IRJILS
Indonesian Research Journal in Legal Studies
Volume 01 No. 01, September 2022
e-ISSN:

The Legality of Electronic Signature (Digital Signature) Judging from Civil Procedure Law

Basir[1*], Osgar Sahim Matompo[2], Maisa[3]
[123]Pascasarjana Universitas Muhammadiyah Palu
(*)Email Korespondensi: basirmh@gmail.com

ABSTRACT

This study aims to determine and analyze the legal position and power of digital signatures as evidence according to government regulation Number 82 of 2012 and to determine and analyze the legal requirements for the operation of electronic systems and transactions according to government regulations Number 82 of 2012.

The results of the study found that an electronic signature will have a perfect legal force if it meets the elements described in Article 53 paragraph (2) of Government Regulation No. 82 of 2012 so if it does not meet the elements of Article 53 paragraph (2) of Government Regulation No. 82 of 2012 then the implementation of the digital signature can be said to be juridical (legal defects). The legal requirements for electronic systems and transactions are based on Government Regulation 82 of 2012. According to what is described in Article 41 paragraphs (1) to (3) of government regulation Number 82 of 2012 concerning the operation of electronic systems and transactions as long as they fulfill these provisions, they can perform legal electronic transactions which are very relevant to people's lives and can make it easier for the public to conduct electronic transactions and various other electronic transactions. In addition, if the users feel that their rights have been violated during exertion, they can make reports and complaints to the authorities in the field of information technology and electronic transactions in accordance with what is described in Article 43 paragraphs (1) to (5) of Law Number 19 of 2016 on the amendment to Law Number 11 of 2008 regarding information and electronic transactions.

The research advice is the need for socialization related to digital signatures by the government at all levels of society, especially in rural areas. There needs to be a definite and clear legal force from an uncertified electronic signature so that in its application it is used effectively and the provisions of laws and regulations by users in conducting electronic transactions in order to get security and definite services.

Keywords: *Signature; Electronic*

ABSTRAK

Penelitian ini bertujuan untuk mengetahui dan menganalisis kedudukan dan kekuatan hukum dari tanda tangan elektronik (digital signature) sebagai alat bukti menurut peraturan pemerintah Nomor 82 Tahun 2012 serta untuk mengetahui dan menganalisis syarat sah penyelenggaraan sistem dan transaksi elektronik menurut peraturan pemerintah Nomor 82 Tahun 2012.

Hasil penelitian menemukan bahwa tanda tangan elektronik akan memiliki kekuatan hukum yang sempurna apabila sudah memenuhi unsur-unsur sebagaimana dijelaskan dalam pasal 53 ayat (2) Peraturan Pemerintah Nomor 82 tahun 2012 demikian apabila tidak memenuhi unsur-unsur pasal 53 ayat (2) peraturan pemerintah nomor 82 tahun 2012 maka pelaksanaan tanda tanda tangan elektronik (digital signature) tersebut dapat dikatakan cacat yuridis (cacat hukum). Syarat sah penyelenggaraan sistem dan transaksi elektronik menurut Peraturan Pemerintah Nomor 82 tahun 2012. Sesuai dengan apa yang dijelaskan dalam pasal 41 ayat (1) sampai (3) peraturan pemerintah Nomor 82 tahun 2012 tentang penyelenggaraan sistem dan transaksi elektronik selama memenuhi ketentuan tersebut maka dapat melakukan penyelenggaraan transaksi elektronik yang sah demikian sangat relevan dengan kehidupan masyarakat serta dapat memudahkan masyarakat dalam melakukan transaksi elektronik dan berbagai transaksi elektronik lainya dan apabila para pengguna pada saat melakukan transaksi elektronik merasa haknya dilanggar dapat melakukan laporan dan pengaduan ke pihak yang berwenang dibidang teknologi informasi dantransaksi elektronik sesuai dengan apa yang dijelaskan pada pasal 43 ayat (1) sampai (5) Undang-Undang Nomor 19 tahun 2016 atas perubahan Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

Saran Penelitian yaitu perlunya sosialisasi terkait dengan tanda tangan elektronik (digital signature) oleh pemerintah kepada seluruh lapisan masyrakat terutama di daerah-daerah perdesaan. Perlu adanya kekuatan hukum yang pasti dan jelas dari Tanda tangan elektronik tidak tersertifikasi sehingga dalam penerapannya digunakan dengan efektif serta Ketentuan peraturan perundang-undangan oleh para pengguna dalam melakukan transaksi elektronik supaya mendapatkan keamanan dan pelayanan yang pasti.

