Proceeding of the 3rd Malikussaleh International Conference on Law, Legal Studies and Social Sciences (MICoLLS) 2023

LEGAL CONSEQUENCES OF MISUSE OF DIGITAL SIGNATURES IN BUSINESS TRANSACTIONS

1st Raina Dahlia
1st Malikussaleh University
raina.190510121@mhs.unimal.ac.id

2nd Manfarisyah
2nd Malikussaleh University
manfarisyah@unimal.ac.id

3rd Hamdani
3rd Malikussaleh University
hamdani@unimal.ac.id

ABSTRACT

A digital signature is essentially an electronic version of a traditional signature found on a physics document. In accordance with the ITE Law, a digital signature is a collection of electronic data that is connected, affiliated, or related to other electronic information. Its function is used as an authentication and verification method. The aim of this research is to examine the potential legal consequences arising from the use of inappropriate or unauthorized digital signatures in business transactions. This research uses normative juridical studies or uses library legal data. Library research is a study that focuses on users of secondary data or includes written legal norms and/or interviews with informants and sources. Regarding the legal impact of misuse of digital signatures in business transactions, it is important to remember that such misuse can result in losses for the person signing the document, it is important for them to comply with the requirements outlined in the relevant laws. In this case, a digital signature can be considered to have the same validity and legal consequences as a handwritten signature, provided that the identity of the individual associated with the digital signature is established with a high degree of certainty and that the signature itself was created, in accordance with article 27 verse (1), (2), (3) and (4) if related to Islamic law, where taking another person's rights without the owner's knowledge is an act that is prohibited by religion and is not recommended in the Shari'a.

Keywords: Legal consequences, signature, business transactions

1. INTRODUCTION

A digital signature is a way to guarantee the authenticity of an electronic document and ensure that the sender of the document cannot at any time deny that he or she has sent the document. A valid digital signature gives the recipient reason to trust that the message sent is from a known sender and has not been manipulated in transit. Digital signatures are unique so they are only opened with each other's key pairs(private and public) so that their existence is a measure or method of securing the transmission of information itself from the sender to the recipient.[1]

The act of validating or approving a document that is valid and recognized in a digital system is in the form of a digital signature, because a digital signature functions to authenticate and verify the identity of the signer as well as the authenticity of electronic information, not with a scanned wet signature embedded in the document or by signing it manually. directly in the document using the draw feature in Microsoft Word or PDF Reader because this cannot guarantee the validity or authenticity of electronic documents because using this method is easy to forge, therefore the right way is to use a digital signature.

The presence of digital signatures in electronic transaction activities is a direct result of a shift in the trading system, where in the past trading was more often paper-based, but now it has switched to paperless. This shift causes differences between the two, namely that paper-based transactions often involve various kinds of fraud, where signatures can still be forged and paper documents can be changed,even stamps, code impressions, stamps and seals that should be safe can still be faked, and can even have double functions. namely guaranteeing the authenticity and integrity of the data/message while also providing a glimpse of the contents of the data/message regarding the identity of the person who signed it during the transmission process.
[2]
Legal problems arise when there is a dispute between parties who dispute the issue of the authenticity of data/messages which usually take the form of digital signatures before the court as evidence. In fact, in electronic commerce, a digital signature is not in written (real) form like a conventional signature on a certain document/deed, but in the form of a mathematical equation created digitally. Usually,when a case occurs, in a civil trial, paper as a company document is the main evidence, because in civil cases people often deliberately provide evidence that can be used if a dispute occurs and the evidence provide dis usually in written form.

Digital signatures in terms of evidence in court can refer to Article 5 paragraphs (1), (2), (3), and(4) of Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law) , States that:
(1) Electronic information and/or electronic documents and/or printouts are valid legal evidence;
(2) Electronic information and/or electronic documents and/or printouts as intended in paragraph (1) are an extension of valid evidence in accordance with the procedural law in force in Indonesia;
(3) Electronic information and/or electronic documents are declared valid if an electronic system is use din accordance with the provisions regulated in this law
(4) Provisions regarding electronic information and/or electronic documents as intended in paragraph (1)do not apply to

[1] Edmon Makarim, Notary and Electronic Transactions, Jakarta, Raja Grafindo Persada, 2013, p. 5
[2] Ono W. Purbo and Aang Arif Wahyudi, Getting to Know E-Commerce, Jakarta, PT. Elex Media

Computindo, 2007, p. 36.

a. letters which according to law must be made in writing;
b. a letter and its documents which according to law are made in the form of a notarial deed or a deed made by a deed-making official.

