Legal Issues Related to Listening to Digital Evidence in Civil Cases

Visitsak Nueangnong[1], Thitirat Itthimechai[2] and Songporn Pramarn[3]

Article History

Received: 02-10-2022

Revised: 31-10-2022

Accepted: 01-11-2022

Abstract

The world has evolved into a digital era of communication, transactions, and almost all of life. Most human beings need to use relevant electronic devices to make transactions and do those things, including data access, collection, and transmission, more accessible and faster. As a result, it is another channel for criminals to use to commit crimes. Civil digital evidence is unique in that it can easily alter, and that amendment can damage information. It allows digital evidence to be credible and listenable in judicial and judicial processes. Therefore, dealing with digital evidence requires a standardized, universally accepted, and reliable method. In particular, the various technical guidelines for dealing with digital evidence. The researcher has presented a guideline to amend and add to the Thai jurisprudence method and clearly define electronic data to clarify what kind of evidence. It is classified as prescribing rules and procedures for an inheritance to have specific characteristics to suit the complex nature of electronic evidence that will directly affect the use of electronic contracts as evidence, including the determination of the authenticity and completeness of electronic data. It is because the state of electronic data can be easily changed and modified by having a specific body established to ensure electronic data. It will be used as evidence to provide credibility, and information has not been modified or altered, including learning, and developing processes related to digital evidence in civil cases. It can determine the work direction that creates credibility and can be used in the judicial process. It is for Thailand to have a law relating to the adequate hearing of witnesses. As a result, the law on hearing digital evidence in civil cases will be more accepted and credible.

Keywords: Digital evidence, Electronic data, Evidence, Judicial process

INTRODUCTION

In civil cases, evidence is essential and necessary to prove the truth in court. The court will use knowledge and ability to make decisions in law and apply discretion in diagnosing evidence in cases. As the world evolves into a digital age, electronic evidence is information or information that can be useful for investigations stored in electronic devices such as computers, cell phones, etc., or sent to another source. Such evidence will only occur when data or electronic devices have been collected and stored. Electronic forensic evidence can be easily

[1-3] Lecture, Faculty of Law, Rambhai Barni Rajabhat University

E-mail: Visitsak.n@rbru.ac.th *Corresponding author

sent across other countries worldwide and quickly through the network. Its fragile state can be more easily altered, destroyed, or damaged than different types of evidence. (Kritsana Changklom, 1999)

There are several types of electronic or digital information, each of which may contain information that may be useful in criminal investigations and used as evidence to prove the guilt of an accused person. The Law Reform Consultants have broadened the definition of computer data and other digital or electronic forms of information, including audio files, backup audio files, files, e-mail or e-mail system history files, backup e-mail files, deleted e-mail temporary data files, website information stored in the form of text, images, or audio, website logs, cache files, cookies, and other information held by electronic devices. (Kramon Thongthammachat & Sombun Suksamran, 2003)

Currently, most people adopt digital technologies in their daily lives. Some parts of the technology could lead to more sophisticated forms of crime. There is the appearance of severe acts like transnational crimes. It threatens the stability of sovereignty, and economic strength or technology has become a tool for committing crimes. On the other hand, digital technology has produced a lot of evidence that "digital evidence" means information that is kept on a storage medium or is in the process of sending and receiving by electronic means, which can be used as reference evidence. (Electronic Transactions Development Agency, 2016)

In conclusion, the chances of us finding digital evidence are even more significant when technology is more advanced. The scope of computer forensics has been forced to expand to include other types of electronic data that are created by countless devices. We can say that digital evidence begins in the form of electronic information. It may come from transactions, documents, or certain types of media. Transactions and electronic data become digital evidence once saved somewhere accessible by some method and recoverable by the forensic investigator. (Sunee Sakawrat, 2016) As mentioned above, digital evidence has a broader meaning than computer evidence and is considered new and essential. But also facing issues of legislation, digital evidence collection, and the problem of listening to digital evidence, which may deteriorate the credibility of such evidence and affect the trial on three issues:

1) Legislative concerns.

2) Problems obtaining and collecting evidence.

3) Problems in listening to digital evidence.

OBJECTIVES

1. To study the history, meaning, concepts, and theories related to the law of digital evidence and provisions relating to the hearing of digital witnesses.

