ARTICLE:

THE EVIDENTIAL VALUE OF THE DATA-MESSAGE IN IRAN

WRITTEN BY:
DR AHAD GHOLIZADEH

Introduction

The borderless, inexpensive, instant nature of the internet has made products easily available to consumers worldwide in a manner that has never existed previously, and spurred the growth of e-commerce internationally. In this connection, decades ago, there might have been controversy surrounding admissibility of data-messages in litigation, but it is now routine. Therefore, at present, the clear global trend is toward a wider recognition of the legal validity of electronic records. Many different jurisdictions have now recognized the legal validity and enforceability of electronic records and documents. Iran joined them in 2004. As a prototype, Iran's legislature has used the UNCITRAL Model Law on E-Commerce.[1]

Parallel with developments in e-commerce, the doubts on admissibility of electronic records previously held by legal institutions are rapidly disappearing. Today, electronic records are widely accepted by courts and other legal bodies. Advances in information technology and the corresponding increase in comfort and familiarity that the legal community has developed with those systems have largely driven this widespread acceptance. New statutes and rules that mandate such acceptance have also facilitated acceptance of electronic data-messages as evidence.[2] Not only contracts, but also any information stored in electronic form may, at some point, need to be introduced as evidence in legal proceedings. A business may need to bring in electronic records to prove the existence of a contract, or may wish to contest the authenticity of an electronic record, or the accuracy of the information it contains in order to disprove the existence of a contract. Also, in litigation, electronic records may be required to prove the facts of liability. Further, electronic records as evidence in jurisdictions around the world, are relevant in litigation between private parties and in cases initiated by governments.

Evidence consists of information that assists a court or other legal institution to identify facts relevant to the dispute. It contains testimony, writings, records, material objects, or other things. According to Article 194 of the Civil Procedure Act of 2000, "evidence is a means which the litigants use either for establishing a case or defending the case," and according to Article 1258 of the Civil Code of 1934, it includes confessions, written documents, oral testimony, indications and oaths.

Types of data-message

Electronic records are widely accepted by courts and other legal bodies. Advances in information technology and the corresponding increase in comfort and familiarity that the legal community has developed with those systems, have largely driven this widespread acceptance. New statutes and rules that mandate such acceptance have also facilitated acceptance of electronic data-messages as evidence. According to Article 2 of the Electronic Commerce Act of 2004 (hereafter E-commerce Act)

> "'data-message' means any symbol of event, information or concept, which is generated, sent, received, stored, or processed with electronic, optical, or new information technology means."

Therefore, in Iran, whatever is visible on a screen on a computer, such as text, photographs, schedules, maps, tables, charts, films, animations, and so on, are

[1] *The United Nations Commission on International Trade Law (UNCITRAL) made special attention to data-messages which indicate the conclusion of contracts, and in order to support the need for valid, internationally recognized commercial contracts in electronic commerce, developed a model law on e-commerce that defines the characteristics of a valid electronic contract for e-commerce, provides default rules and norms for the formation and performance of such contracts, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in arbitration and litigation proceedings.*

[2] *Jeffrey H. Matsuura, Security, Rights, & Liabilities in E-Commerce (Artech House Computer Security Series, 2002), p 19.*

In comparison to paper documents, the sender or receiver can easily change data-messages, and those changes cannot easily be seen without proper professional and technical help.

considered as data-messages. Music also as a symbol of event can be considered as a data-message. These all may be used for the introduction, advertisement, sale or purchase of goods. So, a message sent by e-mail is an example of a data-message, whether it is for commercial or non-commercial purposes.

It is important to remember that digital evidence (data-message) does not just refer to evidence found on personal computers. Computers (in the form of microprocessors, circuits, and memory devices) are also used in watches, pagers, telephones, cars, and many other modern machines. Digital evidence can also originate from these computers.[3] Similar definitions from data-message have been made in other countries. For example, according to Section 6-c of the Implementing Rules and Regulations of the Philippines Electronic Commerce Act 2000, Republic Act No 8792, "electronic data message" refers to information generated, sent, received or stored by electronic, optical or similar means'. Data-messages are a key component of evidence.

