

THE URGENCY OF ELECTRONICS DOCUMENTS AND INFORMATION REGULATORY AS AUTHORIZED EVIDENCE IN INDONESIA'S COURTS

Ismail Rumadan, Universitas Nasional of Jakarta
Marsudin Nainggolan, Jayabaya University of Jakarta
Pri Pambudi Teguh, Universitas Nasional of Jakarta

ABSTRACT

The judges' acceptance of electronic information and documents as legal evidence are very different. The electronics evidence cannot be categorized as evidence that stand-alone, paralleled with the evidence in the Criminal Code. So a variety of electronic evidence are found in some judge's decisions, such as documentary evidence, witness testimony, testimony from the defendant, evidence for instructions and additional evidence for the judge's conviction.

Therefore, it is very important to reorganize the regulations of electronic documents and information as legal evidence in more detail and specific in order to provide uniformity and legal standing for judges in receiving and examining such electronic evidence in court.

Keywords: Documents and Information Electronic, Electronic Evidence, Indonesian Court.

INTRODUCTION

The regulation about electronic documents and information to become legal evidence as stipulated in Law no. 19 of 2016, concerning Electronic Information and Transactions, is still controversy regarding the legality status/legal standing in practicing law in Court. The reasons are, the print outs of electronic documents or information cannot immediately be accepted as legal evidences. Then, it is possible to change the electronic document and information, such as email, which is not personally used. This is because the sender and the recipient server has the same email record (Maya, 2010). So he problem is how is the legality of electronic documents or information can be submitted or admissible as valid evidence in court?

Article 164 HIR/284 Rbg regulates in a limited manner of five evidences known in civil procedural law, namely letters, witnesses, allegations, confessions and oaths. The definition of limitative means that there is no other evidence known than those specified in Article 164 HIR/284 Rbg. So the question is what about electronic evidence? Article 5 paragraph (1) of Law no. 19 of 2016 concerning Information and Electronic Transactions, stated:

"Electronic information and/or electronic documents and/or their printouts are stated as legal evidence." Furthermore, in paragraph (2) it is stated that; "Electronic information and/or electronic documents and/or their printed results as referred to in paragraph (1) is an extension of legal evidence in accordance with the procedural law which applicable in Indonesia".

The article above stated that there is no uniformity for judges to assess the existence of electronic information or electronic documents practically as valid evidence in court. There are still different perceptions among judges in accepting electronic documents and/or electronic information as valid evidence, some judges consider the status of electronic documents/electronic information as evidence under the hands, or as supporting and additional evidence (Marsuddin et al., 2020). However, some decisions reflect the judge's acknowledgment of the evidence in the form of email as legal evidence, as stated in the Denpasar High Court decision no. 150/PDT/2011/PT. Dps. However, in its decision stated that, photos which are part of electronic documents are not considered as evidence. This difference reflects the existence of legal uncertainty due to the absence of uniform regulation regarding the electronic documents and information as legal evidence in court (Muhammad, 2016).

Therefore, it is urgently needed to develop a regulatory basis of electronic evidence, especially in e-commerce transactions. Mainly related to validate the electronic evidence, the procedure acquisition of electronic evidence, easy to access the acquisition of electronic evidence.

Legal Issues

Based on the problems above, it can be identified several problems that will be studied in this journal, as follows:

1. How is the document/electronic information can be admissible as a valid evidence in resolving law disputes in court?
2. How is the urgency of regulating electronic documents/electronic information as legal evidence in court?

Electronic Documents and / or Electronic Information and Their Provisions as Evidence in Court

Definition of Electronic Documents and/or Electronic Information: According to the provisions, Article 1 number (1) of the ITE Law states: Electronic Information is:

“One or a set of electronic data, included but not limited only to writing, sound, pictures, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail), telegrams, processed perforations that have meaning or can be understood by someone who can understand it.”