2. To study the problem of acquiring and collecting digital evidence in civil cases under Thai and foreign law.

3. To study the problem of listening to digital evidence in civil cases according to Thai and foreign law.

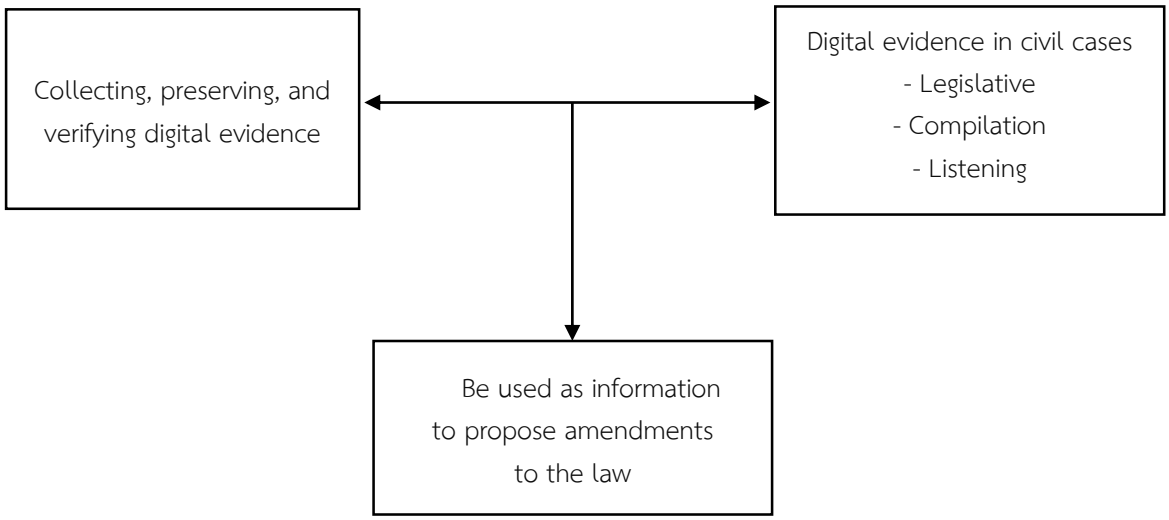
4. To find solutions and have legal measures for hearing digital evidence in civil cases.

RESEARCH DESIGN

Conceptual frameworks of the research project

The provisions of the Civil Procedure Code regarding digital evidence remain problematic and barriers to law enforcement. Due to technology developing rapidly, causing more digital evidence is causing problems with digital evidence, such as the problem of categorizing evidence. Digital evidence is classified as a type of evidence " documented evidence" or " objective evidence", issues with collection, storage, and verification, and the problem of listening to digital evidence in the case of authenticity or the originality of the document, as well as the issue of digital evidence as evidence obtained from wrongful actions. If the provisions of

the said law are amended. This will make listening to digital evidence more efficient and complete.



REVIEW OF LITERATURE

Theory, evolution, and infrastructure of digital evidence

Evidence law deals with the methods of presenting and researching facts to enforce substantive laws properly. Thailand's evidence law divides evidence into different types and criteria for evidence, setting the burden of proof, legal presumption, and witness testimony and weighing each type of evidence. There are measures to prevent attacks on witnesses in order not to take advantage of the lawsuits. That gives the court's discretion to cut off extravagant witnesses or delay the case. Witness law allows litigants to bring evidence to prove the facts in a case. But there must be limitations for selecting quality evidence of origin (authentication) to be the best evidence related to the case issue. As evidence that must not be forbidden to be heard, evidence is presented under the legal process to avoid taking advantage of the case. And to prevent delaying the issue by offering too much extravagant evidence, they should bring forensic evidence to prove the truth in the case. At the same time, the evidence law still intends to protect the people's rights and freedoms and to control government officials' actions in exercising their power to seek evidence using wrongful acts and infringing on the rights of the people. The system for considering and taking witnesses under witness law is a process of finding out the truth (a fact-finding process). But cannot guarantee that the court will decide the case according to reality. A process can only occur if the court has received the cooperation of the parties and those involved in the case: witnesses and those involved in the case, such as the possessor of expert evidence in various disciplines. The witness law only ensures that the court will consider taking evidence through fair play, selecting only the best evidence that can be obtained as evidence obtained by right and without taking advantage of each other in the case. The court's judgment must be accurate, fast, efficient, and just.

