

POSITION OF ELECTRONIC EVIDENCE IN IRAN LAW AND INTERNATIONAL DOCUMENTS

MEHRZAD RAZMI^{a1} AND MOHAMMAD AFRAS^b

^{ab}MA in Private law, Azad University of Ahvaz, International Center of Persian Gulf, Iran

ABSTRACT

Nowadays, various relational and information methods were penetrated in life scene of human being. Using these methods in commercial relationship caused to create new kind of evidences namely electronic evidences. Electronic evidence differ traditional testimony naturally. Detection, proof and maintaining these evidences need to special situation and material in all legal systems. In Iran, in order to recognize new relational facilities in international and national commercial exchanges, a law namely «electronic commerce» has been developed. This law have been approved by ancestral electronic commence- adopted and have been explained each electronic testimony in form of message data is valid. So, document, evidence, profession and oath are realized in electronic form. Finding shows that electronic evidences in other legal systems in the world like united state and European Union has more demonstrability values compared to Iran law.

KEYWORDS: Electronic Evidences, Message Data, Electronic Signature, Electronic Post, Proof Evidences, Law of Electronic Commerce, Ancestral, National Legal Systems

In the past, proof evidences were in traditional form. But today's, new kind of evidence namely electronic evidences is developed by extending electronic exchanges. Electronic evidences could have important role at lawsuit or punitive processes. Primarily, electronic prescriptions could present valuable information which is not available in paper prescriptions.

In this study, difference among electronic evidence and traditional evidences are surveyed after explaining concept of electronic evidences, and then kind of electronic evidences are explained. Comparing validity and proof value of electronic evidences in Iran legal system and other legal systems like United States and European Union and other countries are discussed. How to discover and gathering information is one most important discussion which has special position in regulation of different legal systems. Each country selected special and specific plans to discover and maintain electronic evidences which difference and unity points are discussed. Presenting electronic evidences to courts in Iran legal system and law of other countries are discussed in this study as one of most important issue in this study.

CONCEPT OF ELECTRONIC EVIDENCE

Electronic evidence is a message data which is used by claimant to prove or defend cases. According to definition of message data in clause A of article 2 of electronic commerce law, electronic evidence is a symbol of event, information or concept which is produced, sent,

receive, save and processed by electronic equipment or modern information technology, so claimants rely it to prove or defend cases.

According to extended definition of electronic commerce law about message data, it could be explained that not only electronic equipments but all available instruments like telegram, telex, digital, magnetic, light, electromagnet and other instruments which will be created in future are caused to make electronic evidences (Wang, 2006, P5)

Therefore, data base, operational systems, application programs, computer-generated model, electronic voice and mail message, all saved information in computer memory; ATM transaction log, spread sheet, computer printout and digital audio and video files are kinds of electronic evidence (Gaten, Page 43-44)

DIFFERENCE OF ELECTRONIC EVIDENCE AND TRADITIONAL EVIDENCE

Since format of electronic evidence is message data, so some important differences between electronic evidence and traditional evidence are explained:

Electronic data could be saved in compressed form, so archiving is easier due to low volume, in other hand, it could be hiding easily. For example, a hard drive include more than 1.5 data sheet and a corporate backup tape include 4 million of data sheet. (Rockwood, 2005, P.12)

Unlike paper document, Electronic evidence is not tangible and exact, so it is not available easily and only is readable by software programs which have been created, if software program is not available, so document is not accessed.

Almost, electronic evidence never is missed. Although users suppose to remove file by pressing (Delete) key, but removed documents is always retrieval. In addition, Electronic data are reproducible easily and are saved in Log file and document header when are created, so deleting all of them is difficult (Brereton, 2007, 63)

Frequently, electronic evidence consist of valuable information such as date of create, date of change and delete of file and date of password changes, these could help us to discover the fact, but paper evidence are lack of these information. (ibid, 68)

In electronic documents, realization of traditional concept «original copy» is defined as a document that don't reflect handwriting, signature or fingerprint as intermediate, because in electronic scene before seeing information in computer page, information have been transferred to different component of computer several times, so visible document of evidence is not original.

