Lex Humana, Petrópolis, v. 12, n. 2, p. 34-45, 2020, ISSN 2175-0947
© Universidade Católica de Petrópolis, Petrópolis, Rio de Janeiro, Brasil

CREDIBILITY OF ELECTRONIC DOCUMENTS IN LAW SYSTEM IN IRAN

CREDIBILIDADE DOS DOCUMENTOS ELETRÔNICOS NO SISTEMA JURÍDICO DO IRÃ*

KHALIL AFANDAK**
ISLAMIC AZAD UNIVERSITY, AHAR, IRAN

MINA MEHRVAND***
ISLAMIC AZAD UNIVERSITY, AHAR, IRAN

Abstract: In modern time, data uploaded in internet and virtual world can be posed as documents in claims in court if one can prove their precision to relate them to ordinary citizens or legal entities and it can help the judge greatly in law issues. Can we present any type of electronic documents to the court as evidences? The credibility of electronic documents refers to the validity of electronic data for the court and using it in making the final decisions. In order to use electronic documents like the traditional documents, they should observe two major conditions of credibility as the properness of the assignment, originality and being undeniable. On the whole, the acceptance of these documents as reasons depends on the validity of such documents for the judge in the trial. Regarding the fact that in computer atmosphere one can easily manipulate, change, copy, and delete electronic data it is natural that the magistrate will treat the validity of the documents mentioned very cautiously and in normal states will optimally consider them as a peripheral reasoning for the claims. The author of the present study has utilized a descriptive-analytic method to investigate about the credibility of electronic documents in law system in Iran and has concluded that electronic documents do have credibility and validity in legal system in Iran as like as the traditional documentation and the proof value of such documents depend on the safety level of the technology.

Keywords: Criminal law. Criminal proceedings. Digital documents. Credibility.

Resumo: Nos tempos modernos, os dados carregados na internet e no mundo virtual podem ser apresentados como documentos em ações judiciais se for possível provar sua precisão para relacioná-los a cidadãos comuns ou pessoas jurídicas e isso pode ajudar muito o juiz em questões jurídicas. Podemos apresentar ao tribunal algum tipo de documento eletrônico como prova? A credibilidade dos documentos eletrônicos refere-se à validade dos dados eletrônicos para o tribunal e ao uso deles na tomada de decisões finais. Para utilizar documentos eletrônicos como os documentos tradicionais, eles devem observar duas condições principais de credibilidade como a justeza da cessão, originalidade e inegável. Em geral, a aceitação desses documentos como motivos depende da validade de tais documentos para o juiz no julgamento. Quanto ao fato de que em

* Artigo recebido em 13/12/2020 e aprovado para publicação pelo Conselho Editorial em 20/12/2020.
** Islamic Azad University, Iran. E-mail: kh.afandak@gmail.com. Orcid: http://orcid.org/0000-0002-6900-7193.

*** Islamic Azad University, Iran. E-mail: mi.mehrvand@gmail.com. Orcid: http://orcid.org/0000-0003-2662-1908.

ambiente de computador pode-se facilmente manipular, alterar, copiar e deletar dados eletrônicos, é natural que o magistrado trate a validade dos documentos mencionados com muita cautela e em estados normais os considere idealmente como um raciocínio periférico para o reivindicações. O autor do presente estudo utilizou um método descritivo-analítico para investigar sobre a credibilidade dos documentos eletrônicos no sistema jurídico no Irã e concluiu que os documentos eletrônicos têm credibilidade e validade no sistema jurídico no Irã, assim como a documentação tradicional e a o valor da prova de tais documentos depende do nível de segurança da tecnologia.

Palavras-chave: Direito penal. Processo penal. Documentos digitais. Credibilidade.

1- Introduction

As international internet networks are developing, the use of computer networks has increasingly been growing. Along with the increase of joining such networks, legal issues such as private law and criminal law have been emerged to be important because electronic environment and internet is different from physical environment and touchable geographical environment through which the traditional law system works, in a way that this environment is completely untouchable and virtual and does not know any territory. This has led to issues such as the place of signing a treaty and the location to administer it and the recognition of rules governing the relationships between the two parties in a compromise in private law and issues such as documents presented to prove the claims regarding internet crimes, and the qualification of courts regarding the crimes in criminal law.