The E-commerce Act does not clearly make a distinction between different kinds of data-messages. Computer generated documentary evidence is of three types. First, calculations or analyses that are generated by the computer itself through the running of software and the receipt of information from other devices, such as built-in clocks and remote sensors. For example, in the case of the transfer of an e-mail message, the time and IP address are often recorded in a file on the mail server. Similarly, when viewing a web page, similar information related to the viewer is usually logged on the server. As another example, a bank computer automatically calculates the bank charges due from a customer based upon its tariff, the transactions on the account and the daily cleared credit balance. Secondly, documents and records produced by the computer that are copies of information supplied by human beings, such as cheques drawn, and paying-in slips credited to a bank account. Finally, derived evidence that is a product of a combination of included computer generated information and information supplied to the computer by human beings to form a composite record. However, with respect to evidential value, the E-commerce Act does not make any difference between these messages. But with regard to the Civil Code, each of these messages may be deemed as confession, testimony, document or indication, and will be valued accordingly.

Data-messages are easier than paper documents for others to obtain access to. Therefore they may be trapped by hackers or affected by viruses. In comparison to paper documents, the sender or receiver can easily change data-messages, and those changes cannot easily be seen without proper professional and technical help.[4] Therefore, such a document may not be reliable against the sender. Besides, a data-message can also be easily deleted. Hence, in Iran, when a party loses or destroys a data-message relating to a lawsuit, the presumption arises that the data-message was harmful to him or her.

However, around the world, avoiding court-imposed sanctions or tort liability for evidence spoliation is particularly challenging with respect to electronic data-messages, including e-mail. This is because where a firm retains back-up copies of all e-mail messages, it may face significant time costs in sorting through those messages to satisfy a request for document during discovery, and, if it deletes e-mails that could be crucial evidence in bringing or defending against a lawsuit, it may face significant sanctions. To solve the problem, it is suggested that there should be a media centric view of preserving electronic records and hard drives, floppy disks, or back-up tapes containing pertinent data rather

[3] *Eoghan Casey, Digital Evidence and Computer Crime (Academic Press, 2nd edition, 2004), p 66.*

[4] *See Naahid Ja' farpoor, "Procedure of computer crimes", Informatics Bulletin, 2002, no. 84 (in Farsi), p 42.*

[5] *Troy Larson, "The Other Side of Civil Discovery: Disclosure and Productions of Electronic Records", in Handbook of Computer Crime Investigation, ed. Eoghan Casey, (Academic Press, 2002), p 31.*

By employing an expert, the judge is able to assess the level of security over the data-message, and the level of security determines the level of the reliability of the data-message.

than just the data itself, and it is these that should be preserved.[5] This is more relevant in Iran, because according to the provisions of the Civil Procedure Act, any lapse of time does not prevent a party from filing a case before the court. That is to say, there is no statute of limitation barring the civil cases.

Data-message as legal evidence

With respect to the above debate, there is no doubt that a data-message is a means of proof, mainly a written document, and can also be a container for confessions, testimony, or indications. Due to this specification of the data-message, article 12 of the E-commerce Act provides that "documents and evidence in substantiation of claims may be in the form of data-message and in no court or governmental department can on the basis of existing principles of evidence, reject the proving value of the data-message solely due to its form and framework." But the evidential value of a data-message depends on the degree of security. This is because many of the fears relating to the expansion of e-commerce, particularly over open networks, such as the internet, deal with the risks of possible fraud, security infractions, counterfeiting, and privacy issues.

Consequently, article 13 of the e-commerce Act provides, "in general, the evidential value of a data-message is determined with respect to items used to guarantee its security including fitness of applied security methods with its subject and purpose of the data-message." But despite contrasting opinion,[6] the legislature has not left the value of data-message under the discretion of judges or admitting authorities.[7] By employing an expert, the judge is able to assess the level of security over the data-message, and the level of security determines the level of the reliability of the data-message. Other countries also have the same attitude towards the value of a data-message. For example, according to s6 of the Philippines Electronic Commerce Act 2000, providing for the recognition and use of electronic commercial and non-commercial transactions and documents, "information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data-message purporting to give rise to such legal effect, or that it is merely referred to in that electronic data-message."