Kata Kunci : Tanda Tangan; Elektronik

1. INTRODUCTION

The presence of the information society, which is believed to be important in the world community in the third millennium, is marked by the increasingly widespread use of sophistication in information technology in various activities of human life, not only in developed countries but also in Indonesia. This phenomenon in turn has placed information as a very important and profitable economic commodity. Therefore the law is needed to regulate such information. The use of electronic technology in electronic commerce has a very positive impact, namely in the speed and convenience and sophistication of conducting transactions Face to face agreements (meeting directly) business people are now no longer needed but meet face to face through electronic media so that it can be said this electronic commerce is a new economic driver in the field of technology, especially in Indonesia.

Electronic transactions are non-face (without meeting face to face), non-sign (not using the original signature) and without area boundaries (a person can conduct electronic transactions with other parties even though they are in different countries) using information technology. In its development, the security aspect of information has begun to be considered. When this information becomes corrupted there are risks that must be borne by the people who send it, need it, or just see it. Due to the use of this electronic information, using a public network, where everyone can find out electronic information, is detrimental to interested parties who use information technology for the sale of goods or services. Therefore, there is a great need for legal products that aim to improve the security of electronic transactions through electronic networks, as well as to provide recognition of the legal power of electronic evidence and electronic signatures.

Wider problems occur in the civil sector because electronic transactions for trading activities through electronic systems (electronic commerce) have become part of national and international commerce. This fact shows that convergence in the fields of information technology, media, and informatics (telematics) is developing continuously, along with the discovery of new developments in the fields of information technology, media, and communication.

The analysis of the rationale for electronic information as evidence in civil evidence and the validity of electronic signatures in trading using electronic commerce shows a complex and holistic picture. This happens because of the virtual nature of electronic transactions so that the network system does not recognize regional or state boundaries. On the other hand, the civil evidence law in Indonesia provides restrictions on evidence, namely written evidence, witnesses, allegations, confessions, and oaths before a judge. The main evidence in civil proof law is written evidence which is a problem because electronic commerce uses tools, namely electronic information, and electronic signatures. Therefore, this research was conducted by taking an inventory, systematizing, analyzing, and evaluating the laws and regulations concerning the issue of civil evidence in Indonesia with legal enforcement of electronic information and electronic signatures. It appears that it turns out that through the analysis of the articles of written evidence used to form the basis for the validity of electronic information and electronic signatures, it is not easy because they have many meanings. So the only way to do this is through legal discovery (Rechtvinding) on the written evidence with a statute, comparative, philosophical approach.

Electronic documents signed with digital signatures can be categorized as written evidence. However, there is a legal principle that makes it difficult to develop the use of digital signatures, namely the requirement that the document must be viewable, sent, and stored in paper form. Problems will arise when someone wants to make a transaction. For example, buying goods, the parties have begun to be faced with various legal problems such as the validity of the documents made, digital signatures that are made when the person agrees to make a transaction, the binding force of the contract, and the cancellation of the transaction and so on. One of the crucial issues in E-commerce transactions is related to security in the payment mechanism and security risks in transactions, such as information regarding the transfer of credit card data and consumer personal identities. In this case, there are two main problems, namely: first regarding identification integrity which concerns the identity of the sender which is strengthened through digital signatures, and second regarding message integrity which concerns whether the message sent by the sender is actually received by the intended recipient (Intended Recipient). (Abdul Halim and Barkatullah).