On the whole, computer systems and cyber environment following that, have resulted in three perspectives of crimes' changes: there are some crimes that do not have any dependence on cyber environments regarding the commitment but the documents and effects remained in cyber environments can play an effective role in their proof. Another group of crimes refers to those that although do not depend on cyber environments regarding commitment, if such environments are utilized there would result in even overestimated outcomes. Also there are the third group of crimes that are directly related to cyber environments. In other words, this environment not only provides the situation and the tools to commit such crimes, but it can be affected by crimes greatly and since according to the principles of criminal law their constituents are different, they can not be investigated using the current criminal laws and as it can be observed, many countries have devised and approved some new rules or reformed their current law systems in a way that they can provide the possibility of judging such issues. Today you can almost find no crime that is completely unrelated to cyber environments.

In the past, the documents were only presented in traditional forms such as confession, documents, witnesses, statistics, swear, but after the emergence of information technologies and communication media and their utilization in daily life, a new type of document was introduced called electronic document. After the approval of electronic commerce rule, this type of document was accepted as a new type of proof along with traditional documents in claim proof systems and it can be used to prove claims.

2- The definition of electronic documents

The document is literally meant as a guide, leader, manual, and the route of a representative (DEHKHODA, 1962; 191). The document means as a guide in law system in Turkey and in literal law definition, it means as a tool that shows the occurrence of an incident in real world (MAHMOUDI AND POURZANGBAR, 2014; 34). Also the document to prove a claim (legal document) refers to any legal tool which satisfies the magistrate in any claim proof and it is useful information for the judge (SAFFAR, 2009; 423).

The document means a guide. In article 194 of the civil magistrate law, it can be observed that: "the document is something the parties use to prove or defend a claim" (Katouzian, 2009; 42). In criminal law in Iran there has not been any precise definition about document and only in article 160 of Islamic punishment law approved in 2013, the legislator has defined the documents as: "documents to prove crimes are confession, witness, swear within the realm of cases devised by the law and the knowledge of the judge". As we take a careful look at this definition we can observe that the legislator has mentioned the knowledge of the judge as one of the documents and there is not any violation of the previous rules by Islamic punishments regarding the documentation of the knowledge of judge in claim of the people and rights known as the divine ones and the satisfaction of the spirit of the judge has become important increasingly. Therefore, the judge is free to act as he likes both in document compilation stage and its assessment within the framework of the law system and he can use electronic documents to prove and to enact the crimes. Meanwhile, there has not been any definition posed for such documents in criminal magistrate law system approved in 1993 (reformed in 1995) in the section appropriated to electronic trials.

Electronic document refers to: "any message data documented by the parties in a trial to prove or to defend their claims" (SHAHBAZNIA, 2010; 208). According to this definition, electronic documents are defined using message data explained completely in article 2 of electronic commerce rule. (article 2 of electronic commerce rule: it refers to any symbol of the incident, information or concept that can be produced, sent, received, saved, or processed using electronic, light or novel

information technologies). The legislator has used the law of electronic commerce sample law called Ancitral, electronic commerce law and article 47 of the credibility of electronic documents approved in 2014 to avoid considering message data as the only form of electronic tools and has accepted any other types of documents such as telegram, telex, light tools, and other tools resulted from information technologies' development such as audio and video files as electronic documents.

Electronic documents are not bound to computer and include all referred data of electronic tools such as mobile, fax, telephone pager, phone messenger, audio messages, electronic messages and others (MOHTASHAMI, 2010; 79). The specific nature of electronic document has led to doubts in properness and completeness of electronic documents. We should investigate about how to utilize these data in the process of criminal trials and what characteristics should computer data have in order to be documented by the verdicts in the court and how they should be useful for the knowledge of the judge (KARIMI, 2011; 2).

Regarding the fact that the document assessment in legal system in Iran is bound to five types of confession, written documents, witness, statistics, and swear, in order to provide positive documents for the court, a document should involve one of the forms mentioned above. But in electronic commerce law, without reforms in current articles, electronic documents refer to a new concept of documents equal to the traditional documents that can take any form of the traditional formats and can benefit the approval value in that format (ABDOLLAHI, 2012; 20 & 96).

3- Advantages of electronic documents

On the whole, electronic data have some privileges that physical documents lack. The major part of such advantages is due to the fact that electronic data can be represented in completely different formats in a way that the things not found in the form of computer versions and are exposed to us can not be found in computer systems and are due to a set of 0 and 1 arranged next to each other based on precise mathematical formulae and algorithms. This difference in emerging in different formats exerts countless advantages on electronic data unlike physical documents that exist only in one format everywhere. Some of these characteristics are as follows:

1) Electronic data can be copied precisely, in a way that the only way to isolate the original from the copy is to refer to a set of specifically recorded data in the intended computer system. Meanwhile, such thing can not be applied in paper documents and we can never prepare the exact copy even using copy machines with highest precision as it can be done by electronic copy machines or the print output of electronic data.