Weighing evidence in civil cases

Investigating witnesses in civil cases is considered part of the adversary system. Because a civil case is a civil claim, each party must protect its interests. The court will determine which side's witness has more weight (preponderance). The party with more weight will win the case.

According to the Criminal Procedure Code, Section 46 states that “ in the judgment of civil

cases, the court is obliged to hold the facts as they appear in a criminal case." Weighing court evidence in civil cases is not very common because the facts must bind it in a criminal case. There is Section 42 stipulates as an additional chapter in a civil trial. If the evidence attested in a criminal case is insufficient, the court may summon other evidence for further investigation.

There are also exceptions to group trials under Section 222/7 (2) of the Civil Procedure Code, which is a civil case related to a criminal case in a group litigation. In the case where the judgment in the criminal case determines that the defendant has not committed an offence, the courts that conduct group trials are not obliged to hold the facts accordingly. (Pattharasak Wannasaeng, 2022)

The fruit of a poisonous tree

The principle of cutting off the evidence obtained from the search without good reason or from investigations of coercion or acts of government officials violating the rights and freedoms of the people must be excluded from the proceedings. It confirms the principle that the evidence law is a provision that can protect the rights and freedoms of the people. In the Judiciary of the United States, the conduct of police officers must be pure and according to the law. The U.S. Supreme Court argues that the exclusionary rule's purpose is to deter government officials from seeking evidence by unlawful means or infringing upon the rights of citizens. The court's dignity must not be compromised if the wrongful act must be admitted. In addition, to protect society from such abusive actions in the future, but to not fear that the offender will not be punished. Therefore, some exceptions allow the court to exercise its discretion under the abovementioned principles. In addition, if such wrongful evidence is eliminated, the rest of the evidence, if obtained by right, would lead to the defendant's hearing.

In the British court in the Jeffrey V. Black case (1978), the defendant was arrested for stealing sandwiches when searching for the defendant. The police found marijuana, so they searched the defendant's house without a warrant and found a lot of cannabis at home. That is evidence that was irregularly obtained. The court dismissed the case because " it was obtained as a result of an illegal search". Is it a violation of the law that is unfair to the defendant? (Pattharasak Wannasaeng, 2022)

Hearing all sides

Hearing all sides (le principle du contradictoire) is based on the idea that the judges are limited in their perception of facts, and the person who knows the facts best is a person whose rights are affected by the ruling. Therefore, listening to such a person's facts will enable those who perform the arbitration duties to make the right decisions. (Somsak Inthapan, 1992)

The principle of hearing all parties is the principle of natural justice. Initially, the principle of law and court procedures shall apply if the law is not provided for or is inadequately provided for. This principle has been practiced for a long time and is considered the minimum measure to protect people's rights. This principle originated from the Magna Carta of England which is based on the idea of what is right and what is wrong. (Kamonchai Rattanasakawwong, 1985) They saw that in society, there are rules of right and wrong as objective condition that does not change with time and place. These provisions decide the court subject to dispute and strict adherence to the principles of natural justice. And human beings can discover the law of right and wrong by listening to the two sides. (H.W.R Wade, 2014)

Standards for accepting electronic contracts as digital evidence

Accepting evidence of electronic contracts as digital evidence in foreign laws

United Nations Commission on International Trade Law has developed two model laws: Model Law on Electronic Commerce 1996 and Model Law Electronic Signatures 2001, which are intended to accept the legal effects of electronic data and electronic signatures, respectively, as a template for countries to harmonize their domestic laws based on the guidelines of that model law.

However, in some countries, electronic contracts of digital evidence may enact legislation to support the matter before the template law is completed, but it is based on a similar principle.