Article 5 paragraph 2 of the ITE Law states that "Electronic Information and/or Electronic Documents and/or obtaining printed copies are extensions of evidence from valid penitentiary instruments based on the Procedural Laws that take place in Indonesia". However, specifically for Electronic Information and/or Electronic Documents, such as obtaining interception or surveillance or recording which is part of wiretapping, it must be carried out in the context of enforcing legal regulations at the request of the police, prosecutor's office and/or other agencies whose powers are determined based on the Law. The validation capacity of an electronic document signed using an electronic signature is equal to the validation capacity of an authentic certificate made by a competent general authority.[3]

This research has a main focus on the misuse of digital signatures used in business transactions,in which case there is often misuse of digital signatures for purposes of carrying out business transaction sand resulting in losses for other people, resulting in legal consequences arising from misuse of digital signatures. the. In this case, the government has provided legal protection efforts for electronic transactions through the Information and Electronic Transactions Law.

The use of digital signatures is not only applied in the public environment between state officials but is also commonly practiced in aspects of business and commerce. Effectiveness, efficiency, fast and cheap are the reasons for business people and public agencies to optimize this method. However, this practice is still faced with legal status if it is needed as evidence. The weakness of digital innovation is that it is easy for hacking to occur from various regions, making it possible for misuse of these signatures in the future. Civil procedural law is a game rule that only applies and is binding on players in the judicial game,namely judges and justice seekers. Because it is a game rule that must be obeyed, then the regulations must be imperative, binding, and must not be deviated from, so that through the courts a legal certainty is create din the application of the law in addition to justice and expediency. [4]

Based on the background description above, it is very necessary to carry out legal research to overcome the problem of misuse of digital signatures in electronic business transactions. This legal research can be a real contribution to the legal study of e-commerce in Indonesia, which is still very lacking.

On this basis, the author raises this issue in a thesis entitled Analysis of Misuse of Digital Signatures in Business Transactions According to the ITE Law in Indonesia.

---

[3] Sulma, K. Jamaluddin. Rahman, A. The Validity of Electronic Signatures and Their Strength of Proof in Civil Procedure Law, Student Scientific Journal (JIM), Vol. V, Number 3, (November 2022): 33. https://doi.org/10.29103/jimfh.v5i3.7107.

[4] Saragih, M. Afrizal, T. & Herinawati, Implementasi Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan Secara Elektronik (Studi Penelitian di Pengadilan Negeri Lhokseumawe). Vol. 5, Nomor 2, (April 2022): 53. https://doi.org/10.29103/jimfh.v5i2.7000.

Article 11 states that an electronic signature has legal force and legal consequences as long as it fulfills the following requirements: (a) the electronic signature creation data relates only to the signer; (b)electronic signature creation data during the electronic signing process is only within the control of the signatory; (c) any changes to the electronic signature that occur after the time of signing can be known; (d)any changes to the electronic information related to the electronic signature after the time of signing are known; (e) there is a certain method used to identify the signatory; and (f) there is a certain way to demonstrate that the signatory has given consent to the relevant electronic information.

Based on the provisions of Article 13, it shows that the minimum requirements that a digital signature must fulfill before it can enjoy the "principle of presumption of reliability" which gives it the same legal force and legal consequences as a manuscript signature. The use of the words "electronic signature creation data" should be simplified to "digital signature", so that it is clearer and easier to understand because there is no digital signature without data.

RESEARCH METHODS

The issues that will be studied are the legal strength of digital signatures in business transactions from the perspective of the ITE Law and the legal consequences of misuse of digital signatures in business transactions. The research method used by the author is a normative legal research method. Normative legal research is legal research that places law as a building system of norms.[5]

The approach method used is the statutory approach method. The statutory approach is used to understand all legal regulations (Johnny Brahmin, 2006: 321). This research is guided by existing laws and regulations and theories relating to consumer protection.