2) Due to the fact that the data are in a flexible electronic form and there exist the possibility of precise copying, we can easily apply any type of change and reform on copy versions as in the original version and maintain the original document. It should be noted that such thing is not possible in physical documents. Because first there is not possibility of copying all things and copying mainly can be applied to paper documents and second even in such cases we can not get completely equal copies of the original documents.
3) Another outstanding advantage of electronic data compared to physical documents is that we can record any change or reform applied in isolated files and accordingly we can utilize the tools and varied applications programmed and produced to understand the changes applied to the documents. For example, the message regulation algorithm acts like the black box of the airplane and produces 32 digits for each input. Therefore, even when very trivial changes occur, there would result completely different messages. The other very important advantage of electronic records compared to physical records is that it is difficult to destroy them. The thing we really do when we delete some documents is not their deletion, but we make them inaccessible and save them in slack spaces and unappropriated spaces of the disks and we can recover most of them using special tools.
4) The last characteristic to be noted here is the nature of cyber spaces. If computer data are expelled from a computer system using offline status and are released in cyber spaces, their copies will be saved in many points. This can lead to minimize the decay of documents on the one hand and increase the credibility of them for the court using electronic and varied records, on the other hand.

4- Weak points of electronic documents

On the contrary to considerable advantages of electronic data, they are vulnerable. These data are inconsistent and easily deleted or as it was mentioned above, there is not possibility of recognizing any changes in them and we should not forget that making changes in them is a very easy task while there is a need for certain and developed tools, experienced and skillful workforce and a great deal of efforts to recognize them. Also, such data can be easily depleted. It is enough to add a not completely modern application onto your system and adjust it in a way that you can easily tap on the keyboard several times to delete all the intended data. Sometimes the professional cyber criminals delete their criminal documents in a way that we can not retrieve the contents even using very modern tools. Anyway, the vulnerability of electronic data can be summarized regarding three factors as follows:

1) **Faults in the system or saving medium:** one of the major differences between electronic documents and physical documents is that they are not found out in the real world out and their existence always depends on the presence of a computer. Thus, any type of change in system status can affect the position of the data.
2) **Faults in the programs:** undoubtedly, any data entered into a computer system is being processed by the computer in some way. Even the mere maintenance or saving the data in a system or their transfer into a medium is known as a processing. It is clear that we need a certain program for any type of processing to process the intended data based on the predetermined manual. In this way, even in simplest possible state the data depend completely on one or several programs and if the programs have problems they would encounter problems too and the output of the data will be affected directly. Easy accessibility of unauthorized people to a document or physical evidence could be applicable for a limited number of people. Thus, we can use some guidelines to minimize the probable access of unauthorized people. Such issue can be applied regarding data present in independent computer systems too, because there are few people who exploit them. But when such data are uploaded online in cyber spaces, due to the possibilities in cyber spaces proposed for the public, by applying and administering varied applications whose work processes require high profession, we can have access to them and it should be noted that this means the high vulnerability of online and offline electronic data and basically the data with internet origins are unreliable.

Credibility of electronic documents in law system in Iran

The credibility of electronic documents refers to the validity of electronic data for the courts and their role in announcements of the related verdicts. To make electronic documents credible they should have the following conditions: **first:** presentation capability; in computer environments the recording of documents should be in a way that when needed, they could be presented and reproduced and the law should have formalized its validity, or else when there is debates, they can not be presented to the court to make the case clear. **Second**: originality; computer information can be easily changed and copied; thus, it is impossible to isolate the originals from the copies. **Third:** the capability to create common knowledge; knowledge means the awareness of one regarding the nature of surrounding incidents and phenomena, in such a way that after assessing the evidences, states and conditions dominating the outer world phenomena and after realizing the possibility, there would not be any protests against the verdicts.