Therefore, in many countries it is clear that the law no longer necessitates paper originals in the context of the facts of a transaction. It establishes the concept that electronic data-messages and traditional hard copy records have equal value as proof of a commercial transaction. It also establishes the principle that the legal validity of a record cannot be challenged merely because it is in electronic form. These laws simply grant electronic data-messages legal status equal to paper records. On the contrary, documents and records in electronic form should not be assumed to be truthful or accurate simply because of their form.

According to article 6 of the E-commerce Act:

> "in case the existence of a written document is legally required, a data-message is deemed as a written document, unless in below cases:
>
> Ownership deeds of immovable properties,
> Sale of drugs to final consumers,
>
> Announcement, notification, forewarns and or similar phrases containing special instructions for the use of goods, or prohibiting certain methods, whether in the manner of action or omission."

Other countries have also made similar exceptions. For example, the Electronic Signatures in Global and National Commerce (E-SIGN) provides for exceptions for

[6] *Sattaar Zarkalaam, "E-signature and its situation in legal evidences regime", (in Farsi), Modarrese Olume Ensaani Journal, 2003, no. 1, pp 53-4; Siaamak Ghaajaar, (2005), "Introduction to legal dimensions of e-commerce in Iran" (in Farsi), Collection of papers presented at the 2nd conference on e-commerce, Ministry of commerce, Deputy of planning and economic surveys, p 373.*

[7] *An admitting authority is an administrative authority to whom data-messages are presented as evidence.*

data-messages generated in such non-commercial contexts as the creation and execution of wills, codicils, or testamentary trusts; family-law matters such as adoption or divorce; and documents filed with or issued by courts in the framework of litigation. In addition, E-SIGN does not apply to notices of cancellation or termination, or the right to cure under a credit agreement secured by, or a rental agreement for, a primary residence of an individual; cancellation or termination of health insurance or benefits or life-insurance benefits (excluding annuities); recall of a product, or material failure of a product, that risks putting health or safety in danger; or documents needed to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

Despite contrasting opinion,[8] the evidential value of data-messages and electronic signatures considered in the E-commerce Act automatically extends to other Acts, such as issues concerning civil law, civil procedure, criminal law, criminal procedure, commerce law and so on. In fact, with respect to data-messages, the provisions of the E-commerce Act overrule the provisions of all other similar Acts.

Also, it is said that, "one of the achievements of information technology is an overall change in the legal evidences regime." [9] But this is not true. Almost nothing in the legal evidence regime is changed by information technology. Every thing is the same. Only data-messages were added to other proofs, and their place among the other proofs have been determined.

Evidential types of data-message

A writing may be in forms of a confession (when it is presented to the court by the confessor), a testimony (when its contents are stated by a person other than the litigants), an indication (when a writing other than a confession or a testimony letter, indicates some relevant facts) and a document (when a writing other than a letter of confession, indication, or testimony is presented by a litigant).

Therefore, undoubtedly, data-message as writing can be a proof. But if so, the next issue is what kind of proof, whether it is official or ordinary. With reference to article 6(A) of the E-Commerce Act, a data-message cannot substitute ownership deeds of immovable properties. Immovable properties are of two kinds: registered (notarized) and unregistered (non-notarized). In general, registered immovable properties cannot be transferred by ordinary documents, whereas there is no restriction for the transfer of unregistered immovable properties by ordinary documents, therefore article 6(A) cannot help to determine whether the data-message is an ordinary or an official document in Iran.

Official and ordinary documents differ in value. An official document is much stronger than the ordinary one. According to article 1292 of the Civil Code

> "denial and expression of doubt (demur) is inaudible (unacceptable by the court) against official documents or documents which have the value of official documents, but the party can claim that the documents have been forged or prove that they have for some reason lost their authority".

Whereas, in addition to claims of forgery and losing authority, according to article 216 of the Civil Procedure Act of 2000, "any person against whom a non-official (ordinary) document has been presented may deny the handwriting or the seal or the signature attributed to him and if the document is not attributed to the defendant he may demur".

