Iranian journal of educational Sociology

(Interdisciplinary Journal of Education)
Available online at: http://www.iase-idje.ir/
Volume 1, Number 2, August 2017

Judicial Citation of Electronic Evidence in E-commerce Cases and its Social Effects

Somayeh Bani Yaghoub[1], Abbas Karimi[2*], Morteza SHahbazinia[3]

1. PhD student, Department of private law, UAE Branch, Islamic Azad University, Dubai, United Arab Emirates
2. professor, Department of private law, university of Tehran, Tehran, Iran.
3. Assistant professor, Department of private law, Tarbiat modares university, Tehran, Iran.

Article history:
Received date: 10 April 2017
Review date: 24 May 2017
Accepted date:22 July 2017

Keywords:
Electronic Evidence, Electronic Business, Judicial Reliability, Evidence for Proving Claims.

Abstract

Introduction: With development of technology and its effect on different aspects of human life especially in trade and transactions and regarding increased competition in international business arena, examination of different dimensions of electronic business as one of the main manifestations of this kind of business is inevitable; this paper answers this main question that how is the judicial reliability of electronic evidence in business claims and what are the social and judicial consequences? **Methodology**: this paper is descriptive-analytical (qualitative) and uses inferential methodology applying scholar agreement index in understanding judicial examinations related to judicial reliability of electronic evidence in electronic claims based on existing facts, evidence and circumstances. **Findings**: Using electronic communications as a tool for doing various interactions provides an important issue called electronic business and because of virtual network characteristics, examination of procedure system has a special importance relative to other issues of information technology law along with judicial equality. **Conclusion**: If the process of discovery and obtaining electronic evidence is performed according to legal principles, and in addition to validity, integrity, reliability and undesirability issues, in this case, it can be basis of issue of order and the rules governing evidence proving claims are also used in electronic business claims.

Please cite this article as: Bani Yaghoub S, Karimi A, Shahbazinia M. (2017). Judicial Citation of Electronic Evidence in E-commerce Cases and its Social Effects. **Iranian journal of educational Sociology**. 1(2), 206-211.

* Corresponding Author Email: abkarimi@ut.ac.ir

[DOR: 20.1001.1.26453460.2017.1.2.18.6]

1. Introduction

The demonstration of a right is an unchangeable fact but the proof of a right is making clear that proved right. The real owner of the right in denial of his/her right, should prove the demonstration step with evidence and if s/he couldn't prove it, it is like that s/he has no right, though in the step of right demonstration, s/he owns a right. In civil law, rights are identified in the stage of right demonstration, and in demonstration of those rights, in case of denial, the step of right demonstration is raised that is examined and studied in civil law procedure. According to the mentioned explanation, the significance of evidence for proving claim becomes clear as people prove their right by this evidence in case of denial or ignorance and by using evidence for proving claim, people's right is guaranteed, so one of the most important legal issues is detecting evidence for proving claims and their proving value. In the past, the evidence was only in traditional forms as confess, document, testimony and oath, but by developing information and communication technology new evidence was created called electronic evidence. Evidence for proving claims in virtual network has its own characteristics and in most cases, it is only by using electronic evidence that both parties of an electronic claim can defend their rights. So, dispute in electronic space like real conditions is inevitable, therefore both parties should have valuable evidence for proving their claim. According to the different nature of electronic evidence from traditional evidence, identifying these evidence and examination of their differences are very important; hence, in this paper, we try to answer this main question that how is the judicial reliability of electronic evidence in electronic business claims and what are the legal and social consequences?

2. Methodology

The study and discussion of judicial reliability of electronic evidence in electronic business claims and their social consequences at first require introducing various existing evidence and then recognition of cyber world with its special features. So many available evidence in this world are discussed according to evidence system of Iran and other evidence special for cyber world. As Iranian lawmakers follow legal evidence system with some exceptions, the related issues are analyzed using inferential and descriptive analysis method. The research steps for obtaining goals are as following: At first note taking from books, articles and Persian resources in Civil law is carried out and then foreign resources are examined, translated and some notes are taken and finally, regarding all notes, issues are formulated and the paper is written.

3. Findings

Identifying electronic evidence and their elements: Nowadays, one of the important and complex issues in legal systems, is the concept of electronic evidence, their discovery, reliability or acceptance. This issue is along with transformations in communication and technological arenas, introduces right and commitment limits to virtual world and has made many changes in this communication. The virtual and electronic world has its own requirements, opportunities, threats and limitations. The important point is that required electronic evidence for working in this world should be based on structures and requirements of this world. So, in this section we identify electronic evidence and their elements.