Based on the above understanding, it can be stated that, the main requirement for something to be classified as electronic information is that it must be one or a set of electronic data that has been processed and has meaning. This electronic data is very extensively. It can be meant as data in binary language (8 bits consisting of the numbers 0 and 1), hexadecimal (amounting to 16 bits consisting of 0, 1, 2, 3, ... up to 9, a, b ... to f); text (for example with unicode language, which is a universal coding language that maps common and special characters in hexadecimal numbers); and/or in the form of application data (e.g. office files, audio files, image files, etc.) (Muhammad, 2012).

The definition of electronic information according to the ITE Law is not much different from the definition of electronic information in the UNCITRAL Model Law on Electronic

Signatures with Guide to Enactment 2001 in article 2 regarding "*definition*". There is the term "*data message*" which is basically electronic information in general, namely:

"Information generated, sent, received or stored by electronic optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents. "

From this definition it can be understood that electronic information is information generated, sent, received or stored by electronic devices or other devices, but not limited only to *electronic data interchange (EDI)*, electronic mail, telegram, telex or telecopy; and other actions for personal interest or on behalf of the person being represented) (Ahmad, 2005).

The definition of electronic information above, can be compared with the formulation of electronic information consists in Article 173 of the 2005 Criminal Code Bill, which is one or a set of electronic data including text, symbols, images, signs, signals, writing, sounds, sounds and other forms which have meaning (Barda, 2006) .

Furthermore, Article 1 number (4) of the ITE Law determines the definition of Electronic Documents as follows:

"Every Electronic Information that is created, forwarded, sent, received, or stored in a form of analog, digital, electromagnetic, optical, or others, which can be seen, displayed, and/or heard through a Computer or Electronic System, included but not limited only to writing, sounds, pictures, maps, designs, photographs or its kind, letters, signs, numbers, access codes, symbols or perforations that have meaning or can be understood by the professionals/authorized.

Based on the above definition, a document can be categorized as an electronic document if:

1. It constitutes Electronic information;
2. It is created, forwarded, transmitted, received, or stored in analog, digital, electromagnetic, optical or similar form;
3. It can be seen, displayed, and/or heard through a computer or electronic system;
4. It is included but not limited only to the texts, sounds, pictures, maps, designs, photographs or etc, letters, signs, numbers, access codes, symbols or perforations;
5. It is essential and has meaning.

Based on the explanation above, it can be concluded that every electronic document is definitely electronic information, but electronic information is not necessarily included as an electronic document. In addition to electronic information and electronic documents, Article 1 of the ITE Law also provides an understanding of Electronic Systems, namely:

"a series of electronic devices and procedures that function is to prepare, collect, process, analyze, store, display, announce, and/or disseminate electronic information. The meaning is, the computer has been equipped with an operating system and application, and can be used to prepare, collect, process, analyze, store, display, publish, transmit, and or disseminate electronic information .

As a comparison of the definition above, Article 206 of the 2005 Criminal Code Bill stated that the definition of a computer system is a tool or equipment or a device that is interconnected or related to one another, which follows a program, performs data processing automatically.

Documents/Electronic Information as Evidence in Court

Electronic documents are essentially writings form which is written in an electronic letter. Pitlo, a Professor of Civil Law, explained that the essence of written evidence is as a "*carrier of reading signs to translate a thought*". Meanwhile, Michael Chissick and Alistair Kelman suggested three types of evidence made by computers, namely (1) real evidence, (2) hearsay evidence, and (3) derived evidence (Arsyad, 2021).

Chissick and Kelman stated that calculations or analyzes are made by the computer itself through the application of software and the receipt of information from other devices such as a clock that is built-in directly into the computer or remote sender. This type of evidence is known as real evidence. This tangible evidence appears in a variety of conditions. If a bank computer automatically calculates the value of customer payments to the bank based on the rates, transactions that occur and credit balances that are cleared on a daily basis, then this calculation can be used as tangible evidence (Arsyad, 2021).