In traditional documents, handwriting, signature or fingerprint of issuer shows identity and if documents are denied, it is possible to prove document by accommodating handwriting and signature easily, but this case is not possible in electronic documents, because handwriting and signature of these documents don't consist of biological characters of issuer (Noori and Nakhjavani, 2003, 23)

IMPORTANCE OF ELECTRONIC EVIDENCE

According to extending usage of computer technology in information management and increasing usage of computer systems instead of paper files, there have been created valuable information in computer systems and during last decades have been used in courts of developed countries. Discovering electronic evidences is called electronic media discovery.

In different files of recent claimants like sexual hurt, unauthorized publication, defraud, prove victim and culprit relationship in purpose kiss, and prove robbery of commercial secrets and discovering documents about

criminal actions, electronic evidences have been used at developed countries (Wang, 2006, 22)

Much information is found in electronic evidences which are not found anywhere. There are typed articles which have not printed. There are important evidences which defendant and complainant have not been informed about it or are not aware to delete or save it. For example, during working with software, some log files are created which is registered different information without user awareness or someone maybe thinks deleting an electronic message or email in network, all information is removed, while other documents are available in other networks group. Electronic evidences are not terminated in computers and include all information which is achieved by electronic equipments like cell phone, telegraph, telephone pager, telephone message, voice message, electronic message and etc....

KINDS OF ELECTRONIC EVIDENCES

Since security level of instruments and used methods in producing and saving electronic evidence is different, so validity and proof value is different too. Electronic evidence is categorized in simple evidence and secure evidence.

Simple Electronic Evidence

Simple electronic evidence is a message data which is produced, sent, received, saved and processed by insecure information system. This electronic evidence has insecure electronic signature, so that it could not be sure about issuer and identity. Used information system to produce, sent, receive, save and process of message data doesn't have high technology, these systems are not planned in desirable format and are not accurate, so it is possible to have wrong information. Also, these systems are not secure against abuse and a hacker could easily access to information and could change it. A computer Virus could easily delete or change information in such systems, so these systems could not guaranty integrity and secrecy of information. (Pour Attaei, 216, 2001).

Simple evidence is proved by a normal electronic signature, this signature could be as a simple handy image or a name in the document, electronic post, and intelligent card or selecting «agreement» option, all these cases could not guaranty document relativity to issuer, identity of issuer and document integrity, because all of these cases could be invented easily. Third party could easily attach inverted image of handwritten signature to

document or invert identity by stealing intelligent card or discover pass word. Computers could test all words, locations and terms in a specific language to find password and could find an eight letters password in few minutes (Ahani, 41, 2005)

Secure electronic evidence

Secure electronic evidence is a message data which is produced, saved or processed by a secure information system and has secure electronic signature. Security level of used technology in this document is reliable and could guaranty document relativity to issuer, identity and integrity of document. These documents are irrefragable and could not be inverted. In addition, such evidence should be maintained in secure place (Homan, 54), so a secure information system forms a secure electronic signature and a structure of secure electronic evidence, following there are some discussion:

Clause H of article 2.Q.T.L explains criteria of a secure information system as following:

A secure information system is a information system which:

- 1-is maintained against misuse reasonably
- 2-is accessed in reasonable availability
- 3-is structured according to importance of task.
- 4-is accommodated to safety process.

Most important point is that lawmaker is required reasonable level to security of information system. According to reasonable criteria which have been explained in clause N of article 2 Q.T.L, mentioned situation is evaluated according to access to suggested options, situation of message data like exchange, skill or parties situation.

Situation of secure electronic signature is determined according to article 10 Q-T-L, this article is explained about secure electronic signature:

- 1-should be unique to signer.
- 2-should determine identity of signer of message data.
- 3- Issue by signer
- 4-link to message data, so that each changes in message data could be discovered and recognized.

Secure electronic evidence could be a digital signature or reasonable commercial process in term of

technical characters and could be able to supply application in law. Iran law selected technology –neutral approach following ancitral law about secure signature, this means that following a specific technology is not needed, but situation of a secure signature is determined and any electronic signature which is able to supply situation could be explained as secure signature and judge should reveal situation realization in article 10 (Nouri, 2005,42)

Advantage of this approach is that, if new technical methods are created or security of available methods is removed, any modification of law is needed.