The United States is one country that uses substantive law in the Common Law system and the accusative witness law. Despite the widespread enforcement of various laws relating to electronic documents due to the general use of computers, for example, the Federal Records Act 1950 (as amended), Paperwork Reduction Act 1995, Government Paperwork Elimination Act, and Freedom of Information Act 1996 (as amended 2002), which is often referred to as the Electronic Freedom of Information Act 1996. And later, when Internet use became more widespread, the Uniform Electronic Transaction Act of 1999 and Electronic Signatures in Global and National Commerce Act of 2000 fully supported electronic transactions, or e-commerce. However, using electronic contracts as digital evidence remains a problem because courts in the United States have adopted the rules of proof regulations for hearing witnesses. Listening to the best evidence demonstrates that the authenticity of the evidence also applies to electronic evidence. However, bringing the electronic contract as digital evidence remains a problem because courts in the United States have adopted the rules of proof on the laws of accepting witnesses, the best of admitting evidence, and the authenticity of the evidence, which also applies to electronic evidence.

In England, there are three types of evidence. Like any other country that uses the Common Law system, personal witnesses, documentary witnesses, and witnesses. While the kind of witness will classify electronic data, the courts in England are divided into two cases (Rangsan Pibunsongkram & Charor Yodsombud, 2009) as follows:

1) In the case that the computer is an electronic media manufacturer itself.

2) In the case where the computer is the records

However, the English courts did not accept hearsay evidence because several rules were in place for hearing witnesses. For example, the Rule of Regularly Kept Records, the Rule of Official Written Statements and Certificates, pedigree and ancient documents on interests in property, etc. In addition, parliament has enacted a written law to exclude another ban on accepting evidence, giving British courts a way to get to hearsay evidence in many cases.

Parliament may accept a copy because the electronic data is a copy, but the falsity of the document must be authenticated. Afterward, in 1995, the British Parliament considered electronic data disadvantageous; namely, electronic data should prioritize the possibility of alteration and authenticity. Therefore, the Civil Evidence Act 1995 was enacted to provide electronic data as witnesses. That abolishes the principle of the court's judgment in the Statute of Liberty case so that the authenticity of attestation is the basis for the evidence of documentary evidence. If electronic data is a piece of hearsay evidence, the court must consider it credible if an incident occurs, as required by the Civil Evidence Act of 1995.

The issue of electronic listening and weighing of evidence is a problem facing many countries. The British Commonwealth of Nations held a meeting in 2000 to find a solution to solve the issues that arose. Each country agrees that the Common Law evidence system may not be appropriate for today's technological advancements. In addition, developing the law to keep up with the current situation is the origin of the draft law on electronic evidence to be applied to the Commonwealth of Nations.

Rules of listening to evidence of electronic contracts in digital evidence

In general, the courts of the United States tend to think that using computer records as evidence in proving the facts must take into account two issues: The first point must be to demonstrate the authenticity of the computer record by presenting it. “ Evidence is sufficient to support the

claim that the party has to attest". (The Federal Rules of Evidence Rule, 901(a)) The second point is if a computer record is a record stored on a computer that contains manufactured text, it must show that the manufactured message does not fall within the rules prohibiting accepting evidence. In addition, there is another important legal issue, which is the issue of the best rules for gathering evidence. It can be divided into 3 cases as follows:

1) Accepting evidence with the best evidence rule

The best evidence rule stipulates that to prove the best evidence must use the content of a written memorandum or photograph, the "original" of that writing, memo, or photo. (The Federal Rules of Evidence Rule, 1002) Although the original is only a combination of the numbers 0 and 1, data from a computer is the result of processing through complex technical and electronic procedures. That raises concerns that electronic data from a computer may not be considered "original" by the best evidence rule.

However, the Federal Rules of Evidence state, "If the data is stored on a computer or other device, similarly logged output from a computer or the result of processing has been passed by the human eye and represents the authenticity of the information." It shall be regarded as the "original". (The Federal Rules of Evidence Rule, 1001(3)) So, correctly printed information from the computer is considered the best evidence. When it was first proposed, the Advisory Committee Notes said: " This rule is accepted for practical reasons". Strictly speaking, one might agree that a photograph's "original" is a negative, but in practice and general use.
It is assumed that what is printed from the negative film. It is similar in the course and its usage; the computer-printed record is also considered "original". (Federal Rules of Evidence with Advisory Committee Notes 2022)

Anyway, the laws of the United States have clearly defined terms, writings, or electronic recordings. However, enacting a law in such a manner solves the problem of not adopting the best-accepted evidence rule as a cut-off for this type of evidence.