Then there are documents and data produced by a computer which is a copy of the information provided (included) by another person to the computer. Materials like this are referred to as hearsay evidence (evidence in the form of news from people), written checks and payment slips taken from a bank account, including hearsy evidence (Barama, 2011).

Meanwhile, derived evidence is information that combines real evidence with information provided by someone to a computer with the aim of forming a combined data; this is included as hearsay evidence in modern evidence laws. An example of derived evidence is a table in the daily column of a bank statement obtained from real evidence (which automatically creates bank bills) and hearsay evidence (individual checks and payment entry via ship (pay-in) (Arsyad, 2021).

If electronic documents can be used as written evidence, it must be proven whether or not the electronic documents meet the requirements of written evidence? In Article 1 paragraph 4 of Law ITE explaining the form of electronic documents are variety and depend on its functions. If electronic documents are limited only to the regular information so the document is categorized as regular mail and can not be used as a means of proof in the court. However, if the document is intended as an authentic document, then the document must meet several requirements.

The main requirement of electronic documents can be declared as valid evidence is the use of electronic systems that have obtained electronic certification from the government as regulated in Articles 15-16 of the ITE Law. Article 15 of the ITE Law stated;

1. Electronics must operate the Electronic System reliably and safely and be responsible for the proper operation of the Electronic system;
2. The Electronic System Operator is responsible for the Electronic System Operation;
3. The provisions as referred to paragraph (2) do not apply if it can be proven that the occurrence of forced an error, and/or negligence on the Electronic System user.

Whereas in Article 16 of the ITE Law, it is explained that every Electronic System Operator is required to operate an Electronic System that meets the following minimum requirements:

1. It can display Electronic Information and/or Electronic Documents entirety accordance with the retention period stipulated by the Laws and Regulations;
2. It can protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the Electronic System Operation ;
3. It can operate accordance with the procedures or instructions in the Electronic System Operation;
4. It is equipped with procedures or instructions announced or performed in language, information, or symbols that can be understood by the people who concerned with the Electronic system Operator, and
5. It has a sustainable mechanism to maintain the novelty, clarity, and accountability of procedures or instructions .

Another requirement is, must affix an electronic signature, and put it in a standard electronic contract. Written evidence is divided into authentic deeds and private deeds. , An authentic deed based on article 1868 of the Civil Code, is a deed made determined by law or before a public official authorized, where the deed was made. From this point of view, electronic documents cannot be said to be authentic deeds because based on Article 5 paragraph (4) of the Law, it is explained; The provisions regarding Electronic Information and/or Electronic Documents as referred to in paragraph (1) do not apply to:

1. A letter which according to the law must be in written form;
2. A letter and its documents which according to the law must be made in the form of a notarial deed or a deed made by the official authorized.

However, an electronic document can be said to be an underhand deed because it is a deed which intentionally made for verification by interested parties without assistance from the authorized official. From this verification point of view, in order for a deed to be of valued as a private deed, it must meet the main requirements, namely;

1. The letter or writing is signed;
2. The contents described to the legal state of law;
3. Intentionally made as evidence of acts or relationship in it.

The contents of the electronic document explain the legal actions carried out by the parties and the purpose is to be used as evidence by the parties who make the electronic document. Regarding to the requirement that an underhand deed must be signed, electronic documents do not use a signature like documents on paper. In electronic documents used is a digital signature (digital signature).

A digital signature is a signature that is created electronically that functions the same as a regular signature on a regular paper document. The digital signature must also meet the requirements so that it can be said to be valid as evidence, such as:

1. The Electronic signature maker data relates only to the signer.
2. The Electronic signature maker's data at the time of the electronic signing process is only by the signer;
3. Any changes to the Electronic Signature that occur after the signer's time can be noticed;
4. Any changes to the Electronic Information related to the Electronic Signature after the signing time can be notified
5. There are certain ways that can identify who the signer is, and
6. There are certain ways to show that the signer has given his/her consent to the related electronic information

Judge's Assessment of the Existence of Electronic Evidence in Court

The existence of electronic document evidence or electronic information as evidence in court as regulated in the ITE Law is not immediately accepted as legal evidence in the process of resolving cases in court, especially in civil disputes. When discussing the assessment of evidence, the evidence submitted by the parties to the trial will be assessed and validated, in this case the judge is authorized to conduct the assessment.