Validity and proof value of electronic evidences

There are a few law about electronic evidences, even there is not seen in laws of countries like European union about electronic evidences (Brown, 2010, 128), any way electronic evidences is defined as information which is originated of electronic equipment or digital intermediate, so that is used to prove fact of cases.

Article 12 Q-T.L without any definition about electronic evidence is provided that:

Documents and proof evidences of claimants may be a message data and proof value of any message data could not be denied according to available evidences in court or public office.

This article is invert of article 19 of anistral law about electronic commerce that has adopted electronic evidences. Context of this article is clear, so that there is no doubt about electronic evidences.

Article 14 Q-T.L is provided that

All message data which are maintained in secure methods, parties' commitment are valid in legal offices. Article 15 is relied to secure message data.

So, when secure methods about lawmaker are not regarded, it is revealed in any evidences except document and electronic signature, all electronic evidences are equal to paper evidences.

According to article 15 Q-T-L that secure electronic evidence is most important document in notary public, some believes that these evidences should have proof value, so secure electronic evidence is a certificate and meet needing when documents like donee certificate or immovable documents are needed (Dost Mohamadian, 2007)

Although, aforesaid doubt in article 14 Q-T-L is accurate, but it seems to be wrong replace secure electronic evidence by certificate, because there are some differences between secure electronic evidence and certificate, following some of them are discussed:

According to article 1287 of civil law, certificate is a document which is regulated by officary in notary public, other documents is considered as normal documents, so this definition is not included in secure electronic evidence, although issue of digital certificate is considered as a officary in regulating documents, but this article refer to physical presence of officary to regulate documents.

According to articles 50,52,57,64, 66, 67 and 68 of notation law, notary should determine identity, mansuetude and satisfaction of contract parties. If identities of contract parties are determined by secure electronic signature but appearance healthy are not determined, this contract is not supplied in electronic evidences.

Certificate has other effect, according to article 1305 of civil law certificate is valid against third parties and these documents are carried out without court permission. Secure electronic evidence is not included in this article.

In article 6 Q.T.L about ownership of immoveable property and sale medical material to end consumers, message data is not equivalent to writing, also clause B of article 113 of fourth plan of development, permission to supply services is as computer form to notary organization, but electronic evidence is not valid.

Discover and gathering electronic information

Discover and gathering electronic information is important due to dispersion and extending these information and special skill, so this system differ traditional legal system. It is supposed to there are profitable and unprofitable information. Often, finding these evidences and gathering and regulating them is time and cost consuming. So, due to some cost in judge system, someone complains about these costs. In legal systems of countries like England, these costs are paid by lost person in contest. (Development center of technology information, 2008) in united state union, if one parties of contest rely to electronic evidence, person who owes information and be professional is responsible to recover information. (Brown, 2010, 89)

In Iran law according to articles 515 and 519 of civil law, cost of discover and gathering these evidences is related to proof or defend, so someone who sustain these costs could get by proof faulty of other part.

Electronic information has incomes like complexity and cost consuming specially in civil judge. But we could withstand against this criticism and stated that discovering this information only have not created new problems, but these information are easier, low cost and rapid compared to paper document. Most important income of discovering electronic information is that leads to electronic evidences.

Presenting electronic information to court as an evidence

This stage usually is done in format of CD or DVD, but other methods like presenting on evidence handwriting should not be ignored.

Situation of presenting electronic evidence to court in Iran law

In iran law, there are not several regulations about electronic evidences, except some approved regulation about computer crime and civil and commercial claimants. Important issue in this section is that someone believes electronic commerce law of Iran is not restated judicial operation in electronic space. (Ahani, 2005)

Wherever, legal ceremony is needed by context sign, this situation is possible in electronic space. In addition, article 8 of this law explains: when law is required to maintain information as original, this is possible by maintaining information as message data and juridical system replace paper archive by electronic archive.

Out of these two areas, whenever legal regulation is required at physical operation of presents of claimants like audit meeting, testimony listening, swear or Electronic evidence is not possible.

Used reasoning is not related with article 12 of law. Regulated order includes all electronic evidence from document to swear and lawmaker permission to use of electronic evidence needs to permission to present to court.