Also, according to article 1305 of the Civil Code, "in official documents the date of drawing up (of the document) is valid, even against third persons, but in ordinary documents the date is valid only in respect of those persons who have had participation in their drawing up and their heirs and the person in whose favour a will has been made". Further, according to articles 22, 24, and 72 of the Act on Registration of Documents and Immovable Properties, 1931, registration of immovable properties, and also transactions on registered immovable properties are valid also against third persons. Furthermore, with reference to article 1334 of the Civil Code, "...the person who has made a confession may request an oath, for what he claims, to be taken by the other party, except where the suit raised by the claimant is supported by an official document or a document the validity of which has been established in the court."

The legislature has given attention to the above problem, so article 15 of the E-commerce Act provides that

> "in respect to secure data-message, secure electronic records and secure electronic signature denial and demur is inaudible and only the party can claim that the data-message has been forged or prove that the

[8] *Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", Kaanoon Journal, 2005, no. 55 (in Farsi), pp 57-94.*

[9] *Sattaar Zarkalaam, "E-signature and its situation in legal evidences regime", p 34.*

said data-message has for some reason lost its authority."

Therefore, merely in respect to preventing a litigant from denying or demurring the document, a secure data-message is dealt with as an official document. This is an exception, and in comparison to paper documents, the legislature has given support to data-messages; because, a paper document would not be prevented from being denied or demurred unless it is formed according to article 1287 of the Civil Code, but secure data-messages, without any need to comply with the provisions of that Article, are deemed as undeniable and un-demur-able. However, despite contrasting opinion,[10] it cannot absolutely be concluded that a secure data-message is a formal (notarized or non-notarized) document. In this connection, it has been said that "titled as official or semi official cannot officiate a document, even if the title has been given by the legislature. Hence, provisions of the article 15 of E-commerce Act are expressly against other provisions concerning official documents and proofs."[11] It is suggested that this conclusion is wrong, because the legislature has not provided that the data-message is official, only the secure data-messages have been given a status similar to official documents, which is only good against deny and demur. Also, it is under the discretion of the legislature to deem something as official without requiring it to comply with provisions of article 1287. It is also wrong, without any reason, to assert that the legislature has authenticated the photostat copies of data-messages.

But this is sufficient about secure data-message; with respect to article 6 of the Act, an insecure data-message is deemed as ordinary document. However, to define a secure data-message, article 14 of the Act provides that

"all data-messages, which are generated and stored via secure method, are deemed as valid documents and are reliable in legal and judicial forums in respect of their contents and signature made therein, parties obligations or the party who has promised and all persons who legally substitute them, application of their contents and other consequences."

Therefore, the legislature states that secure data-message is a data-message generated and stored in a secure way.

To define a secure method, article 2(l) defines 'secure method' as "a method for comparing authenticity of data-messages' recording, its source and destination with determining date and for detecting any kind of fault or modification in communication, contents or data-messages storage from a certain moment." The aim of computer and network security is to protect network-connected resources against unauthorized disclosure, modification, utilization, restriction, close down, or destruction. Therefore, the security of data-message depends on the software used for the purpose of securing the production, dispatching, receiving, saving and processing of electronic documents.

Despite some comments,[12] it is wrong to suppose that secure data-messages are those produced in CSP (Certification Service Provider) offices, bearing signatures confined by them. Articles 10 to 16 of the E-commerce Act do not confirm such comments. With regard to article 31, electronic signatures provided by Certificate Authorities are one type of the many kinds of signatures available. In fact, with regard to articles 2 (H, I & K), 10 and 11 of the E-commerce Act, security is a matter of software, and not a matter of signature. In case the software applies the secure method (as provided in article 2(l)), the data-message and signature generated and transmitted in its environment are secure ones, otherwise they are not secure even if they are generated in the office of a Certificate Authority. A digital certificate defines and confirms a general key (within a PKI) for persons. This certificate would be issued by a recognized and reliable authority, which is called a Certification Authority. In this way, as Mason asserts, the signing party using a key pair (private and public key) affixes the digital (or cryptographic) signature using the private key and the recipient checks the signature with the public key.[13] If the signature was used, the Certification Authority proves that the public key is merely confined to a particular person.