An e-commerce agreement is made by interested parties in the form of electronic documents, if one of the parties violates the agreement or the achievements of one of the parties, the aggrieved party can sue the Court with electronic document evidence. In civil cases, in this proof stage, the parties are given the opportunity to show the truth of the legal facts which are the main points of the dispute. Thus, the judge examines and decides the case based on the evidence submitted by the disputing parties. Proving is an effort to collect facts that can be analyzed from a legal perspective and related to a case that is used to give the judges confidence in making decisions. While proof is a process to prove a case accompanied by facts that can be analyzed from a legal perspective to give the judge confidence in making decisions. Article 11 of the ITE Law discusses electronic signatures where this law expressly acknowledges that although it is only a code, electronic signatures have the same position as manual signatures in general which have legal force and legal consequences. The requirements as referred to in this article are the minimum requirements that must be met in every electronic signature.

This provision opens the widest opportunity for anyone to develop methods, techniques, or processes for creating electronic signatures. The government regulations in question, among others, regulate the techniques, methods, facilities, and processes for making electronic signatures. Article 12 of UU.ITE discusses who has the right to and can use electronic signatures. Limitations for security are also required in this electronic signature. Article

11 paragraph 1 part c and d of UU.ITE requires a method to find out any changes to electronic signatures regarding the validity of transactions and the strength of proof. In addition, electronic transactions do not require hard copies or paper slips, however, every transaction involving execution is provided with proof in the form of a number or code that can be stored or recorded on a computer or printed.

Proof of the contents of the file or document can also be proven. The trait to be proven is integrity. This property can be maintained and proven if a digital signature is used to certify the file because, with a digital signature, a change of just one letter in the contents of the file will be able to show that the file has changed even though it is not shown which part has changed.

With the understanding of electronic information that covers a broad spectrum, it becomes essential in virtual activities, especially e-commerce activities. So electronic information as evidence in civil proof law is important because it involves the identity of the subject, the substance of the information, the fixation methodology, and the storage media that makes the information clear to know. How about the original signature as well as the information signed on paper converted to electronic data by scanner equipment, does it have legal force and legal consequences? Of course, it does not have legal force and legal consequences, because the signature is not made based on the agreed information in other words the agreed information does not become the hand-making data, so that changes to the electronic signature and/or electronic information after the signing time cannot be is known.

Based on several descriptions of the background, the author formulates the main research issue (legal issue) "Legacy of Electronic Signatures (Digital Signature) in terms of Civil Procedure Law". What is the position and legal force of an Electronic Signature (Digital Signature) as evidence according to government regulation Number 82 of 2012? What are the legal requirements for the operation of electronic systems and transactions according to government regulation Number 82 of 2012?

2. LITERATURE REVIEW

1. Overview of Electronic Transactions

Electronic Commerce or abbreviated as E-Commerce is a business activity involving consumers, manufacturers, service providers, and intermediaries using the internet. The use of internet facilities is a technological advancement that can be said to support the entire spectrum of commercial activities.

This is because the internet is a computerized network that is very global in nature and can be accessed throughout the world at an unlimited time or in other words online 24 hours every day 7 days a week. All information can be accessed anytime, anywhere, and at any time. So with the sophistication of a computer network called the internet, entrepreneurs and providers are creative to take advantage of this land as an arena for commercialization, which is to get the maximum profit. He runs it very creatively, namely shopping or making transactions in cyberspace, which is known as shopping on the internet. Shopping on the internet is what is known as E-Commerce.

a. Types of Electronic Transactions

According to Adi Sulistya Nugroho, electronic transactions are a basic concept consisting of the following aspects:

1) Automation Automation of business processes instead of manual processes;
2) Streamlining or Integration An integrated process to achieve efficient results;
3) Publishing, ease of communication and promotion for traded products and services;
4) Interaction, exchange of information or data between business actors by minimizing (Human Error);
5) Transaction, an agreement between two business actors to transact by involving other institutions as a payment function. (Eka Nugraha et al 2017).