In general, as long as the law does not stipulate otherwise, the judge is free to evaluate the evidence. In this case, the legislators can bind the judge on certain evidences (eg documentary evidence), so that the judge does not free to vote. One example is the written evidence that has its strength proof binding the judge or the parties.

Instead, legislators can submit and give freedom to the judge in assessing the proof of evidence, such as witness testimony that has the strength of evidence, freely, meaning it is privileged for the judge to assess the proof, the judge may be bound or not the information given by the witness (Council of Europe, 2013).

According to Jumadi, a judge at the Magelang Religious Court, (Heniyatun, 2018), the way how to use Electronic Information as evidence submitted to the court in dispute resolution, that the evidence must be submitted in front of the court by attaching digital forensic results issued by officials/agency/authorized party and/or bring in the expert witnesses. Digital forensics is a technique of collecting, identifying, analyzing, testing and presenting electronic evidence used to resolve legal issues in court.

It means that one of the requirements to test the validation of electronic information or electronic documents submitted as legal evidence in court must be accompanied by an attachment of digital forensic results issued by officials/agencies/authorized parties and/or bring in expert witnesses.

Meanwhile, other judges states, that the method of submitting Electronic Information evidence in front of the trial, is in the form of printed results, meaning that the submission of electronic information evidence is as same as submitting written evidence before the court, which is the form of printouts. On the contrary, according to some other judges, the submission of Electronic Information evidence does not have to go through expert witnesses. Judges in adjudicating civil cases can apply electronic information evidence as initial evidence (Heniyatun, 2018).

Based on the results of research conducted through a survey of the perceptions of judges in understanding the existence of electronic evidence in the form of documents or electronic information, it can be summarized that the perceptions and understanding of judges are very diverse about the existence of electronic evidence. The diversity of perceptions can be categorized or grouped as follows: (Marsudin et al., 2020)

1. Electronic evidence as witness' testimony
2. Electronic evidence as proof's of letters/letter of proof
3. Electronic evidence as expert's testimony
4. Electronic evidence as a statement of the defendant
5. Electronic evidence as evidence
6. Electronic evidence as evidence of instructions/guidances

7. Electronic evidence as a stand-alone evidence

Likewise, it can be found in several judges' decisions regarding electronic evidence submitted to courts, both in criminal cases, civil cases, religious civil cases, as well as state and military administrative cases. There are different judges' considerations. This difference is not only seen in a judge's decision with another judge's decision, but there is also a court decision in which one panel of judges considers different terms and names related to the existence of electronic evidence submitted in court (Marsudin et al., 2020).

In religious civil cases, for example, whether or not evidence with electronic information evidence, in the form of short message service (SMS), video, compaq disk (CD), photos printed from mobile phones (HP), can be used as evidence depends on the legal considerations from the panel of judges. The panel of judges of the Religious Courts accepts or does not accept the evidence; it is still guided by Article 164 HIR, Article 284 RBg, 1866 BW, and evidence of local examination and expert testimony. If the evidence is accepted by the judge, then the position of the evidence is only assessed as preliminary evidence or preliminary evidence. The Electronic Information evidence can become valid only by the panel of judges consideration, because the panel still believes that judges can only make decisions based on the evidence specified in the law (Puji, 2018).