Giving sympathy to notary offices, it is said that "CSPs do not have a right to confirm the certifications given by them, and that must be done by the notary offices".[14] But with regard to the express provisions of article 31 concerning certification of electronic signatures as genuine, this opinion cannot be correct.

Despite some attempts to bring every electronic document into compliance with the requirements of notarization,[15] data-messages are not, on the face of them, notarized documents. Therefore, the originator

[10] *Sattaar Zarkalaam, "E-signature and its situation in legal evidences regime", p 50.*
[11] *Mostafaa Elsaan, "Legal aspects of e-notarization", Kaanoon Journal, 2006, no. 60 (in Farsi), p 9-40.*
[12] *Khosro Abbaasi D., "Suggestions on amending draft bylaw for Article 32 of electronic commerce Act", Kaanoon Journal, 2006, no. 60 (in Farsi), pp 86-108.*
[13] *Stephen Mason, "Electronic Signatures in Practice", Journal of High Technology Law, 2006, Vol 6, no. 2, p 158.*
[14] *Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", pp 57-94.*
[15] *Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", pp 57-94.*

Evidence in Iran is not solely restricted to testimony, documents and confessions. Indications and oaths are other kinds of evidence.

does not have to refer to a CSP or a notary office to generate and transmit a signed or unsigned data-message. If the originator is willing to notarize the documents, he or she refers to the notary offices; and if they wish a middle person to be involved in the message, and to keep the records and certify the signature, they refer to a CSP office.

It is said by Elsaan that, "without security, data-message and e-signature is of no value."[16] But this is wrong, because, according to the Act, the secured data-messages and electronic signatures have been deemed as undeniable and un-demur-able, but the Act never provides that insecure data-messages and signatures are invalid or of no value. On the contrary, article 12 of the E-commerce Act shows that in the case of a data-message that is not secure, it is deemed as an ordinary document. Where it is denied or demurred by the defendant, the plaintiff has to prove its authenticity. If an ordinary document is not denied or demurred, or if after it is denied or demurred, its validity and authentication is proven, it would be considered against the defendant by the court.

The data-message as indication or testimony

Many of our daily actions leave a trail of digital evidence. For example, all service providers (for instance telephone companies, ISPs, banks, credit institutions) keep some information about their customers' actions. Digital evidence gets stored in a variety of places in operating systems and computers. Therefore, in this connection, article 16 of the E-commerce Act provides that, "any data-message recorded and retained by a third person in accordance with the provisions of the Article 11 of this Act, is considered as authentic." In this connection, article 11 provides, "a secure electronic record is a data-message, which is stored by the observance of the requirements of a secure information system, and is accessible and perceivable as needed." Principally data-messages, if made by others, may not affect the parties of a legal dispute, unless they are as written testimony or indication, proving some facts related to the claim in trial. However, if the data-messages retained by third parties are originally made with the parties, they may be used against them as documents. Therefore, data-messages, if related to the trial or made by one of the parties, even if recorded and kept with third parties (persons other than parties to the transaction), are considered as authentic and can be used as evidence for or against any of the parties (both claimant and defendant). Those data-messages, if made by third parties, may be deemed as testimony, and as they are in a material form, they may be deemed as written testimony.

In some instances, where a related information system or the computer system generates the data-message, it is the system that makes the testimony. This is brought about by article 2(M) of the E-commerce Act, which provides that 'person' includes "any natural or juridical person and or the computer systems under their control." This means that computer systems are also deemed as persons. But this does not comply with the fundamental principles of Iranian law. Therefore, it must be interpreted restrictively.

However, notwithstanding all these, it is possible to consider the data-messages made by the computer or information system of a third person as indications, and rely on them as means of proof. Evidence in Iran is not solely restricted to testimony, documents and confessions. Indications and oaths are other kinds of evidence. Indications are called 'real evidence' in other systems of law. For instance, fingerprints, DNA samples, and bloodstains are common examples of indications.