Definition of electronic evidence: electronic evidence is a kind of evidence that has "electronic" feature, in other words, "electronic evidence" is a concept derived from evidence; but this does not mean that this kind of evidence includes all kinds of features of traditional evidence, but its electronic nature differentiates it from other traditional evidence (Abdollahi, 1391: 22). By rapid development of technology, there are various forms of documents and contents saved in many formats and this issue has made impossible to identify

[DOR: 20.1001.1.26453460.2017.1.2.18.6]

Cyberia evidence and their modifications. This evidence can be in the form of digitally saved data in the formats of text, graphic files, voice, motion pictures, database, contemporary files, hidden files, deleted files and computer data created by operative system or applications on saver systems.

Value and importance of electronic evidence: At the moment so much of the information playing an important role in legal claims or criminal procedures is only created, saved and maintained in a computer system in readable format. So by developing and using computer technology in different fields, each investigation requires computers or networks and each party of the investigation can benefit from technical and legal knowledge of this technology. Lawyers should use them well while identifying exonerating evidence. It is possible that ignoring electronic data and evidence by a lawyer in a legal procedure cause missing a claim that has the capability of winning. Also this can face the clients with costly and inevitable verdicts or impose punishments to them because of default in presentation or damaging existing files. Therefore, is is essential that lawyers become more familiar with computers and networks as sources of evidence to be successful in challenging these kinds of evidence and use common reasoning's in these fields (Qolestani, 1396: 78). In fact, lawyers can obtain electronic evidence for these reasons: regarding increase in using computer technology in information management and higher usage of computer systems instead of paper cases, valuable information is saved in computer systems that its discovery and reliability have special importance. Another reason can be this: Modern/Cyberia electronic evidence has this capability that is more convincing than paper documents. On the other hand, at the moment e-mail is one of the most important communication tools in giant commercial companies. The informal character of this tool has caused that some problems are proposed in an e-mail that are not presented in a formal and written note. Electronic evidence provide access to these informal notes. It is also possible that draft of documents with their available printed copies are just in electronic forms. It is possible that we get electronic copies from paper documents which have been changed, hidden or distorted.

It is possible that electronic copies of documents have double information or an electronic copy may have system information or hidden crypts and they can be used for discovering forgery (like changing the date of a document) or gathering information about producing and distributing a document (Allen, 1383: 75). In adition to lawyers, judges, and judicial authorities also require electronic evidence. If these people don't have required training and awareness in this case, they won't be able to utilize these evidence accurately. Along with this, article 16 of comprehensive electronic business development program stipulates: "It is upon he ministry of justice to cooperate with judicial and commercial ministry to instruct strategies of applying electronic business and instructing them to judges and trial personnel under headlines such as international definitions of computer crimes and offences, identity discovery, methods of locating and tracing data in web and computer networks, encryption and decryption principles in data stacks (comprehensive electronic business development program, ratified in 1384/4/5).

Elements of electronic evidence: As the security level of used methods and devices in production and saving electronic evidence is different, the credit level of evidence and its proof value is also various. Electronic evidence can be divided into two kinds of usual evidence and secure evidence that we examine them in the following:

Usual electronic evidence: Usual evidence is message data produced, sent, received, saved or processed by an insecure information system having insecure electronic signature as we cannot make sure from assigning the document to issuer, his or her identity or document's integrity (Abdollahi, 1387:53). So, a simple electronic signature and insecure information system are constituents of usual evidence. Insecure information system means a system that has not been planned desirably and without enough precision, so there are always possibility of mistake in its performance data. It is also insecure faced with penetration and abuse and an intruder can easily access the information by entering the network or changes them or receives the sending information from the internet network, modifies them and sends them again or the entrance of a virus to this system can lead to modification or deletion of data. For this reason, this system can't guarantee

[DOR: 20.1001.1.26453460.2017.1.2.18.6]

integrity or privacy of information (Mahdipour attae, 1380:216). The usual evidence is confirmed by a simple electronic signature. The law of electronic business hasn't clearly mentioned simple electronic signature, but in the paragraph "y" of the article 2 Electronic signature has been generally defined. As in the paragraph "k" of this article, the secure electronic signature has not been especially defined, we understand that a simple electronic signature, is a signature that has the requirements stipulated in paragraph "y". According to this paragraph, electronic signature is any annexed sing or logically connected sign assigned to data message that can be used for identification of data message. This sign can be a simple picture, manual signature or typing the name of person under document, his/her e-mail address, a smart card, choosing the I agree choice or a password that none of them can guarantee the assignment of the document to the issuer, his or her identity and document integrity. All of these cases can be easily forged (Abdollahi, 1387:55).