Even in divorce cases, most judges cannot accept electronic evidence as evidence at trial. For example, in the case of the husband as the applicant accusing his wife (the respondent) of committing adultery with another man in a hotel. The applicant submits photo evidence that is printed/printed from the cellphone. The panel of judges could not accept the printed evidence of the photo which is a form of Electronic Information, because according to Islamic law, the accusation of committing adultery must be proven by presenting four male witnesses who meet the requirements as witnesses who witnessed the adultery directly. The next mechanism, if the husband insists on divorcing his wife who he thinks has committed adultery, is that the husband must swear four times accusing his wife of adultery, then followed by a fifth oath with the curse of Allah on him if the accusation of his wife for adultery is a lie as stipulated in Article 125-127 Islamic Law Compilation.

Then in criminal cases, most of the judge respondents stated that in some cases, they had never considered electronic evidence as valid evidence. It is because the process of obtaining, confiscation, searching, storing, and analyzing the evidence was not in accordance with the criminal procedure law. So the judge can refuse electronic evidence submitted by the public prosecutor in the trial if the acquisition of the electronic evidence, inconsistent with the procedural law.

It means that the electronic evidence does not have legal force, if the acquisition of the evidence is not carried out in the context of law enforcement from the police, prosecutors, and/or other law enforcement institutions requests, stipulated by law as regulated in Article 31 paragraph (3) UU ITE. Based on the considerations stated in the Constitutional Court Decision No. 20/PUU-XIV/2016 dated 7 September 2016 related to the legal considerations of the panel of constitutional judge in No. 20/PUU/XIV/2016 which arranges the position of the evidences as part of the valid evidence, the method of acquisition must be also applicable to the laws and regulations.

In this case, the evidences are electronic information and/or electronic documents used to commit a criminal act, objects obtained from criminal acts or objects indicating the occurrence of a crime. In addition, the panel of constitutional judges determines electronic information and/or electronic documents can only be submitted as legal evidence, the evidences must be obtained in a legal way, otherwise they can be ruled out because they have no evidentiary value.

The Reception of Electronic Information/Electronic Documents as Legal Evidence in the Court

The existence of electronic evidence or electronic documents as regulated in the ITE Law is not immediately accepted as legal evidence in the dispute resolution process in the Court, especially in civil disputes. There are different views of judges regarding the receipt of electronic devices or electronic documents at the Court.

From some point of views mentioned above, it is clear that there are differences of opinion among judges in accepting and understanding the existence of electronic information or electronic documents as legal evidence in court. However, there is one point of view stated, electronic information or electronic documents can be evidence. Although, there is a slight difference on trial, such as there must be an acknowledgment from the owner to be shown or displayed in court and can be used as legal evidence such as other written evidences. In addition, electronic information can be categorized and recognized, if such recognition is done before trial and can be proven against those who claimed (Marsuddin et al., 2020). So it is a decisive evidence, namely strong evidence. So the judge is obliged to accept that the confession is true, the confession cannot be revoked.

Based on the differences in understanding regarding the reception of electronic documents and information in Court, it is necessary to immediately make legal norms which regulate technically as a reference for the parties, including judges, to accept the electronic information or documents as legal standing evidence in court. It is because the use of electronic information and documents type are very diverse so it is difficult for consumers to access the valid electronic information and data from the source.

The Urgency of Regulating Electronic Evidence in Procedural Law

Identifying the legal aspects of the existence of electronic evidence as regulated in several statutory provisions such as the Corruption Crime Act, the Money Laundering Law, the Terrorism Eradication Act and the Electronic Information and Transaction Law. There are some designations and categorization of the legal standing of the electronic evidence. The Corruption Crime Law categorizes electronic evidence as evidence of guidance. However, the Money Laundering Act, the Combating Terrorism Act, and other laws place electronic evidence as independent evidence.

The non-uniformity in the regulation of electronic evidence causes various perceptions and views, as well as understanding from judges regarding the existence of electronic evidence as mentioned previously. The difference in understanding by the judges was caused by several factors. First; the legal standing of electronic evidence is not clearly and explicitly stated in the rule of law. Second; the judge's own understanding of the ITE Law which regulates the

electronic evidence is various. Forty-nine percent (49%) of the 358 judges who were asked for comments regarding electronic evidence regulated in the ITE Law both in the scope of civil disputes and in criminal cases, stated that the existence of electronic evidence was not clear in the rule of law and not clearly regulated. (Masudin et al., 2020) .