[16] *Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", pp 57-94.*

New kinds of indication arise, automatic records made by computer are fairly recent developments, which the law has not put any barrier into their reception as evidence.

There are some other indications in this case. Data automatically generated and stored in computer systems or information systems of litigants can be deemed as indications and used in a trial. This has not been expressly provided in the E-commerce Act, but close consideration of article 2(A) shows that definition of data-message can embrace these records. It defines 'data-message' as "any representation of facts, information, and concepts generated, sent, received, stored, or processed by use of electronic, optical or other information technology means."

Electronic signature

Article 2(J) of the e-commerce Act defines electronic signature as "any sign appended or logically affixed to a data-message which may be used to identify its signatory". Therefore, no difference has been made between digital signatures and other forms of signature. According to article 7 of the E-commerce Act, "any when the law requires the existence of signature, electronic signature is enough." This is because, despite opinions to the contrary,[17] the Iranian legal system does not principally require a signature to authenticate a document. This may appear to be against the common understanding from the cases where signatures are held that they must be used. For instance, it is asserted that a document in writing may be attributed to somebody where it is signed by him or her. The signature indicates statements and undertakings in the document are certified, and before the act of signing, the writing must be deemed as a scheme under study and assessment, which has not been decided on.[18] This cannot be correct, because when a document is attributable to the counter party, it is reliable before the court, even if it does not bear a signature.

Attributing a piece of writing to somebody can be verified through means other than a signature. A signature is required in exceptional cases, such as in case of generating a testament (a will). Therefore, there is mainly no difference in value between a signed and unsigned data-message. Account books are reliable evidence for and against the business, but they do not need to be signed. A book or a personal letter may be used against its writer as evidence, but those are not usually signed. However, if a signature were required, an electronic signature on the electronic document shall be equivalent to the signature of a person on a written proof. In this connection, the European Union Directive also gives electronic signatures the same legal status as their hand written equivalents.[19]

Seemingly, electronic signatures provided by a CSP, at most would work like seal, because there is no natural relation between the seal and the person whose signature it purports to be. Therefore, to be reliable, it must be proved that it belongs to the claimed holder, and that the document has been signed (sealed) intentionally. In this connection, the digital signature is nothing but a bundle of mathematical formula, confirmed by signature certificating authorities and confined to the user. Although called signatures, in legal analysis they are seals because they are produced by a third party and confined to the user, and they are exclusively used in their original shape.[20] But it is worth noting that despite its nature, such a sign would legally be deemed as a signature, because article 7 of the E-commerce Act provides that "any when the law requires the existence of signature, electronic signature is enough." Therefore, in cases such as issuing a cheque that requires a signature, and a seal will not suffice its issuance, the electronic signature would be sufficient.

Although some commentators have pointed out that "inclusion of e-signature in data-massages makes them as official documents,"[21] this cannot be correct, because there is no difference between ordinary signatures and electronic signatures in value, and the difference between ordinary and official documents is not dependant on their signatures. Even if the signature is a secure one, it cannot make an insecure document into a secure one.

One reason for using a signature is to confirm that the signor has ratified the document. Therefore, despite the contrasting opinion of Elsaan in this connection,[22] there is no difference between digital and ordinary electronic signatures. A digital signature has the ability to confirm the identity of the signor and it attributes the signed document to him. The beneficiary, if in doubt concerning

[17] *Morteza Vesaali N., "Electronic Signature and its situation among Legal Evidence", Kaanoon Journal, 2006, no. 59 (in Farsi), p 54; Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", pp 57-94.*

[18] *Naaser Kaatooziaan, Proving and Proving Evidence, Volume 1 (Nashre Mizaan, Tehran, 2001) (in Farsi), p 278, no. 174.*

[19] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12), article 5(2).*

[20] *Amir, Saadeghi N., "Legal Analysis of Electronic Payment's Certain Aspects", Proceeding of the Seminar on Reviewing the Legal Aspects of Information Technology (2004) (in Farsi), p 172.*