RESEARCH RESULTS AND DISCUSSION

A signature is a sign as a symbol of a name as commonly used, including initials, signature stamps or initial stamps as a substitute for a signature. According to Article 1 Paragraph (12) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, an electronic signature is a signature consisting of electronic information that is attached,associated or related to electronic information.

Other Electronic Information is one or a collection of electronic data, including without limitation writing, sound, images, maps, plans, photos, electronic data interchange (EDI), electronic mail, telegram,telex, telescope, while what is meant by Electronic Document is any Electronic Information that is created,forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form, which cane seen, displayed, and/or heard via a computer or electronic system.[6]
Digital signatures can actually provide more guarantees for document security than regular signatures. Recipients of digitally signed messages can check whether the message actually came from the correct sender and whether the message was altered after being signed, either intentionally

[5] Zainuddin Ali, Legal Research Methods, Jakarta, Sinar Graphics, 2009, p. 105. Ridwan, Nur. M, & Sulaiman. Criminal Liability

[6] Ridwan, Nur. M, & Sulaiman. Criminal Responsibility for Perpetrators of Hacking Crimes (Hackers) in Law Number 19 of 2016 concerning Electronic Information and Transactions, Student Scientific Journal (JIM), Vol. vi, Number 1, (January 2023): 118.
https://doi.org/10.29103/jimfh.v6i1.7007

or unintentionally. In other words, digital signatures can provide a guarantee of the authenticity of documents sent digitally, both guarantees about the identity of the sender and the veracity of the document.

If someone sends a digitally signed message to another party, he creates the contents of the document in a format that is a "digital fingerprint" of the document. Digital signatures allow recipients of information to first test the authenticity of the information obtained and also to ensure that the data they receive is intact.

A digital signature is in the form of a virtual signature, meaning that it is a signature that is executed in scanned form by an authorized official. This is very risky because anyone who has the signature can use it without any authentication or proof that the official has given the signature. To be able to have legal force and valid legal consequences, the electronic signature must meet the requirements in Article 11paragraph (1) The ITE Law, namely:
1. Electronic signature creation data relates only to the signatory;
2. Electronic signature creation data during the signing process is only within the control of the signatory;
3. Any changes to the electronic signature that occur after the time of signing can be known;
4. Any changes to the electronic information related to the electronic signature after the time of signing cane known;
5. There are certain methods that can be used to identify who the signatory is; And
6. There are certain ways to show that the signatory has given consent to the relevant electronic information.

Certified digital signatures that use electronic certificates provide a guarantee of trust for the owner, namely in the form of data authenticity, by showing the identity of the certificate owner in the electronic document, integrity so that activity in the electronic document that has been signed can be monitored, and guarantees non-refutation, namely proof of the truth of the signing. cannot deny having carried out electronic transactions. However, even though digital signatures have made efforts to use electronic certificates, acts of forgery or misuse of digital signatures are still ongoing.

If misuse of digital signatures is brought into the realm of law, it can be caught in Article 263 of the Criminal Code with a maximum penalty of 6 years in prison. This shows that identity validation, either directly or digitally, is often a problem and has quite high criminal potential. Especially in the digital realm,with technological advances that are evolving to become more sophisticated day by day. Therefore, to avoid misuse and even forgery of digital signatures, it is necessary to understand the importance of the verification and authentication process so that the signed file is truly carried out by the owner of the document, so the signature must consist of encrypted electronic information in the form of an electronic certificate issued by Electronic Certificate Provider (Pare).

Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number11 of 2008 concerning Information and Electronic Transactions provides express recognition that electronic signatures have legal force and legal consequences as long as the electronic signature complies with the requirements stated in Article 11 of the ITE Law which is a minimum requirement and must be fulfilled in every digital signature, the level of security of an electronic signature will be guaranteed if it hasan electronic certificate containing information or identity of the user. The electronic certificate is obtained on the basis of an application to the Certification Authority (CA) by the user (subscriber)

The establishment of legislation that specifically regulates digital signatures is very beneficial for digital signature users in carrying out business transactions electronically. Apart from that, the formation of an electronic signature is also supported by fingerprints as authentication and verification which will reference the original document that will be signed. If the verification and authentication stage shave been carried out, it will be known that the document that has been created and will be signed corresponds to the private key that is owned. After a digital signature has been carried out, and you want to make changes, you must first report it to a third party. Therefore, this can prevent fraud from parties if they want to misuse documents or electronic signature.[7]

Electronic business transactions in Article 1 point 2 of the ITE Law are legal actions carried out using computers, computer networks and/or other electronic media. The existence of an agreement in electronic transactions carried out by business actors and consumers creates a contract or legal relationship between the parties. If the consumer agrees to the terms and clauses proposed by the seller,then an agreement is entered into even though the sale and purchase agreement is agreed via an electronic signature.

A digital signature is often confused with a signature on paper and then through a scanning process, the signature is entered (input) into the computer so that it becomes a signature image which is then attached to a document to state that the document "has been signed". It is not uncommon for a digital signature to be understood as a signature made directly on a computer using a mouse so that it takes the form of a signature like a signature on paper.

Legal force and legal consequences, electronic signatures are equated with manual signatures sin the explanation of Article 11 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. In Article 1874 paragraph (1) of the Civil Code and other articles in the Civil Code which mention signatures, there is no further explanation regarding the meaning of signature. By signing, it shows that the signer agrees to the information or electronic document he is signing and at the same time guarantees the correctness of the contents contained in the writing.

The purpose of a digital signature in a business transaction document is to ensure the authenticity of the document. A digital signature uses a different way to mark a document, so that the document or data not only identifies the sender but also ensures that the integrity of the document doesn't change during the sending (transmission) process. The benefit of using a digital signature applied to messages or electronic data sent is that it can guarantee that the message or electronic data has not undergone any changes or modifications by unauthorized parties.

based on the description above, digital signatures have the same legal force in court as conventional signatures in deeds made by the parties as stated in Article 11 of Law Number 19 of 2016concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.Referring to Article 5 paragraph (4), it is known that documents made in the form of notarial deeds are not included in electronic information and/or electronic documents. On the other hand, electronic document information cannot be used as an authentic deed. Notaries as public officials who have the authority to make authentic deeds in this context only legalize digital signature.

[7] Agus R., Cybercrime, Understanding and Efforts to Prevent Technological Crime, Bandung, Citra AdityaBakti, 2007, p. 91.

After the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law Number 19 of 2016, there were developments in the law of evidence.Whereas previously electronic evidence could only be used as presumptive evidence in civil cases or as indicative evidence in criminal cases, then with the issuance of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016, electronic documents and their printouts were expressly recognized. as valid evidence in court as long as it is also stated that electronic information and electronic documents can bused as evidence in court. However, any electronic information/document can be used as evidence at trial.As evidence, electronic documents or electronic information must be valuable, that is, they can explain situation.

An electronic signature can only be said to be valid if it uses an electronic system that complies with the regulations in force in Indonesia. Electronic evidence, in this case an electronic signature, can have legal force if the integrity of the information can be guaranteed, can be accounted for, can be accessed and can be displayed, thus explaining a situation. The person submitting electronic evidence must be able to show that the information they have comes from a trusted electronic system. Legal efforts to resolve disputes regarding electronic transactions where electronic documents are signed with an electronic signature are based on an agreement between both parties regarding the choice of law and institution to resolve the problem that occurs. As is generally the case, disputes in transactions occur because of losses suffered by one of the parties, either due to default or because of unlawful acts. Dispute resolution through public justice institutions takes a lot of time, money and energy. Meanwhile, settlement through arbitration does not take time, money and energy when compared to settlement through general court.

In general, if you encounter a problem and have to make the right decision regarding the problem, you first try to gather various facts related to the problem. The collected facts are used to prove the problem and find a solution. Therefore, in order to have full penitentiary power in a trial, it is appropriate that when presenting a fact, the party submitting the fact should submit evidence as an Authentic Deed.