The third factor, the ability to identify the validity of the electronic evidence in court. The average judge has limited knowledge in information and technology, so judges find it difficult to ensure that electronic evidence can be submitted as valid evidence in court, or not. Therefore, in some certain cases the existence of such evidence is ruled out by the judge.

As the result, the judge's limited knowledge becomes a serious problem when the judge has difficulty identifying the procedure for obtaining the electronic evidence. As stated on the decision of the Constitutional Court Number 20/PUU-X, in order for electronic evidence to be valid evidence, it must be obtained legally. Unauthorized acquisition will result in the waiver and no legal value of the evidence.

Therefore, according to some judge's point of view, if the acquisition of electronic evidence is not applicable to the procedural law, the electronic evidence can be set aside. Putting aside the electronic evidence submitted to the court due to non-compliance procedure is not solely based on technical considerations, but also the issue of protection of human rights. If the procedure for taking electronic evidence is not in accordance with the applicable procedural law, certainly it has great potential for violations of human rights, such as the protection of privacy rights and property rights to data, information, or documents. For a certain degree, dissenting about the acquisition of evidence with human rights is increasingly assertive when it comes to personal data or sensitive data, while the purpose of law enforcement in the context of criminal law is to protect human rights.

Another issue that needs attention is that the only rule that provides a procedural basis is in Article 43 paragraph 3 of the ITE Law. Furthermore, the ITE Law stated that the procedures only apply to criminal acts regulated in the ITE Law, which means all criminal acts outside ITE law, will be no provisions regarding the procedure for obtaining electronic evidence (Miko, 2019) .

It is mutually understood that in the context of criminal law, the Criminal Procedure Code (KUHAP) regulates searches, confiscations, examinations in court, to the status of post-trial evidence. However, it should be understood that the characteristics of electronic evidence are very different from non-electronic evidence. Electronic evidence is vulnerable and easily manipulated, deleted, duplicated or disseminated. Therefore, relying on the regulation on the substance of the current Criminal Procedure Code is clearly inadequate.

For example, searches in the Criminal Procedure Code are aimed at homes or other closed places and against bodies. KUHAP does not recognize any searches of electronic devices or systems. Not to mention if the devices and systems are locked or in the form of server-based systems, such as electronic mail, social media, or cloud-based storage media. There is a regulatory gap between the Criminal Procedure Code and the development of law enforcement which is increasingly dynamic following technological developments (Miko, 2019).

As the result, the differences' point of view among judges are various in understanding the existence of electronic evidence, the void of the rules of prosedural law, and clearly shows the uncertainty in law enforcement. Law enforcement in this condition will of course be faced with

different standards. For example, in case A, the electronic evidence obtained is completely undisputed. However, in other cases, the electronic evidence was questioned and even rejected by the judge.

Consequently, on the individual side, is the lack of guaranteed protection of human rights when dealing with law enforcement. This applies not only to the accused / defendant, but also a witness, or even not parties litigant but have data related to the law enforcement. In fact, philosophically, procedural law contains the substance of human rights which were created to limit power and protect human rights.

Likewise, in civil cases, the ITE Law does not provide the clarity of legal standing and the protection of parties in civil disputes. In fact, if you look closely, the substance of the ITE Law is basically regulating an electronic transaction which aims to make the parties feel comfortable and feel protected by the government through the rule of law in conducting business transactions using information technology facilities.