2. Overview of Theory Regarding the Validity of Electronic Signatures.

The use of a signature is a formal custom used to express a person's approval while at the same time confirming the identity (authentication) of a person who is signing for something, whether it has legal implications or not. According to Tan Thong Kie, a signature is a statement, the signer's will, that by affixing his signature under an inscription, he wants the writing to be considered his own by law. (Tan Thong Kie 2007). The definition of a signature in a general sense is an arrangement of signs (letters) in the form of writing from the signer, where the person who makes the statement or statement can be individualized (Herlien Budiono 2007).

The definition includes an assumption that statements made in writing must be affixed with the signature of the person concerned. According to the American Bar Association (ABA), the notion of a signature can be any sign made with the aim of providing approval and authentication of a document.

The definition of electronic signature, based on Article 1 paragraph (12) of Law Number 11 of 2008 concerning Electronic Information and Transactions is as follows: "Signature consisting of electronic information attached, associated or related to other electronic information used as verification and authentication tool". The signer is the legal subject associated with or related to the electronic signature. This definition includes an assumption that statements made in writing must be affixed with the signature of the person concerned. A digital signature is security on digital data that is made with a private signature key whose use depends on the public key that is the partner (Din Mudiardjo, 2008). According to Julius Indra Dwiparyo, an electronic signature is an electronic identity that serves as a sign of approval of the obligations attached to an electronic deed (Julius Indra Dwipayono, 2005).

Factors related to the validity of electronic signatures

1. Confession

According to Sudikno Mertokusumo, acknowledgment is a one-sided statement, both written and verbal, that is firm and stated by one of the parties that confirms either in whole or in part an event, right or legal relationship proposed by the opponent, resulting in no need for further examination by the judge. (Ahmaturrahman, 2005).

Confessions at trial are evidence:

a. Perfect evidence means that no other evidence is needed as regulated in Article 311 Rechtsreglement voor de buitengewasten (RBg) or Article 174 Herziene Indonesische Reglement (HIR).
b. Evidence that determines the meaning does not allow proof of the opponent (Article 1916 paragraph (2) point 4 of the Civil Code).
c. It cannot be withdrawn (article 1926 of the Civil Code).

2. Electronic Signature

Based on Article 1 paragraph 12 of Law Number 11 of 2008, an electronic signature is a signature consisting of electronic information that is attached, associated, or related to other electronic information used as a means of verification and authentication.

Electronic information using public networks has a higher risk of being manipulated. It is possible for someone with malicious intent to replace electronic information that has been signed by the parties with other electronic information but the signature does not change. In electronic data, these changes are easy to occur and not easily recognizable. Therefore, electronic signatures must be associated with electronic information.

Associated is the electronic information that you want to sign into the electronic signature creation data. Thus, the electronic signature and the signed electronic information are closely related to paper functions. The advantage is that if there is a change in the electronic information that has been signed, the electronic signature will also change. (Ronny, 2008).

3. Electronic Documents

Based on article 1 paragraph 4 of Law Number 11 of 2008, electronic documents are any electronic information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, 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, symbols, or perforations that have meaning or can be understood by people who are able to understand them. .

Electronic documents can be used as legal evidence, according to the Law on Information and Electronic Transactions, an electronic document is declared valid to be used as evidence if it uses a reliable and safe electronic system, and meets the following minimum requirements:

a. can display electronic information and/or electronic documents in full in accordance with the retention period stipulated by the laws and regulations;
b. can protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the operation of the electronic system;
c. can operate in accordance with procedures or instructions in the operation of the electronic system;
d. equipped with procedures or instructions announced in language, information, or symbols that can be understood by the party concerned with the operation of the electronic system;
e. have a sustainable mechanism to maintain the novelty, clarity, and accountability of procedures or instructions.