In legal system in Iran and in article 1258 of the civil law and in section 10 of the magistrate civil law there exist different types of documents as follows: confession, written documents, witness, swear, location check, surveys in the location and expert opinion. Nearly all lawyers have a consensus that the documents mentioned here are bound and the only document is considered valid that involves one of the proof reasons of the documents mentioned to prove a claim. Regarding this issue, the experts have proposed two approaches: based on the first approach, since electronic documents are not in any forms of those validated by the legal system, this type of documentation should be considered as a new type of document (ABBASI KALIMANI, 2006; 62). But regarding the second approach, it is believed that since in legal system in Iran there is importance in applied cases not emphasis on forms, we can utilize equalizing methods. This method first identifies the goals and functions of the elements of traditional documents and then introduces the satisfaction method for such functions using electronic documents. Using this approach will result in satisfying the need to approve the credibility of electronic documents (HASSAN BEIGI, 2005; 56). It seems that in legal system in Iran, the satisfaction method has been used in credibility of criminal documents. The sample rule of Anciteral uses the same method.

In legislation system in Iran and in article 50 of computer crimes, the legislator has proposed two conditions to document computer data: first – computer data should be created or processed or saved or transferred through the claim party or a third party not aware of the claim. Second – the correctness, completeness, validity, and undeniable feature of the data should not be violated. By applying the two conditions above, it seems that there is a controversy in the first condition and the legislator has considered the claim party as the same with the third party who is not beneficiary, incumbent, processor, saving entity, or the transfer agent of the data. Meanwhile, the person may be the claim party and may not have any biased intentions; but there can exist such a doubt in the mind that comparing this person with the third party who is not aware of the claim is not so favorable and it is somehow considered as the violation of the second condition. By computer data meant in article 50 of computer crimes, the very same items in article 32 of this law consider the following: traffic data, user information, content data. In article 35 of computer crimes, it has been stated that: "the judicial incumbent can order the persons to present maintained data above in articles 33, 22 and 34 (refer to notes) to the officers. The one who evades the administration of such orders will be sentences with the punishments stated in article 34. Due to the fact that the items mentioned are found in the section entitled with maintenance and presentation of the data, it seems that all three types of data such as traffic, user, and content unless the content could be presented to the judicial offices and should be maintained in a proper way and in such a way that

there happens no harms to the originality, completeness, and lack of their undeniable nature. The reason for this clam is to follow the document acceptance system in Iran regarding an integrated documentation system through which any document without considering the content to satisfy the judge has approval value and this has clearly been explained in articles 161 and 162 of Islamic punishment law approved in 2013. To put an approval to such a claim in credibility manual of electronic documents approved in 2014, the articles 7, 16, 18, and 35 have explained in details.

Conclusion:

Currently you cannot find any legal system where electronic documents are not utilized for approval. The German Roman law countries consider the value in dealing with electronic documents that the law have appropriated for such a group of documents and in common law countries the approval value of documents are determined by the judge in courts based on the topic of the file and the situation dominating the case and the identification of the amount of the value of such documents is left to the judge. Also in legal systems based on Ancitral, the law systems through which rules are devised based on the articles in international Ancitral treaty approved by United Nations Organization, such as Iran and Turkey, there exists a dual system. This means that the approval of a certain claim has a specific legal value and the approval value of other approval documents in uncertain claims is left to the judge (SHAHBAZINIA, 2012; 121).

In judgment processes in Iran, there have been many doubts about the acceptance of digital documents but finally the approval of electronic commerce law in the year 2003 led to recognize the credibility value of such documents by the legislator. (as mentioned in articles 12, 13, and 14 of electronic commerce law, refer to notes). Also the credibility of digital documents has been mentioned in computer crimes' punishment law. In this law, where there exist very detailed regulations regarding the discovery, probe, stop, save and maintenance of digital documents, the acceptance of digital documents gained properly has been emphasized. Finally, after the approval of computer crimes' punishment law in year 2009, such an inefficiency in criminal law was stopped in Iran, but we cannot consider it as a complete set to avoid the problems related to credibility of digital documentation in Iran.

References

1- DEHKHODA, ALIAKBAR. (1962). Dehkhoda Encyclopedia. Tehran, Tehran University Publications.