The administrative sanctions that can be applied for misuse of digital signatures in business transactions at an early stage are by providing a written warning to the party who misuses them and can urge them to correct the violation/misuse of the digital signature. In cases of serious misuse of digital signatures, processing activities related to digital signatures may be temporarily stopped. Abuse of data protection regulations may result in requirements to delete or destroy personal data obtained through noncontroversial signature activities. Therefore, those who abuse may be subject to administrative fines calculated based on the severity of the abuse violation.

Telugu Samurai is of the opinion that proving is explaining or stating the actual legal position based on the judge's belief in the arguments put forward by the parties to the dispute. In the academic text of the draft law on electronic signatures and electronic transactions, it is stated that proving is an effort to collect facts that can be analyzed from a legal perspective and are related to a case which are used to give judges confidence in making decisions, while proof is the process of proving a case accompanied by facts that can be analyzed from a legal perspective to give the judge confidence in making a decision.

After the issuance of Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law Number 19 of 2016, there were developments in the law of evidence.Whereas previously electronic evidence could only be used as presumptive evidence in civil cases, then with the issuance of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016, electronic

documents and their printouts are expressly recognized as valid evidence in court. provided that it is also stated that electronic information and electronic documents can be used as evidence at trial. However, any electronic information/document can be used as evidence at trial. As evidence, electronic documents or electronic information must be valuable, that is, they can explain a situation.

An electronic signature can only be said to be valid if it uses an electronic system that complies with the regulations in force in Indonesia. Electronic evidence, in this case an electronic signature, can have legal force if the integrity of the information can be guaranteed, can be accounted for, can be accessed and can be displayed, thus explaining a situation. The person submitting electronic evidence must be able to show that the information they have comes from a trusted electronic system.

Legal efforts to resolve disputes regarding electronic transactions where electronic documents are signed with an electronic signature are based on an agreement between both parties regarding the choice of law and institution to resolve the problem that occurs. As is generally the case, disputes in transactions occur because of losses suffered by one of the parties, either due to default or because of unlawful acts. Dispute resolution through public justice institutions takes a lot of time, money and energy.Meanwhile, settlement through arbitration does not take time, money and energy when compared to settlement through general court.

In general, if you encounter a problem and have to make the right decision regarding the problem, you first try to gather various facts related to the problem. The collected facts are used to prove the problem and find a solution. Therefore, in order to have full penitentiary power in a trial, it is appropriate that when presenting a fact, the party submitting the fact should submit evidence as an Authentic Deed.

An authentic deed is a deed made in a form determined by law by or before a public official whops authorized in that place. It can be concluded that the form is in writing, made by or in the presence of unauthorized official or public employee. The official referred to here is a person who has authority because on the basis of his position he is appointed by the state, for example the notary profession or PPAT (Land Deed Official).

There is one thing that should be considered in recognizing an electronic document signed with digital signature, namely the security of a system and the involvement of people in the computer system.Meanwhile, the existence of an electronic signature in an electronic document must be recognized as having the same legal force and legal consequences as a signature in other written documents. This starts from the understanding that electronic documents have legal force as evidence and the same legal consequences another written documents.

So that an electronic signature on an electronic document can have penitentiary power in court,the digital signature must be registered with the Certification Authority (CA). So the CA can act as a public official, thereby utilizing the infrastructure provided by the CA, especially the ability to know when an electronic business transaction was signed. Digital signatures that have received a certificate from the Certification Authority will be more guaranteed to be authentic, and digital signatures are very difficult to forge.

Using a digital signature requires two processes, namely from the signatory and the recipient. In detail these two processes can be explained as follows:
1) Formation of a digital signature using a special value generated from the document and a previously defined private key. To be able to guarantee the security of a particular value, there should

be a very small possibility that the same digital signature can be generated from two different documents and private keys.
2) Digital signature verification is the process of checking a digital signature by referring to the original document and the public key that has been provided, in this way it can be determined whether the digital signature was created for the same document using a private key that corresponds to the public key.

To sign a document or other piece of information, the signer first defines exactly which part swill be signed. This restricted information is called "message". Then the digital signature application will form the hash value into a digital signature using the private key. The digital signature formed is unique for both the message and the private key.