[21] *Morteza Vesaali N. "Electronic Signature and its situation among Legal Evidence", p 68; Siaamak Ghaajar and Gholaam N. Feyzi and others, "2nd monthly session – reviewing the Electronic Commerce Act", Collection of papers presented in the second conference on e-commerce, Ministry of Commerce, Deputy of Planning and Economic Surveys, 2005 (in Farsi), p 445.*

[22] *Mostafaa Elsaan, "Legal aspects of e-notarization", (in Farsi), Kaanoon Journal, 2006, no. 60 (in Farsi), pp 9-40.*

the identity of signor, can verify his or her identity by referring to the relevant Certification Authority. In the traditional manner, the signor makes the signature, and he can refer to a notary office for the certification of his signature. With a digital signature, the Certificate Authority makes the signature and confines it to the signor, therefore, in making a certified signature, there is less or no need for the presence of the signor at the office of the Certification Authority. This is because, unless otherwise proved, when that signature is made, it appears that it has been made by the person to whom the signature has been made by the Certification Authority. Therefore, despite contrasting opinion,[23] it is wrong to persist on requiring the presence of the signor to make each signature at the CSP office.

However, it is correct that when a signor makes a signature out of a CSP or notary office, his status at the moment of signing, for instance his legal capacity, assent, willingness or reluctance, mental health and so on cannot be ascertained with any certainty.[24] Such a situation sets the signature at the exposure of being nullified. The use of an audio and video connection between the CSP office and the signor at the time the signature is used may overcome some of these shortcomings. On the other hand, in business to business and business to consumer commerce relations, the parties to a contract rarely refer to notary offices for getting their contracts certified; therefore a digital electronic signature gives them the advantage of using a verifiable signature without wasting time by referring to notary or CSP office for each signature.

A new problem that might occur is where members of staff at the CSP office may forge the digital signature. Traditional forms of forgery are easier to discover. There must be preparations and measures in place at the CSP to prevent the generation and use of duplicate copies of digital signatures. Although, even this may not prevent dishonest staff from misusing the identity of the holder of a digital signature.

It is worth noting that at present no CSP office has been established in Iran, therefore, the required infrastructure for making digital signatures is not established.[25] Apparently, in the Board of Ministers there are some doubts about assigning the task of electronic certification services to present notary offices supervised by the organization for the notarization of deeds and real estates, a subdivision of the judiciary, or to new independent offices that are likely to be under the supervision of the ministry of commerce.[26]

It is suggested by Elsaan that, "electronic signature of an e-document shows that all required ceremonies for its formation has been met." [27] However, there is no reason to suggest that this is correct. The E-commerce Act has not barred the use of the digital signature for notarization. Even in that case, making the signature does not indicate the observance of all the required ceremonies. In this connection, in the United States of America, according to s101(g) of E-SIGN, registration (notarization) may be accomplished with an electronic signature. However, it must be borne in mind that this does not mean that every electronically signed data-message is a notarized one.

Data massage for investigating crimes

Using the data-messages for investigating crimes such as murder and so on has not been directly noted in the E-commerce Act, but for instance data-messages exchanged between victim and murderer undoubtedly can assist a criminal investigation. Electronic commerce is the main title of this Act, whereas it would have been better to create an Act that contains all aspects of electronic massaging issues, whether of commercial or non-commercial nature. However, some actions or omissions containing computer fraud, computer forgery, infringing the exclusive rights in an electronic transaction, and infringing data-message protection in electronic transactions are deemed as crimes encountering specified sentences or fines.

Where the subject of a trial is non-commercial, whether of criminal or non-criminal nature, the question remains: whether the regulations of this Act, which is confined to e-commerce, can validate the related data-messages as reliable evidence. In this connection, article 1284 of the Civil Code provides that "'document' means any writing which can be referred to in connection with a claim or a defense". Here, there may be a question that a data-message is not deemed as 'writing', because 'data-message' is only referred to as a piece of writing in the E-commerce Act. However, this may not be a difficulty, because customarily there is no

[23] *Mostafaa Elsaan, "Legal aspects of e-notarization", (in Farsi), Kaanoon Journal, 2006, no. 60 (in Farsi), p 9-40. ; and Khosro Abbaasi D., "Suggestions on amending draft bylaw for Article 32 of electronic commerce Act", Kaanoon Journal, 2006, no. 60 (in Farsi), pp 86-108.*