It can be understood that in the context of electronic transactions, the relationship between parties in this case between consumers and business actors in conducting electronic transactions, the consumer party has a very weak and unbalanced position with business actors in the event of a dispute. It is very difficult for consumers to prove that there was a mistake made by business actors that resulted in losses for consumers. Access to obtain evidence in the form of electronic information or electronic documents is very difficult, because the information technology is under the control of business actors. This is of course different from criminal cases, those who have the obligation and responsibility to prove a criminal act are the police or the prosecutor's office, while in civil cases, the burden of proof is of course on the parties, the parties themselves who prove the argument of their claim for a loss due to mistakes in an electronic transaction.

Thus it can be said that the existence of the ITE Law has not clearly regulated the procedures for proving in civil disputes relating to transactions or electronic business to protect parties, especially consumers who are in a weak position. Therefore, what is important and urgent at this time is the need to develop a regulatory basis to provide legal certainty/legal standing regarding the existence of electronic documents and electronic information as valid evidence to be used in court.

In the context of criminal procedural law, of course, it is related to the procedure for obtaining electronic evidence, which starts from search, confiscation, examination in court, to its return or destruction. As a principle regulation, changes at the level of procedural law are important, especially to provide a uniform standard for related regulations.

However, this is not enough if it is not followed by regulations or guidelines in the respective law enforcement institutions and courts, especially for the judiciary environment. A technical rule of law in the form of a Supreme Court Regulation (PERMA) is urgently needed to fill the void of the current procedural law which has not yet been updated.

In principle, the importance of structuring regulations relating to electronic evidence is aimed at strengthening law enforcement as well as providing guarantees for the protection of human rights. These can go hand in hand without colliding with each other. The urgency of this regulation is also related to upholding the rule of law by placing the law enforcers to their duties,

functions and authorities and adapting to advance the information and technology and legal developments in society.

CONCLUSION

Based on the problem of receiving electronic documents and electronic information as legal evidence by judges in court, and the urgency of regulating electronic documents and information as legal evidence in court, it can be concluded that; the judge's considerations and approval on electronic evidence in the form of electronic information and / or electronic documents are different from to another. In addition, Electronic evidence can not be categorized as a stand-alone parallel evidence with evidence in the Criminal Code. So in some verdicts the status of electronic evidence are found diversity, such as charcoal evidence; letter of evidence, witness' testimony, the defendant's testimony, instructions and additional evidence for the judge's conviction.

Thus, it is very important to organize the regulations of the existence of electronic documents and information as legal evidence in more detail and specific in a procedural law and in order to provide uniformity and legal standing/certainty for judges in receiving and examining electronic evidence in court. The Urgency of regulating electronic evidence is also concerned with upholding the rule of law by placing the law enforcement to their duties, functions and authority and adapting to the information and technology's law development in society.

REFERENCES

- Ahmad, M.R. (2005). *Towards legal certainty in the field: Information and electronic transactions, ministry of communication and information technology of the republic of Indonesia*. Jakarta.
- Arsyad, M.S. (2001). Business transactions in electronic commerce (E-Commerce): Study of legal problems and solutions. *Journal of Law*, 16(8), 1-9.
- Barda, N.A. (2006). *Mayantara crime development of cybercrime studies in Indonesia*. Raja Grafindo Perkasa, Jakarta.
- Council of Europe. (2013). *Electronic evidence in civil and administrative proceedings*. Bandung.
- Heniyatun. (2018). Juridical study of evidence with electronic information in the settlement of civil cases in court. *Varia Justicia*, 14(1), 1-9.
- Maya, I. (2010). *Aspects of electronic commerce agreements and their implications on the law of evidence in Indonesia*.
- Muhammad, I.T. (2016). Electronic documents as evidence in the perspective of Indonesian civil procedure law reform. *USU Law Journal*, 4(1), 1-9.
- Muhammad, N.A.A. (2012). *Digital forensic, practical guide to computer's investigation*. Jakarta: Salemba Infotek Publisher.
- Puji, S. (2018). Juridical study of evidence with electronic information in the settlement of civil cases in court. *Varia Justicia*, 14(1), 1-9.