Generally a digital signature is included with the document and is also saved with the documents well. Digital signatures can also be sent or saved as separate documents, as long as they can still be associated with the document. Because digital signatures are unique to the document, separating digital signatures like this is unnecessary.

The process of creating and verifying a digital signature fulfills the most important elements expected for a legal purpose, namely:
1) Authentication of the signer, if the public key and private key pair are associated with a defined legal owner, then the digital signature will be able to connect or associate the document with the signer. Digital signatures cannot be forged, unless the signer loses control of their private key.
2) Document authentication, namely digital signatures, also identify signed documents with a much higher level of certainty and accuracy than signatures on paper.
3) Confirmation, creating a digital signature requires the use of the signer's private key. This action can confirm that the signer agrees and is responsible for the contents of the document
4) Efficiency is the process of creating and verifying a digital signature that provides a high level of certainty that the existing signature is a valid and genuine signature of the owner of the private key.

The purpose of signing a valid document must have the following attributes: First, authenticate the signer. A signature should be able to identify who signed the document and be difficult for others to imitate. Second, document authentication, a signature should identify what is being signed, making it impossible to forge or change (both the signed document and the signature) without being noticed.Authentication of signers and documents is a tool to avoid forgery and is an application of the concept of"non repudiation" in the field of information security. Non repudiation is a guarantee of the authenticity or delivery of the original document to avoid denial by the signer Article 5 Paragraph (1) to Paragraph (3) of the ITE Law, explicitly states: electronic information and/or electronic documents and/or printouts are valid legal evidence and are an extension of valid evidence in accordance with the procedural law. applies in Indonesia in accordance with the provisions regulated in law. However, in Paragraph (4) there is an exception which states that electronic information and/or electronic documents do not apply to: (a) letters which according to law must be in written form;and (b) letters and documents which according to law must be made in the form of a notarial deed or deed made by a deed-making official.

Regulations regarding electronic signatures in Indonesia before the enactment of the ITE Law can be found in Article 10 paragraph (6) of Law Number 40 of 2007 concerning Limited Liability

Companies(UU PT)[8], 8which regulates electronic signing by the Minister of Law and Human Rights of ratification liability company. Therefore, this digital signature can be defined as a signature that is included or attached to electronic data by an official who has authority and can prove the authenticity and authenticity of detain the form of an electronic image, from the signature of an official who has authority, which is made using media. computer. It can be said that a digital or electronic signature is in the form of a virtual signature,meaning that it is a signature that is executed in scanned form by an authorized official. This is very risky because anyone who has the signature can use it without any authentication or proof that the official has provided the signature.

Electronic evidence is increasingly appearing in practice in society, for example e-mail, witness examination using video teleconference, short message service systems (SMS), hidden camera recordings(CCTV: closed circuit tel vision), electronic information, electronic tickets, electronic data/documents another electronic means as data storage media. An instrument that can be used to determine the authenticity or validity of electronic evidence in the form of documents or electronic information is a digital signature.Digital signatures aim to ensure the authenticity of a document in an electronic transaction and ensure the integrity of the contents of the document does not change during the delivery process.

The legal consequences of misuse of digital signatures in business transactions are that if therein misuse of digital signatures in business transactions, it will cause material losses to parties signer, therefore, to avoid misuse of digital signatures, they must fulfill the requirements in accordance with the provisions of Article 11 of the ITE Law. In this case, digital signatures can be recognized as having the same legal force and legal consequences as manuscript signatures with the condition that the legal subject related to this digital signature must be able to be identified very convincingly, and this digital signature is created and stored in conditions that guarantee its integrity.

As a Muslim, you need to be careful in obtaining sustenance. Don't let the good fortune you getbe obtained through false methods such as taking other people's rights.

For example, someone who builds a company by taking other people's land and claiming that the land is his or in other cases such as corrupting funds that should be channeled for the benefit of the community, and so on. Because in reality, people who take other people's rights will suffer misery on the Day of Judgment. As the hadith of the Prophet Muhammad:

وَقَالَ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ: مَنْ أَخَذَ مِنَ الْأَرْضِ شِبْرًا بِغَيْرِ حَقِّهِ خُسِفَ بِهِ يَوْمَ الْقِيَامَةِ إِلَى سَبْعِ أَرَضِينَ.