2) The evidence accepted with the hearsay rule

The hearsay rule is a rule in common law that cuts off evidence that does not wish to be in the court. Due to the nature of hearsay witnesses, the United States has also adopted the rules of witness acceptance for the case of electronic data. The consideration is divided into two topics: computer-generated records and computer-generated records. In the United States, courts often assume that computer records are hearsay witnesses. But some opinions suggest that only some computer records are hearsay. When a computer record is displayed, a person's messages, whether a computer processes them or not, have been presented as evidence to prove that such records may be hearsay witnesses. The parties must confirm that the records are within the hearsay exceptions, such as business records exceptions. (The Federal Rules of Evidence Rule, 803(6)) The opinions are divided into two approaches as follows:

2.1) Not applying the hearsay rule to use computer-generated records

The hearsay rule is in place to prevent inconsistent out-of-court statements from affecting the outcome of a trial because they may be misunderstood as a testimony of what has been heard. The hearsay rule requires that the person's facts be verified, which means they must bring that person to the court to testify and ask for an objection. But this law does not apply to the introduction of evidence obtained from machinery. (The Federal Rules of Evidence Rule, 801(a)(b))

The United States courts and academics have said that the ban on the hearsay rule is a primary method for introducing non-human computer-generated records that are not considered hearsay. The Supreme Court of the United States has ruled differently in the early cases

related to the use of phone records made automatically. The printout record results from computer processing and should not be considered hearsay evidence. Such records are not the processing of statements on the speaker's computer performed outside of court, and do not think computer-printed records are “ statements” as the hearsay witness. The essential rule of this hearsay evidence derives from statements made without an oath, and witnesses cannot be questioned. It may be suspected that the witnesses have heard it again. Probably testify on a matter seen in error from reality, whether intentionally or unintentionally. However, if a witness's testimony is obtained from a machine, there should be no problem with deliberately misrepresenting the facts. And the possibility of getting unclear or inaccurate information when the engine malfunctions. So, computer-generated recordings that are authenticated can be accepted. (Supreme Court of Louisiana, 2018)

2.2) Not applying the hearsay rule to use with the computer-stored records

In the case of records stored on computers that involve human statements, an exception is made for hearsay witnesses. Because if it is offered to prove the fact that it is said before the court accepts it, the record must show the court that the statement contained in the document is credible. Courts are generally permitted to listen to documents stored on a computer as business records by Federal Rules of Evidence Rule 803(6), as follows: (Federal Rules of Evidence, 2022 Edition, 2022)

In the United States v. Briscoe case, records stored on the computer can be accepted as business records. If it is “stored in the normal course of business and is a normal practice of doing that business to make a record as endorsed by the record keeper or related person.” It is observed that computer-printed records may be made for litigation purposes without exception for business records. And the rule that “such records must be kept by normal means of doing business” means the computer data itself, not the computer-printed recorder. (Supreme Court of The United State, 2021)

So, most business records exceptions are hearsay exceptions that apply to computer records. It is worth noting that exceptions to hearing other hearsay witnesses may also be used, such as exceptions to public records. (Alshibly, H, Chiong, R & BAO, Y, 2016)

3) Certifying the authenticity of the evidence

The parties can easily modify electronic contracts of digital evidence, and opposing parties often make claims about the authenticity of such agreements. Therefore, there can be three arguments against the authenticity of electronic contracts in digital evidence. (Arno, R, Lodder, A & Oskamp, 2006) The rules for certifying the authenticity of electronic contracts in digital evidence are based on the same rules as conventional document licensing. That is, the degree of realism does not differ simply because the record is electronic, but accurate authentication may be possible. The person citing such evidence must present evidence that can explain the process or a system that can produce actual results, which is a step before accepting electronic evidence. That may lead the data provider to testify to certify the authenticity of the said contract or the person receiving the electronic contract of digital evidence to confirm that the agreement is sufficient according to the court's decision. (Timur Giorgievich Okriashvili, et al, 2020)

Due to the widespread adoption of computers, consider data deficiencies to be about weighing evidence, not obtaining evidence. In other words, it pushes the burden of proof that the computer's functioning is defective to parties who wish to object to the authenticity of electronic evidence. However, the courts in the United States currently assume that courts can accept electronic evidence without realism. (Denfah Rueangritthidet, 2006)

Listening to evidence of electronic contracts in Thai law

Thailand's witness law's procedural and legal provisions are heavily influenced by countries that use the Common Law system. However, technology has continued to advance, causing changes in many aspects of the laws. These are essential rules in the social order that need to be updated and developed to keep up with social trends in the age of globalization. For this reason, a study of foreign solutions in the use of electronic data as evidence in courts such as the United States and England is a reasonable consideration for the amendment of the Thai witness law to keep up with the changing social conditions and to be in line with international standards.