In other word, impossibility of presenting some of evidence is due to lack of some equipment not because of finding legal nature. When there is no equipment to

present electronic, how to present these evidences to court? Electronic commerce law of Iran is not capable to plan all complex discussion about electronic world. So, there is special regulation about electronic evidences. For example, in countries in European Union, electronic evidences are equivalent to traditional evidences (Zarkam, 2005, 12)

Electronic document is equivalent to paper document and electronic signature is equivalent to handy signature, even electronic post is equivalent to normal post.

In countries like Portuguese, electronic post is equivalent to telephone conversation and we know electronic post consist of voice post (Douglas, 2004, 102)

If each part of claimant wants to present electronic evidence to court, there is no way to use traditional principles in civil law. Management system has created process to make electronic court and realize electronic judgment in our country. This system has provided possibility to change, present, following complaints or prophecy of judgment time.

There is a question which if claimant has permission to prove in court by providing information? Answer is that there is no restriction in this regard.

In other hand, article 12 of electronic commerce law is adopted possibility of any evidence in form of message data. So, if evidence in normal form is not possible in court or presenting original form of evidence is needed, electronic evidence could be presented to court by providing needed equipment by court approval. So, other part of claimant has opportunity to defend according to this evidence.

When presence of witness is not possible in the court, claimant parties could present their evidence to court. In this case, other part of claimant could use of legal law. Validity of these witnesses is considered.

Situation of presenting electronic evidence to court in foreign law

There are a few cases in law of countries about electronic evidence, so that this case is a modern legal issue.

In United States union, federal court of this country has proceeded to create electronic court. Electronic court is a network based on web and federal court use it as a real meeting. To send other orders and

decisions, court could receive evidence and issue some vote.

Both parties to communicate to electronic court should enter issued username and password, so posted message to network is read and their message are posted (Brereton). It is possible to send evidences in addition to message and documents. Experimental period of electronic court of federal have started from 2001 and continue. During experimental period, access to electronic court is limited to two parties and representatives. Technical setting of electronic court is formed by court on network and revised by results of court.

According to regulation of this court, both parties in civil law are encouraged to following cases: (Ibid)

- Using electronic information to prepare a list of documents and evidences
- Adopting result of electronic information exchange related to protocol
- Exchange of electronic evidence and documents
- Regulating represented issues to analyze in needed cases using electronic information
- Attending to use of electronic information in judgment

If both parties agree to make decision to exchange a protocol, that protocol should consist of:

- Exchange of documents or evidences of court and announcing in electronic format
- Electronic exchange of necessary list of documents
- Suitable instrument to exchange electronic information
- Using technology in judgment

In some cases, court encourage both parties to deliver evidences in electronic format, this could be as a saved disc.

Both parties are encouraged to analyze better ways at information technology to present evidence. Best way to present information technology is related to degree and level of documents. If both parties determine and specify evidence, make decision is announced in simple technology.

Some of unions of this country have proceeded to present some evidence. In court of «newhamshayr» union, this instruction is observed. According to this

instruction, if each of parties wants to present documents in electronic form should follow below situation:

Such request should be regulated in a written form,

Each written form should show below cases:

Domain of evidence

Method which electronic evidence is presented. So, some equipment like computers should be provided by court or claimants.

Needed system should be surveyed. Installation way and using of system should be explained to court five days before representing. Also, value of discretionary of system and cause of electronic evidence should be explained.

Methods which electronic evidence should be analyzed before receiving. This description shows:

1-if jury could receive electronic information and revise them?

2-if jury training is needed or skill level is sufficient to finish process?

Also, suggested to apply a computer by complaint to present evidence and documents are saved on CD to apply by jury easily.

If court provides needed equipment to present electronic evidence, complaints should sure about equipments during presenting electronic evidence process. If special software to evidence management is not needed, claimant and court should be informed (Ibid)

Requested person is responsible to regard regulation and ceremony and also is responsible to present evidence to court.

In some unions of this country like youtha and California unions, there are some branches to present evidence to court. In these two unions, there are branches to present electronic evidences.