2- SAFFAR, MOHAMMAD JAVAD. (2009). Legal entities. First edition, Behnami Publications.
3- KATOUZIAN, NASSER. (2009). Approval and approval documents. 6th edition, Tehran, Mizan Publications.
4- SHAHBAZINIA, MORTEZA; ABDOLLAHI, MAHBOUBEH. (2010). Electronic documents in claim approval systems. Quarterly Journal of the Department of Law and Political Sciences, Vol. 40, No. 4, Winter 2010, PP: 193-205.
5- KARIMI, MOHSEN. (2011). Collection and credibility of electronic documents in criminal law in Iran. Allameh Tabatabaei University.
6- ABDOLLAHI, MAHBOUBEH. (2012). Electronic documents in claim approval systems. First edition, Tehran, Khorsandi Publications.
7- ABBASI KALIMANI, ATEFEH. (2006). A comparative study of internet crimes in legal system of Iran and international documents. Qom Paradise of Tehran University.
8- HASSANBEIGI, EBRAHIM. (2005). Law and safety in cyber spaces. First edition, Tehran, The Institute of International Studies and Research of Abrar-e-Moaser Tehran.

Notes:

Articles of Computer Crimes' Punishment Law

Article 32- the providers of access services are responsible to maintain traffic data at least for 6 months after the creation and the users' information should be kept at least for 6 months after the end of the subscription.

Article 33- local host service providers are responsible to maintain the data of their users at least for 6 months after the end of subscription and the content saved and traffic data resulted from the changes created should be kept at least for 15 days.

Article 34- when there is a need to maintain computer data for probes or trials, the judicial incumbent can order to keep them safe for persons who somehow dominate or control them. In emergencies, such as hurts or changes or the deletion of data, the judicial officers can issue the order to maintain them and can report it to the judicial incumbents at most 24 hours afterwards. If any of government officers or judicial officers or other persons avoid administering the order or reveal the preserved data or persons with the data mentioned are informed about the articles in the order, the judicial officers and government officers will be sentenced with imprisonment from 91 days to 6 months or cash fares of 5 million Rials to 10 million Rials or both punishments.

Article 34- No. 1- the preservation of data does not mean to present or reveal them and requires the observation of related regulations.

Article 34- No. 2- the time span to preserve the data is 3 months at most and if needed, it can be postponed further with the order of a judicial incumbent.

Islamic Punishment Law

Article 161- in cases through which criminal claims are approved using religious documentation such as confession and attestation, the judge can issue verdict unless the counter approval is brought to the court.

Article 162- when the documents do not have the required religious and legal conditions, they can be used as judicial justifications. This is so if other conditions lead to judge's knowledge.

Electronic Document Credibility Law

Article 7- content data and traffic data and users' data should be kept, maintained, stopped, and presented based on this regulation in a way that the properness and completeness, confidentiality, validity, and lack of undeniable characteristic of them should be maintained.

Article 16- preserving the data should be in a way that confidentiality, completeness, properness, and lack of undeniable characteristics of the data should be observed.

Article 18- data presentation should be in a way that confidentiality, completeness, properness, and lack of undeniable characteristics of the data is observed and possibly is maintained without creation of obstacles for the activity of the terminal or through the known methods and with low costs using the following methods:

a) The delivery of a printed copy of the data
b) The delivery of a computerized copy of the data
c) Creation of access to the data
d) The transfer of computer and communication equipment

Article 35- the probe on data or terminals in locations or through the network or in the laboratory or the appropriate location with an order issued by the judicial incumbent should be carried observing confidentiality, completeness, properness, and lack of undeniable characteristics of the data.

Electronic Commerce Law

Article 12- the documentation and claim approval documents may be in the form of message data and the validity of any message data can not be denied due to its format and framework based on current documentation principles in any court or governmental office.

Article 13- on the whole, the approval value of message data can be identified through certain factors such as appropriation and safety methods utilized in order to exchange the message data.

Article 14- all message data created and maintained through a secure method are considered valid regarding the contents and the signature on them and they are considered valid regarding the commitments of the parties and the party that has committed to perform in a certain way and all persons who are considered their legal representatives. The administration of the items in this rule and other effects are considered as the valid and credible documents in judicial offices and legal institutions.

Universidade Católica de Petrópolis
Centro de Teologia e Humanidades
Rua Benjamin Constant, 213 – Centro – Petrópolis
Tel: (24) 2244-4000
synesis@ucp.br
http://seer.ucp.br/seer/index.php?journal=synesis

CC BY NC

AFANDAK, Khalil; MEHRVAND, Mina. CREDIBILITY OF ELECTRONIC DOCUMENTS IN LAW SYSTEM IN IRAN. **Lex Humana**, v. 12, n. 2, p. 34-45, mar. 2021. ISSN 2175-0947. Disponível em: <http://seer.ucp.br/seer/index.php/LexHumana/article/view/2027>