The legal system of evidence has categorized four types of evidence: personal witnesses, documentary witnesses, object witnesses, and expert witnesses. There need to be clear rules for presenting and accepting such evidence. In the case of electronic evidence, when considering the Civil Procedure Code and the Criminal Procedure Code of Thailand.

Thailand enacted a law to certify the legal status of electronic transactions, both in making a legal contract and hearing as evidence if a lawsuit is filed. This law is the Electronic Transactions Act, B.E. 2544; later, in 2008, the Electronic Transactions Act No. 2 was issued. Amendments, repeals, and additions of specific provisions, especially in the matter of listening to evidence of electronic data, have been provided in Section 11 as amended by the Electronic Transactions Act B.E. 2551 (No. 2) by using the new text as follows:

Section 11, it is forbidden to deny electronic data transmission as evidence in legal proceedings in civil, criminal, or any other case. It is just because it is electronic data.

In weighing evidence as to whether electronic data is reliable or not, one should consider the credibility of the nature or method used to create, store, or electronic information; the nature or form of preservation or completeness and non-alteration of the text, the heart or method used to identify or identify the sender of the information, including all relevant circumstances.

The provisions of paragraph one shall also apply to the publication of electronic data. Section 11 prohibits the court from denying electronic data as evidence in legal proceedings simply because the data is electronic. Currently, the rules for accepting evidence in electronic data are in addition to the specialized courts that have their requirements. Other courts can also hear evidence in the form of electronic data. However, when prescribed to receive or hear, it does not mean that every piece of evidence in electronic data must always have a reliable weight. Therefore, in paragraph 2 of this article, the criteria for weighing electronic data evidence are set out, including those applicable to the publication of electronic data.

It accepts the evidence in electronic data. Although the Thai Electronic Transactions Act has been enacted to support the legal effects of electronic data, including electronic contracts as evidence, the rules in this law section broadly stipulate that the Thai Electronic Transactions Act can accept electronic evidence. Still, it does not specify that it can be assumed to be in the form of proof of any kind and by what method. (Chaiwat Wongwatthanasan, Thawisak Koranantakul & Surangkana Keawjumnong, 2001) In addition, Section 3 of the Electronic Transactions Act B.E. 2544 provides a scope that applies to civil and commercial transactions conducted using electronic data. Except for transactions in a royal decree, it prohibits the application of this Act in whole or part to enforce it.

RESULTS

Analyze the problem of listening to electronic contracts as digital evidence under Thai law compared to foreign laws

Although, at present, there is an Electronic Transactions Act B.E. 2544, which has come into force with the rules or conditions outlined in other relevant laws. As a result, the parties still have to create, use and store the contract in paper form or

comply with the law alongside the electronic contract because they are not confident that it can be used as a reference as evidence in court if a dispute arises. There still needs to be a solution with the weight of the testimony to prove the contract's authenticity and the extent to which the court can accept the affidavit. One of the main reasons is that Thailand needs a clear legal basis for using electronic data to determine what type of evidence to consider.

Electronic data can make some actions required by law electronically and legally binding. However, the Electronic Transactions Act B.E. 2544 provides an essential principle by stating the legal status of electronic data to be presented on paper or printed out of electronic data. The rules for accepting and weighing electronic evidence are stipulated in Section 11 prohibits the court from refusing to accept electronic data as evidence simply because it is electronic data. Therefore, the parties can claim the electronic contract as evidence in court proceedings. If considering the approaches to solving problems in foreign countries, the United States of America has established rules for accepting the evidence that is electronic data if there is using electronic data as evidence in court. In this regard, the authority for taking and getting proof of this type shall be similar to the method of taking documentary witnesses. Still, it must specify precisely what kind of witness. The United Kingdom has set the rules for accepting this electronic evidence as documentary evidence. Electronic evidence can be relevant in civil and criminal cases. Therefore, the Thai witness law should be amended by clearly specifying what type of evidence electronic data is, which has different rules and methods for witnessing. Every kind of witness may designate electronic data as other evidence separate from all four types of evidence to determine the rules and procedures for taking evidence of that evidence to give unique characteristics suitable for the complexity of electronic data separately from other types of evidence. Since Thailand's legal system is codified, the law on witnesses should be enacted, thus creating a standard for international law enforcement.

