Harahap, *Pembahasan
Permasalahan dan Penerapan
KUHP : Pemeriksaan Sidang
Pengadilan, Banding, Kasasi dan
Peninjauan Kembali*, Sinar Grafika,
Jakarta, 2002.

Widodo, Hukum Pidana di Bidang
Teknologi Informasi *Cybercrime
Law : Telaah Teoritik dan Bedah
Kasus*, Aswaja Pressindo,
Yogyakarta, 2013.

R. Subekti dan R. Tjitrosudibio, Kitab
Undang-undang Hukum Perdata,
Jakarta: P.T. Pradnya Paramita,
2005, Cet. XXV.

Retnowulan S dan Iskandar O, Hukum
Acara Perdata Dalam Teori Dan
Praktek, Bandung: C.V . Mandar
Maju, 2005, Cet. X.

R. Soesilo, RIB/HIR Dengan Penjelasan,
Bogor: Politeia, 1995