[24] *Khosro Abbaasi D., "Suggestions on amending draft bylaw for Article 32 of electronic commerce Act", Kaanoon Journal, 2006, no. 60 (in Farsi), p 86-108.*

[25] *For more information, see Mostafaa Elsaan, "Legal aspects of e-notarization", Kaanoon Journal, 2006, no. 60 (in Farsi), p 9-40.*

[26] *Mahmood Mohammadzaadeh, "E-commerce and e-signature", Kaanoon Journal, 2006, no. 61 (in Farsi), pp 12-28 ; Khosro Abbaasi D., "Suggestions on amending draft bylaw for Article 32 of electronic commerce Act", pp 86-108*

[27] *Mostafaa Elsaan, "Placement of e-signature in e-notarization of documents", Kaanoon Journal, 2005, no. 55 (in Farsi), pp 57-94.*

The books and essays written on legal aspects of e-commerce in Iran do not exceed 500 pages, and most of them mainly offer explanations of issues concerning electronic signatures.

difference between writing as data-message and other writings. On the other hand, according to the Act concerning punishment of publishing and disclosing state confidential and secret documents of 1984, documents are not only writings but also messages, files, photographs, maps and graphs, tables, films, microfilms and sound tape recordings. It is hard not to accept that this definition extends to all documents, whether state or private in nature. In respect to other forms of evidence, confessions and testimonies also will be in form of writing and there would be no difference between electronic or hard copies. Oaths can only be made in court, in the presence of the respective judge. Generally, in Iran there is no difference between civil and criminal evidence. Only with respect to certain crimes, such as murder and rape, ceremonies and procedures may differ.

Conclusion

Today, there is almost no controversy in respect to the admissibility of electronic records (data-messages) as evidence. Governments inevitably ratify regulations on electronic records, their validity and value. Iran, like many other countries, has accepted the evidential value of data-messages. But it is only the beginning. The law has yet to be understood in society. The legal writers and critics have not yet completely extracted its points and problems. The books and essays written on legal aspects of e-commerce in Iran do not exceed 500 pages, and most of them mainly offer explanations of issues concerning electronic signatures.

With respect to evidential value, the law in Iran has deemed the data-message as writing. It has deemed the electronic signature as a signature made on paper. But, it has declared the secure data-messages as non-deniable and non-demur-able. Also, it has prepared the ground for a generation of certified signatures. Iran's legislature has been aware of advances in information technology, and has accepted the legal evidential value for data-messages and their signatures.

This article shows that, a data-message is as like a piece of writing. Therefore, it can be considered a confession, document, testimony or indication. Data-messages are ordinary writings unless they are secure, official or notarized. If secure, they would be a distinguished type of writing, and if official or notarized, they would enjoy the legal advantages of official or notarized official writings. To make a data-message official, the provisions of article 1287 of the Civil Code must be met, and to be a notarized document, requisites provided in the Act for notarization of deeds and real estates must be fulfilled. Detecting the security level of a message is not the job of a judge, but for a computer and e-commerce expert.

It seems a mistake has taken place. The E-commerce Act is not exclusively confined to commercial issues. Therefore, the name of the Act is carelessly chosen. In fact, it is the electronic communication Act, not the e-commerce Act. Therefore, it can be even applied in cases other than those of commercial nature. It must be made clear that security is one thing and reference to CSP offices is another. This has not satisfactorily been highlighted in the Act, and it adds to the confusion.

Identification is the issue missed in the E-commerce Act. A signature is not the mere instrument that attributes the data-message to its originator. Other evidence, such as the internet or e-mail address, can play a part in identifying an originator. This works only if the address belongs to a particular site and the e-mail address has been given to the originator after identifying him or her. In case the e-mail address refers to a general site such as yahoo and so on, the address would not be legally reliable.

Ahad Gholizadeh LL.B, LL.M (National University of Iran), PhD in Multinational Companies' Law (Delhi University), presently assistant professor at Isfahan University (Isfahan, Iran) and a member of Central Bar Association Tehran, Iran.