Weighing evidence is a process where courts use their discretion to reconsider how reliable they are, for which the court's discretion has no fixed rule. However, before reaching this stage, the electronic contract to be used as a witness in court must be able to listen as evidence-section 11 of the Electronic Transactions Act 2544 B.E. But the law does not specify what kind of evidence electronic data is because the determination of the type of evidence affects the rule and methods of bringing witnesses to court. In particular, the key to accepting witnesses is the adequate assurance of the authenticity of that piece of evidence. That will allow the court to trust the electronic data evidence and consider the value of that kind of evidence. The evidence-weighing principle requires consideration of the credibility of the evidence by the rule established by law in Article 11, paragraph 2. Thus, to make the court trust any evidence presented, it depends on the process and procedure that can show the court that the part of the evidence is actually in its use.

The Electronic Transactions Act 2544 B.E. provides a mechanism for establishing electronic contracts' witness weight and legal credibility. From the statutory presumption of this Act as the legal validity of electronic contracts in the critical sections for the listening and weighing of electronic evidence.

Therefore, the author believes that as a guideline to building the credibility of electronic contracts, there should be a service business relating to electronic transactions that will strengthen credibility and trust among both government and government sectors and private sectors as well as build more confidence in the counterparties who wish to conduct electronic transactions.

CONCLUSIONS

Thailand has stepped into an information technology society in full, as evidenced by Thailand's trade liberalization. Consequently, it must

comply with the World Trade Organization (WTO) framework, which tends to promote paperless trading more and more, leading to a greater prevalence of electronic transactions. However, despite the advancement of technology and the expansion of electronic commerce. However, developments have also caused legal problems in other countries, such as the United States and the United Kingdom, as studied above. If both government and private organizations still use paper to conduct transactions and collect such contracts and supporting documents as evidence. In case of disputes, the creation, storage, and use of such paper contracts burdens transportation costs and storage locations and increases daily paper usage. The problem above is caused by the lack of credibility and confidence in electronic transactions by various agencies in Thailand. However, there is currently the Electronic Transactions Act (No.3) B.E. 2562. But the law still needs to determine what kind of evidence electronic data is straightforward. That will affect the criteria for carrying out and listening to evidence according to the Thai witness law.

It was causing problems in using electronic contracts as evidence in court proceedings as to what type of evidence is considered. That will affect the criteria and methods of bringing evidence to be examined in court proceedings. According to a comparative study of other countries' evidence laws, electronic data is the rule for accepting evidence in the United States. However, in principle, it does not specify electronic proof. Therefore, the study found that the Thai Civil Procedure Code has not yet defined the meaning of "electronic data" clearly stated. But suppose electronic data is used as evidence in court. In that case, the rules for carrying out and listening to this type of evidence are similar to the method of taking documentary evidence. In England, it was found that to solve the problem. The law was amended by requiring the document to be meaningful, including electronic data. So, there is no problem interpreting the electronic data as any evidence and making sure that the court will use the rules and procedures to ascertain and prove evidence that is electronic data. The law must support the methods of escorting and obtaining electronic evidence to accept electronic contracts as evidence for proof that electronic data is equivalent to other types of witnesses and can be applied to all kinds of cases in court proceedings.

To be consistent with the assumptions set. At present, although the Electronic Transactions Act 2544 B.E. has prohibited the court from refusing to listen to electronic data as evidence in the proceedings. But the reliability of electronic contracts considered electronic data remains an issue of data security and authenticity. Since the law has not clearly defined the legal status and criteria for presenting and hearing this type of evidence, it is necessary to adopt the security technology of the system for the preparation, use, and management of this type of evidence to keep electronic contracts to apply as well.