The Prophet said, "Whoever takes an inch of land that is not his right, he will surely be drowned on the Day of Resurrection to the depths of the seven layers of the earth." (HR Bukhari).

The Law of Taking Other People's Rights Based on the book Usu Fish of Sharia Economic Law by Imron Rosyadi et al (2020: 278), taking other people's rights is harm. Allah SWT says in Surat An Nisa verse 29:

[8] Article 10 Paragraph (6) of Law Number 40 of 2007 concerning Limited Liability Companies: "If all the requirements as intended in paragraph (5) have been fulfilled completely, no later than 14 (fourteen) days, the Minister shall issue a decision regarding the legalization of the Company's legal entity electronically signed."

يأَيُّهَا الَّ ذينَ ءَامَنهوا لَتأَه كُلهوا أَمْوَالَ هكم بيْنَ هكم بألْبَا ط لَ

O you who believe! "Do not consume each other's wealth in a false way," (QS. An Nisaa': 29)

Rasulullah SAW also prohibited his people from taking other people's rights without permission.In fact, the Prophet really hated this act. As in the History of Bukhari, the Prophet said:"Allah SWT said that there are three types of people who will fight against them on the Day of Judgment.Those who swear in the name of Allah but deny it, someone who sells with three people but they take the money from the price, and someone who employs and then does not pay his wages.

"The reason why it is forbidden to take other people's rights is also explained in the Hadith narrated by Abu Daud and Dartmouth, that it is not halal to take the rights/property of a Muslim, unless that person is willing.If someone dares to take another person's rights, that person will suffer a huge loss. The reason is, he willnot only experience torment in this world, but also the torment in the afterlife that awaits him.According to the word of Allah SWT in Surah Al Baqarah verse 188, it is explained that

وَلَ تأَ هكْلهوْا امْوَالَ هكمْ بَيْنَ هكمْ بالْبأَ ط لَ وَتهدلْهوْا بهأَ الَى الْ هحكَّا مَ لتأَ هكْلهوْا ف ريْقاً منْ امْوَا لَ النأَ سَ با لْث مْوَانْتهمْ تعْلَ همونَ

meaningless: "And do not eat the wealth between you in a false way, and (don't) you bribe the judges with that wealth, with the intention that you can consume some of other people's wealth in a sinful way, even though you know.

"Regarding this prohibition, in the Hadith History of Muslim explains that Baha'ullah SAW said: "Whoever takes away the rights of a Muslim with his oath, Allah determines hell for him. Then, forbids heaven for him.

There was a man who asked the Prophet SAW: Even though this is a very simple, O Messenger of Allah?Then the Prophet Muhammad SAW answered: Even if it is a piece of Shiva wood from the arak tree.

"Likewise, misuse of digital signatures in business transactions can also be categorized as an act that is prohibited by religion. Misusing other people's digital signatures can also result in losses for someone who misuses their signature and can also cause someone to fall into actions that are prohibited by religion.

AUTHORS' CONTRIBUTIONS

OUR ROLE INVOLVED IN THE PROCESS OF PRODUCING THIS SCIENTIFIC ARTICLE IS ASFOLLOWS:
1. RAINA DAHLIA THAT IS, AS THE MAIN WRITER IN THIS ARTICLE WHO SERVES A ROLE AS A WRITER
2. MANFARISYAH THAT IS, IN GUIDING ME IN THE CREATION OF THIS ARTICLE AND PARTICIPATING INMY SCIENTIFIC FINISHING OF CHAPTERS II AND III AS WELL AS ASSISTING IN CORRECTING THECONTENTS OF THIS ARTICLE STARTING FROM THE DISCUSSION TO THE BIBLIOGRAPHY
3. HAMDANI THAT IS, IN GUIDING ME IN THE CRAFT OF THIS ARTICLE REGARDING THE CONTENTS ANDFOOTNOTES, AND PARTICIPATING IN MY SCIENTIFIC RESEARCH FOR CHAPTERS II AND III ANDASSISTING IN CORRECTING THE CONTENTS OF THIS ARTICLE STARTING FROM THE DISCUSSION TO THEBIBLIOGRAPHY