In Australia, federal court of this country has proceeded to create an electronic court which is similar to united state union. Creating branches to manage cases is done before judgment. These courts could receive request, evidences of parties (Rochwood)

International institute have been established to organize process of gathering evidences. Some of international institute is international organization about

computer evidences which have been developed in 1993. Purpose of this organization is to assist in gathering computer evidence to present legally (Ibid)

Also, in countries of European union, possibility of adopting electronic evidences is considered in court by holding some congress. Purpose of holding these congresses is to reveal court task to face electronic evidences. But main purpose is to reveal challenges in laws of countries and offering best way to achieve more guarantees and developing electronic evidences as a useful tool to prevent electronic crime. As result, this analyzes reveals that in European countries except England and Belgium, electronic evidences have not been intended. (Ibid)

ELECTRONIC EVIDENCE OF CLAIMANT PROOF

Electronic certificate

One of evidences which could be realized in massage data format is written evidence (certificate). Article 12 Q.T.L of Iran use of certificate terms clearly. Electronic certificate should prove claims. When certificate is originated by computer tools, such certificate creates those documents. So, in order to use written evidence in computer or electronic system, other tools should be created to prove evidence.

Electronic witness

Electronic witness could be presented to court in two forms: one form is recorded witness in electronic information instruments like CD or memory. Second form is presenting electronic witness. Presenting witness is in line. This kind of witness is based on equipment, so that witness could represent alive and voice, image and state is understood by judge and claimants.

There is a question that how is validity of this witness?

Survey of Iran law revealed that physical presence of witness is necessary in the court. Presenting witness on line, if witness is not present in court but this relation is felt by claimants and judge

Seems, this kind of witness is not considered as an evidence for judgment due to physical and traditional approach of civil law and its validity for judge is not a witness but is a document. We are able to present witness as voice or video communication when witness presence is not possible. Although this method is not better than

witness presence in the court, but prefer on witness certificate.

Electronic profession

Electronic profession is similar to electronic witness, especially in presenting form to court. Electronic profession could be represented as voice or video recorded in disc or light memory. Profession could be represented as written form.

CONCLUSION

Development of information technology and communication in current world has caused to create electronic evidences to prove claimants claims in commercial and criminal affairs. Electronic evidences differs traditional evidences naturally. Evidences are divided to simple and secure kinds.

Simple electronic evidence is similar to normal traditional documents and secure evidences are irrefragable. Discover and access to electronic evidence and maintaining consist of presenting process of electronic evidence. Electronic evidences are presented in three formats to court like document, profession and witness. Presenting electronic certificate is possible in two ways. First way is presented information to court by transmitter instrument and second way is to present information as written document to court. Profession and witness are presented to court in two aforesaid forms too.

REFERENCES

- Gaten, Allen (2004), electronic evidence, translation Mosayeb Ramezani, Tehran, Supreme Council of Information
- Purataei, Khosro, (2001), e-commerce, Dibagaran Cultural Institute Tehran
- Ahani, B., (2005), Coagulation and proof of the conclusion of electronic contracts, Private Law PhD Thesis, Faculty of Law, Tehran University.
- Noori, Seyed Masoud, (2005), e-commerce legal principles with an emphasis on e-commerce law in Iran, Journal of Science, Year eleventh Number 44
- Noori, Mohammad Ali and Nakhjivani, R., (2003), E-Commerce Law, Tehran, Ganje danesh Mohammadian doost, Hamid, cyber crimes and

electronic evidence taken from the internet, go on 2014/17/03

- The development and exchange of knowledge, information technology (2008), use of information technology in civil proceedings (electronic court)
- Zarkalam, Satar, (2005), Law on Electronic Commerce, Proceedings of the conference on legal aspects of information technology, Qom, publisher salsabil.
- Rockwood, Rebecca, (2005), Shifting Burdens and Concealing Electronic Evidence: Discovery in Digital area, Journal of Law and Technology, vol. xll, Issue 4
- Wang, Minyan, (2006), The Impact of Information Technology Development, Journal of Law and Technology, vol.15, No.3.
- Brereton, (2007), Evidence in Civil Proceedings: An Australian Perspective on Documentary and Electronic Evidence, Speech to the National Judges College of the Supreme People's Court of The People's Republic of China
- Brown, Christopher L. T, (2006), Computer Evidence: Collection and Preservation, Charles River Media, US,
- Douglas, Young, (2004), Advising the Corporate Client on the Duty to Preserve Electronic Evidence, available at: www.fbm.com/docs/publications/4950cvr-9AC830CCB4.document.pdf