Secure electronic evidence: secure electronic evidence is a message has been produced, saved or processed by a secure information system having secure electronic signature. The security level of used technology in this document is such that guarantees the assignment of the document to the issuer, his or her identity and document integrity. Secure information system is one of the necessities of gaining secure evidence (Abdollahi, 1387: 56). Secure information system is a kind of system that saves information in a way that's available in time of necessity and on the other hand it's organized in a way that guarantees integrity and privacy of information by preventing any penetration or misuse. The law of electronic business has also proposed the criteria of a secure information system that its realization depends on the modern technology. The paragraph "H" of article 2 of the law of electronic business states that: "secure information system, is a kind of information system that: 1-It is wisely protected against misuse and penetration. 2- It has reasonable level of accessibility and appropriate tenure. 3- It is reasonably and consistently formulated and organized with the importance of the performed task. 4- It is compatible with secure procedure.

According to this article, secure information system is a kind of system that saves information in such a way that is available in time of need and on the other hand by maintaining privacy of data, prevents any penetration. Lawmaker, considers it necessary to exist "a reasonable level" of mentioned conditions for ensurance of an information system, according to reasonable measuring criterion presented in paragraph "N" of article 2 of electronic business law. The mentioned conditions are evaluated according to conditions of data transaction, skill and position of parties, transaction volumes of parties in similar cases, availability of proposed choices, common, reasonable and used methods in these transactions (Shahbazinia and Abdollahi, 1389:198).

Accepting electronic evidence in electronic business claims procedure: The most important part of procedure is related to computer technology supervising evidence for proving claim. Evidence for proving are proposed after crime so definition of computer evidence, its resource, way of obtaining, acceptability, how to present, how to issue a verdict in computer world are disputable issues. With emergence and evolution of information and their penetration into criminal procedures, the issue of Cyberia and computer evidence is presented. Issues like non-paper computer data and information, permanency, durability and their originality are proposed. Observable data and documents appear in monitor screen but they disappear, modified or removed with turning off the system or changing the file. The features of permanency and durablity don't have physical concepts and they lack the originality of formal documents as we can't consider a valuable copy or copies for them (Jafarpour, 1381: 2).

Essentially, the acceptability of evidence from computer documents in the court depends on fundamental principles of proving evidence in each country. Countries relied upon written law act based on the freedom principle of obtaining evidence and free assessment of evidence. Criminal systems based on these principles generally have no doubt in accepting computer documents as evidence and in countries based on Common Law, procedure is carried out orally and defensively. In these countries, witnesses on the basis of their observations, knowledge and experience give testimony and in this legal system, according to the rule (the best evidence) the original document (not the copy version) should be rendered to the court to be confirmed.

[DOR: 20.1001.1.26453460.2017.1.2.18.6]

About this issue that how computer and Cyberia texts are considered real evidence, there are so many arguments and rulers of some countries like England and Australia have ordained new laws that according to them, computer evidence under special conditions is considered as representable evidence to the court. One of the most important hindrances in reliability of Cyberia and computer information is that they can be easily changed. In non-electronic documents and evidence, this problem is recoverable by requesting the presenting original version instead of its copy, but in Cyberia environments we can't differentiate between original and copied version (as we can make original versions infinitely) and the mentioned ways for ensuring their authenticity are useless and we can hope that by encouraging lawmaker in using it, the risk of changing and forging it decreases. In some countries like England, this issue leads to establishing centers of confirming documents. The main questions are: should the document used for approving be original? If the copy version is acceptable, what are the acceptance conditions? In various countries, there are three different kinds of answers to these questions.

First: Countries in which there is no difference between original and copy version and each of them if presented, are acceptable. Denmark uses this procedure as it follows moral evidence system. In this system, judge can consider both versions of the document and assess decisively the validity of presented documents (Zandi, 1393: 271).

Second, countries that under special conditions accept the copy version of original documents. In Spain, Portugal and Greek for accepting the mentioned evidence, it should be formalized meaning that the process of discovery, investigation, custody, reserving and … are based on law. In Holland, Belgium and Italy the copy version is acceptable until it is faced with objection. In France and Lukzamburg the copy version is not accepted unless its original version has been destroyed and the authenticate copy of original version is available (Zandi, 1393:272).

Third: Countries that act upon the best evidence like England, Ireland, United States. In these countries based on the mentioned rule, a document isn't acceptable without presenting its original version and copy of the original is not accepted unless its owner prove that s/he couldn't get its original copy (Qajar Qionlo 1374: 29).