ACKNOWLEDGMENTS

I SAY THANK YOU TO MOTHER Dr. MANFARISYAH., S.H M.H. WHICH HE AS MY MAIN SUPERVISOR HAS HELPED A LOT IN THE CREATION OF THIS ARTICLE WHO ALWAYS TAKES HER TIME IN GUIDING THIS ARTICLE AND I ALSO SAY THANK YOU TO Mr. Dr. HAMDANI S.H., LL.M. WHICH HE ALSO HELPED ME IN MAKING THIS ARTICLE, WHO HAS PASSED A LOT OF TIME IN MAKING THIS ARTICLE, FOR THE LECTURERS OF MALIKUSSALEH UNIVERSITY, FACULTY OF LAW, BOTH FROM THE ACADEMIC PARTY AND THE ENTIRE STAP OF EMPLOYEES WHO HELPED ME, BOTH ACADEMIC AND NONACADEMIC, I ALSO SAY THANK YOU TO ON MY FAMILY ESPECIALLY MY PARENTS WHO HELPED AND SUPPORTED ME MUCH IN ANY SITUATION UNTIL THIS ARTICLE WAS RELEASED, I DON'T FORGET TO SAY THANK YOU TO MY FRIENDS WHO ARE ALWAYS BESIDE ME IN ANY CONDITION

REFERENCES

Asnawi, H. E-Commerce Business Transactions from an Islamic Perspective. Moldings I, Yogyakarta: Magistra Insania Press, 2004.

Budiono, H. Collection of Civil Law Writings in the Field of Notary Affairs. Bandung: PT. Citra Bandung Aditya Bakti, 2007

Budhijanto, D. in IT Law., FCBArb. Indonesian Cyberlaw Revolution Update and Revision of the 2016 ITE Law, PT Refika Aditama. 2017.

Eddy O.S. Hiariej. Theory and Law of Evidence. Jakarta: Erlangga, 2012.

Makarim, E. Notaries and Electronic Transactions. Jakarta: Raja Grafindo Persada, 2013.

Makarim, E. Compilation of Telematics Law. Printing 1, Edition 1, Jakarta: Raja Grafindo Persada, 2003.

Hadikusuma, H. Methods for Making Legal Science Working Papers or Theses. Bandung: Mandar Maju. 1995.

Haris. Legal Aspects of Electronic Transactions in the Capital Market. Jakarta: Grasindo, 2000.

Ibrahim, J. Theory and Methodology of Normative Legal Research. Malang: Bayu Media, 2006

Ono W. Purbo and Wahyudi, A. Getting to Know E-Commerce. Jakarta: PT. Elex Media Computindo, 2007.

Marzuki, M. Legal Research. Jakarta: Raja Grafindo Persada, 2011.

Rick Wiebe, Jurisdiction. E-Commerce and The Law Seminar. Bandung: Citra Aditya, 2002.

Ridwan, Nur. M, & Sulaiman. Criminal Responsibility for Perpetrators of Hacking Crimes (Hackers) in Law

Number 19 of 2016 concerning Electronic Information and Transactions, Student Scientific Journal (JIM),

Vol. vi, Number 1, (January 2023): 113-123.

https://doi.org/10.29103/jimfh.v6i1.7007.

Saragih, M. Afrizal, T. & Herinawati, Implementation of Supreme Court Regulation Number 1 of 2019 concerning Electronic Administration of Cases and Trials in Court (Research Study at

Lhokseumawe District Court). Vol. 5, Number 2, (April 2022): 52-63. https://doi.org/10.29103/jimfh.v5i2.7000.

Soerjono Soekanto and Sri Mamudji. Normative Legal Research A Brief Overview. Jakarta: Raja Grafindo Persada, 2001.

Sulma, K. Jamaluddin. & Rahman, A. The Validity of Electronic Signatures and Their Proof of Strength in Civil Procedure Law, Student Scientific Journal (JIM), Vol. V, Number 3, (November 2022): 29-38. https://doi.org/10.29103/jimfh.v5i3.7107.