3. METHODS

This research uses normative legal research (Abdul Kadir Muhammad 2004). The selection of this type of normative research is related to the formulation of the problem that becomes the issue of legal research. This type of normative legal research is used to analyze the content, nature, and legal duties regulated in laws and regulations or in those contained in the legal

substances. Normative juridical research is also used to study/analyze secondary data in the form of legal materials, especially primary legal materials and secondary legal materials (Ronny Hanitijo, 1988). The research specifications in this thesis include descriptive analysis, which describes the applicable laws and regulations related to legal theories and legal implementation practices concerning the above problems.

Theories and laws and regulations analyzed e-contracts or online contracts and e-commerce transactions without using mathematical or statistical formulas. After the data analysis is complete, the results will be presented descriptively, namely by telling and describing what is in accordance with the problems studied. Based on these results, the authors formulate a conclusion that is the answer to the problems raised in this study, namely the position and Legal Power of Electronic Signatures (Digital Signatures) as evidence according to government regulation Number 82 of 2012.

4. RESULTS AND DISCUSSION

1. The position and legal force of the electronic signature as evidence according to Government Regulation Number 82 of 2012.

Electronic signatures will have legal force and consequences as long as they meet the requirements as described in government regulation number 82 of 2012 Article 53 Paragraph (2) states that:

a. The electronic signature maker's data relates only to the signer;
b. The electronic signature creation data at the time of the signing process is only in the power of the signer;
c. Any changes to the electronic signature that occur after the time of signing can be noticed;
d. Any changes to the electronic information related to the electronic signature after the time of signing can be known;
e. There are certain methods used to identify who the signer is, and

the type of electronic signature is described in government regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions in Article 54 paragraphs (1) to (3) states that:

a. Electronic signatures include
b. A certified electronic signature; and
c. The electronic signature is not certified.
d. The certified electronic signature as referred to in paragraph (1) letter must meet the following requirements:

(1) made using the service of providing electronic certification; and
(2) proven by electronic certificate

e. The non-certified electronic signature as referred to in paragraph (1) letter b is made without using the service of providing electronic certification (PP.82.2012).

According to the elDAS regulation initiated by the European Union, digital signatures are divided into 3 types based on the technology used, namely:

a. Simple

A simple electronic signature is an electronic signature in its simplest form because it is not protected by any encryption method. The most common example is a wet signature which is scanned by an electronic device and then inserted into a document.

b. Basic

A basic electronic signature does not have much difference compared to a simple electronic signature, the advantage of a basic electronic signature from a simple electronic signature is only its ability to show changes that occur after the document is signed.

c. Advanced and Qualified

An advanced and qualified digital signature is the most secure electronic signature and has the legal force equivalent to a wet signature on paper. Advanced and qualified digital signatures are created using asymmetric cryptography technology and public key infrastructure.

The attributes and how the electronic signature technology works are explained as follows. Digital signatures are created using cryptography techniques and public key cryptography, where the algorithm uses two keys. The first key is the key to form a digital signature and the second key is used to verify the digital signature or restore the message to its original form. This concept is also known as an asymmetric cryptosystem. The use of digital signatures requires two processes, namely from the signatory and from the recipient. In detail the two processes can be explained as follows:

1. Formation of a digital signature using the hash value generated from the document as well as a predefined private key. In order to guarantee the security of the hash value, there should be a very small chance that

the same digital signature can be generated from two documents with different private keys.

2. Digital signature verification is the process of checking digital signatures by referring to the original document and the public key that has been provided. Thus it can be determined whether a digital signature is created for the same document using a private key that corresponds to the public key (Husnul Hudzaifah 2015).

Table I
Comparison of advantages between certified digital signatures, non-certified electronic signatures, and ordinary signatures.

Certified digital signatures	**Non-certified electronic signatures**	**Ordinary signatures**
It is used to secure the document if there is a change in the document, whether written (even if it is 1 character) or metadata, the digital signature becomes invalid.	It is used to verify documents	Regular signature without internet network
No need for physical documents because it uses digital documents	It can be in the form of images, writings, and even checklists	Wet signatures are easy to do. Wet signature users don't need higher education
It has legal force as regulated in government regulation number 82 of 2012 Article 53 paragraph (2)		
It is registered and regulated under the authorities		
It can be validated by all individuals concerned with the document		

The document integrity can be guaranteed		
In accordance with the digital lifestyle that is currently happening a lot, demands a more secure, practical, and efficient signature method		

Table 2.
Comparison of the disadvantages of certified digital signatures, uncertified electronic signatures, and ordinary signatures.