In the current legal system, lawmaker in Iran by accepting wonderful electronic transformations, tries to create required contexts for Cyberia evidence reliability. Along with this, lawmaker in Iran by ratification of electronic business law take long strides toward using computer technology and its evidence. Lawmaker in the second section of the mentioned law, under the subject of acceptance, assessing the proof, background and electronic signature, codifies regulations about document acceptance and digital evidence. On the basis of this, in article 12, it has been stated: "documents and evidence for claim proving may be in a message data and in any court or official organization no one can reject the proving value of message data merely based on its form". Article 13 also regards data value amount and differentiates them in terms of reliability level. According to this article, "generally, proving value of message data is determined based on decisive factors like the congruity of applied safety methods with the subject and transaction purpose of data message." Hence, Cyberia evidence and documents under some circumstances are formalized as claim proving or legal act in legal system of Iran and are accepted as legal evidence. Article 14 of electronic trade law states: "all of the messages created and maintained in a secure mode and both parties and their successors commit to their contents and signatures are considered reliable documents in legal systems." Computer crimes act ratified in 1388 also by accepting the significance of IT transformations and advancements in computer age, has predicted pretty comprehensive regulations against computer crimes and determines required strategies for discovery, pursuit, investigation and maintenance of Cyberia and electronic documents and evidence and tries to block the abuse of criminals from legal chasms. Acceptance or reliability of evidence by computer processing are faced with errors in most cases but for its understanding, there is no accurate tool, so their evidence come up with serious doubts. It should be said that these perspectives are fundamentally related to non-differentiating between hardware and software. In reality, hardware is rarely faced with errors and by

[DOR: 20.1001.1.26453460.2017.1.2.18.6]

careful treatments the possibility of their inaccurate function reaches to zero. The main errors are made in software and operations. So the computer programmer or a machine operator may give incorrect input data to the machine (Babazadeh, 1382, 21).

It should be noted that the main problem in acceptance of digital evidence is difficulty with confirming content authenticity. We mean content and information in computer memory. Therefore, it seems that when we succeed to consider technical strategies to assign accurately the computer data to their owners, then we can present it as an "evidence" to the court. Of course, it should be noted that besides these problems and for avoiding legal and technical deadlocks in law procedures of most countries, digital and electronic data can be described explicitly or implicitly as evidence in criminal procedure. Though there are essential differences in document values and their presentation, the main issue faced with all law procedures is acceptability and reliability of these evidence. The lawmaker ratified the electronic procedure section and law procedures of computer crimes on 1393/7/8 and annexed them to criminal law procedures on 1394/12/4 that have considerable effects on evidence for proving electronic business crimes and claims.

4. Discussion

Using electronic communications as a tool for performing various exchanges such as transactions brings about the important issue of electronic business to us. It has special significance related to other issues of information technology law and judicial justice because of virtual network features considering trial system in electronic business claims. If the process of discovery and obtaining electronic evidence is performed according to legal principles, and in addition to validity, integrity, reliability and undesirability issues, in this case, it can be basis of issue of order and the rules governing evidence proving claims are also used in electronic business claims. According to the proposed issues, the necessity of ratification of electronic business law procedures seems essential in electronic business court. In law system of Iran about legal procedures of electronic court, no law or regulation has been ratified or formulated yet and it is necessary for the lawmaker to examine this problem as soon as possible; therefore, we should currently use general rules of civil trial procedures in law.

References

Abdollahi M. (2008); Electronic evidence in legal claims, M.A. dissertation, Tarbiat Modares University.
Abdollahi M. (2012); Electronic evidence in evidence system for proving calim, first ed, Tehran, Khorsandi Press.
Allen M. Gutten (2004); Electronic evidence, translated by Mosayeb Ramezani: Infroming council secretariat, first edition.
Babazadeh Q. (2013); Discovery, investigation and pursuit of computer crimes, Informatics Newsletter, no 90. (2009), Civil procedure law, third vol, Tehran: Drak Press, fourteenth ed.
Jafarpour N. (2002); Procedure law of computer crimes, Informatics Newsletter, no 84.
Katozian N. (1995); Proof and evidence for proof, Mizan, first vol, Tehran: Mizan Press, Fifth ed.
Mahdipourattee Kh. (20011999); Electronic business, Tehran: Dibagaran Cultural Institute.
Qajar Qionlo S. (2005); Study of proving evidence in digital worlds (computer evidence) according to law system in Iran, Tehran, Informatic council secretariat of the country.
Qohestani S. (2017); Claim proving evidence in Cyberia crimes, M.A. dissertation, Islamic Azad University, Shiraz Branch.
Shahbazinia M, Abdollahi, M. (2019); Electronic evidence in system of evidence for proving claim, journal of law, Faculty of Law and Political Science, 40th ed, no 4.
Zandi M. (2014); Elementary research in Cyberia crimes, Tehran: Jungle Press, new and first edition.

[DOR: 20.1001.1.26453460.2017.1.2.18.6]