RECOMMENDATIONS

Therefore, the development and improvement of the Thai evidence law concerning electronic data to be clearer can solve this problem. It is also helpful to weigh this type of evidence for credibility. Therefore, we would like to suggest solutions as a guideline for building legal weight and credibility for electronic agreements as follows:

1. There should be amendments to the Thai procedural law by defining the definition of "Electronic data" to clarify the type of evidence.

2. The law should establish methods for proving the authenticity of electronic contracts with the same criteria in case the electronic agreement is considered documentary evidence.

3. The law should establish necessary technological standards for confidentiality so that confidentiality, integrity, access control, and electronic data security help weigh this type of evidence.

4. Should cancel the rules prohibiting the taking of witnesses and amending the documentary witnesses; however, once it is accepted, the law can receive the electronic contract.

5. There should be a requirement of the President of the Supreme Court on the hearing and the method of taking evidence in electronic data to have clear rules and procedures for using electronic contracts as witnesses.

6. Promoting electronic transaction service businesses should help build confidence in both the public and private sectors.

REFERENCES

Alshibly, H, Chiong, R & BAO, Y. (2016). Investigating the critical success factors for implementing electronic document management systems in governments. *evidence from Jordan information systems management, 33*(4), 287-301.

Arno, R, Lodder, A & Oskamp, (2006). *Information technology and lawyers: advanced technology in the legal domain, from challenges to daily routine.* Springer Science & Business Media, p.198.

Chaiwat Wongwattanasant, Thaweesak Koranantakul & Surangkana Kaewchamnong. *Explanation of the Electronic Transactions Act 2001*. n.p.

Denfah Ruangritdet. (2006). Legal issues related to accepting the electronic documents, Dunlapar, 53(3), p.95.

Electronic Transactions Development Agency. Recommendations for digital device management standards in forensic evidence Version 1.0. March 23, 2016.

Federal Rules of Evidence with Advisory Committee Notes 2022 Edition. (2022), Federal Judiciary of the United States, Independently published (September 4, 2021).

Federal Rules of Evidence, 2022 Edition, (2022) with full Advisory Committee notes, legislative history, Rule 502 explanatory note, internal cross-references, quick-reference outline, and enabling act. As amended through January 1, 2022.

H.W.R Wade, (2014), Administrative law (11th edition), Oxford: Clarendon Press.

Kamonchai Rattanasakawwong. (1985). Legal practice of administrative officials in common law countries. Journal of Law, 15(4), p.7.

Kritsana Changklom. (1999). Draft research study report on electronic commerce law. Bangkok: National Electronics and Computer Technology Center.

Kramon Thongthammachat & Sombun Suksamran. (2003). Interesting facts about government and the Constitution of the United States. Bangkok: Social Science Publisher.

Pattharasak Wannasaeng. Unit 12 listening to evidence in criminal cases. Retrieved 18 June 2022, from https://www.stou.ac.th/schoolsweb/law/UploadedFile/41717-12.pdf

Rangsan Phibunkitsakul & Chalor Yossombat. (2009). Legal forms for electronic transactions and electronic signatures: Study for only the case of accepting the evidence of electronic data. n.p.

Somsak Inthapan. (1992). Procedures of the Administrative Dispute Arbitration Committee in Thailand (Thesis, Master of Law). Bangkok: Chulalongkorn University.

Sunee Sakawrat, Translation. "Digital evidence for legal professionals.", by Larry E. Daniel, Lars E. Daniel, Foundation for Internet and Citizen Culture, (2016), P.57.

Supreme Court of Louisiana, (2018), States v. Armstead, in The United State Court of Appeals for The Fifth Circuit, The United Stated of America, Case: 17-30439.

Supreme Court of The United State, (2021), Kenneth Lamont Sanders v. United States, On petition for writ of certiorari to the united states court of appeals for the eighth circuit, june 1, 2021, p.1.

Timur Giorgievich Okrishvili, et al. (2020), Legal status, role and features of electronic document management, Universidad del Zulia, Utopía y Praxis Latinoamericana, vol. 25, no. Esp.12, p. 178-186.

The Federal Rules of Evidence Rule 2021 Edition, (2021), Updated through January 1, 2021,

Michigan Legal Publishing Ltd. Crand Rapids, Michigan.