Certified digital signatures	**Non-certified electronic signatures**	**Ordinary signatures**
Requiring an official certificate is proof that an electronic signature can be legally recognized	The validity is questionable	Prone to be faked
It requires education in which not everyone knows technology	Relatively weak because it can still be accommodated by the person concerned or easily changed by others	Prone to be faked
The implementation is not easy		Prone to be faked

Whereas the implementation is still not in accordance with what is stated in government regulation number 82 of 2012 due to technical constraints that require basic knowledge of the application of a good electronic signature (digital signature);

2. Legal Requirements for the Operation of Electronic Systems and Transactions According to Government Regulation Number 82 of 2012.

The operation of electronic systems and transactions is said to be valid as long as it fulfills the requirements as stipulated in Article 41 paragraphs (1) to (3) of government regulation Number 82 of 2012 explaining that:

a. The implementation of electronic transactions in the public or private sphere using an electronic system for the benefit of public services must use a reliability certificate and or electronic certificate;
b. In terms of using a reliability certificate, the implementation of electronic transactions in the public sphere must be certified by a registered Indonesian reliability certification agency;
c. In terms of using electronic certificates, the implementation of electronic transactions in the public sphere must use the services of a certified Indonesian electronic certification provider.

Operators of electronic systems and transactions as stipulated in government regulation number 82 of 2012 article 1 point (14) are:
"a series of electronic transaction activities carried out by the sender and recipient using an electronic system". Government regulation Number 82 of 2012 in article 2 regulates several things, including

a. Electronic System Operation;
b. Electronic agent operation;
c. Electronic transaction implementation
d. Electronic signature;
e. Implementation of electronic certification;
f. Reliability certification body; and
g. Domain name management.

The implementation of the electronic system as described in government regulation Number 82 of 2012 article 3 paragraphs (1) to (3) concerning the operation of electronic systems and transactions states that:

a. The operation of the electronic system is carried out by the operator of the electronic system;
b. The operation of the electronic system as referred to in paragraph (1) can be carried out:
    1) Public services; and
    2) Non-public services;
c. The criteria for public services as referred to in paragraph (2) letter a refers to the provisions of the legislation

The electronic system operator as referred to in Article 3 paragraph (1) above covers the following arrangements:

a. Registration;
b. Hardware;
c. Software;
d. Experts;
e. Governance;
f. Security;
g. Electronic system feasibility certification; and supervision.

a. Registration:
    1) The operation of the electronic system for public services is required to register;
    2) Electronic systems for non-public services may register;
    3) The registration obligation for the electronic system operator for public services as referred to in paragraph (1) is carried out before the electronic system begins to be used by the public;
    4) Registration as referred to in paragraph (1) and paragraph (2) shall be regulated in a ministerial regulation;
    5) Further provisions regarding registration procedures as referred to in paragraph (1) and paragraph (2) shall be regulated in a ministerial regulation.

b. Hardware
    1) The hardware used by the electronic system operator must:
        a. Meet the aspects of interconnectivity and compatibility with the system used;
        b. Obtain a certificate of eligibility from the minister;
        c. Have technical support, maintenance, and after-sales services from both the seller and the provider;
        d. Have supporting references from other users that the hardware is functioning according to its specifications;
        e. Have at least 3 (three) years of essential spare parts availability guarantee;
        f. Have a guarantee of clarity about the condition of the new and;
        g. Has a warranty free from product defects.
    2) Electronic system operators must ensure the neutrality of technology and freedom of choice in the use of hardware;

3) The Minister shall determine the technical standard of hardware used by the electronic system operator;
4) Further provisions regarding hardware technical standards as referred to in paragraph (3) are regulated in a ministerial regulation (PP.82.2012).

c. Software

The software used by the electronic system operator for public services must:

1) Registered with the ministry that administers government affairs in the field of communication and informatics;
2) Guaranteed safe and reliable operation as appropriate, and
3) In accordance with the provisions of the legislation.

Further provisions regarding software requirements as referred to in paragraph (1) shall be regulated in a ministerial regulation. Furthermore, article 8 paragraphs (1) to (3) in the government regulation Number 82 of 2012 explains that:

a. Providers who develop software specifically made for an agency are required to submit the source code and documentation of the software to the agency concerned;
b. In the event that the submission of the source code and documentation of the software as referred to in paragraph (1) is not possible, the provider may submit the source code and documentation of the software to a trusted third party to store the source code;
c. The provider is obliged to guarantee the acquisition and or access to the source code and documentation of the software to a trusted third party as referred to in paragraph (2).

5. CONCLUSION

From the descriptions that have been described previously, it can be concluded that:

1. The legal power of digital signatures according to Government Regulation Number 82 of 2012. The electronic signature will have perfect legal force if it meets the elements described in Article 53 paragraph (2) of Government Regulation Number 82 of 2012 the elements of article 53 paragraph (2) of government regulation number 82 of 2012 then the implementation of electronic signatures (digital signatures) can be said to be juridical defects (legal defects).

2. Legal requirements for the operation of electronic systems and transactions according to Government Regulation Number 82 of 2012. In accordance with what is described in Article 41 paragraphs (1) to (3) of government regulation Number 82 of 2012 concerning the operation of electronic systems and transactions, as long as they fulfill these provisions then it can carry out the implementation of electronic transactions that are legal and very relevant to people's lives. It can also facilitate the public in conducting various electronic transactions. If users when conducting electronic transactions feel that their rights have been violated, they can make reports and complaints to the authorities in the field of information technology and electronic transactions in accordance with what is described in Article 43 paragraphs (1) to (5) of Law Number 19 of 2016 on the amendment to Law Number 11 of 2008 concerning information and electronic transactions.

Based on the conclusion of the study, the researcher recommends the following.

1. Regarding the legal power of electronic signatures, the need for socialization related to digital signatures by the government to all levels of society, especially in rural areas. There needs to be a definite and clear legal force for uncertified electronic signatures so that in their application they are used effectively.
2. Provisions of laws and regulations by users in conducting electronic transactions in order to obtain certain security and services.

References

Ahmaturrahman, 2005. Hukum Acara Perdata Di Indonesia, Fakultas Hukum Universitas Sriwijaya.

Din Mudiardjo, 2008*, Telekomunikasi Dan Teknologi Hukum E-commerce (grattan), www.google.com.*

Eka Nugraha Dkk, *EfektivitasPelaksanaan Sertifikasi Keandalan Website Jual Beli Online Dalam MenanggulangiPenipuanKonsumen*, Jurnal Cakrawala Hukum, Vol. 8 No. 2, (Desember 2017).

Herlien Budiono*, Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan, P*T.Citra Aditya Bakti, Bandung, 2007.

Husnul Hudzaifah, Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia, e-Jurnal Katalogis, volume 3 Nomor 5, (Mei 2015)

Menurut Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum*, PT. Citra Aditya Bakti, Bandung, 2004,.

Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 53 Ayat (1) Sampai (3)

Ronny, 2008, *Sembilan Peraturan Pemerintah Dan Dua Lembaga Yang Baru Undang-Undang Informasi Transaksi Elektronik*, *www.ronny-hukum.blogspot.com,*.

Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri,* Ghalia Indonesia, 1988.

Tan Thong Kie, *Studi Notariat dan Serba-Serbi Praktek Notaris,* PT. Ichtiar Baru Van Hoeve, Jakarta, 2007, Hal. 473

Julius Indra Dwipayono, 2005, *Pengakuan Tanda Tangan Elektronik Dalam Hukum Pembuktian Indonesia,* www.legalitas.org.