IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 22, Issue 4, Ver. 7 (April 2017) PP 45-49
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Authenticity of The Electronic Document in Evidence (Comparative Study)

Dr. Abdalrazak Alsheban
Faculty of Law/ Cihan University / Sulaymaniyah

Abstract:- One of the greatest achievements of man is the computer, since its arrival computers and other. electronic storage devices have played a key role in aiding business. Since the arrival of computers and other electronic storage devices it has greatly aided business both domestic and international. Gone were the days when people carry huge cash on them for every transaction. Business has moved from paper base to electronically base. Electronic fund transfer and Automated Teller Machines have taken over business. Because of this achievement by man mentioned above, many countries in the world have amended their laws, to be computer compliant. The subject of the legal force of the electronic document is one of the most recent topics relating to the legal framework for electronic transactions through advanced means of communication using digital technology. The idea of the electronic document to date in many countries is still unclear. Its final picture is not yet clear, There is a practical difficulty in attaching the evidentiary power to the electronic document, especially in the field of electronic correspondence, since it does not leave a written impact of the same nature of the written effect, it accepts the amendment and the replacement without any evidence to prove that work, showing the problem of adoption of the electronic document as evidence. The issue whether electronically generated evidence is admissible or not has been a very topical issue amongst litigation lawyers in Iraq. the problem of hearsay evidence. Hearsay evidence refers to evidence given by a person who is not called as a witness in case, did not make such statement on oath and cannot be cross examined these statements are not admissible as evidence. With regards to computer printout, there is difficulty in admitting such documents is that the person who feeds the information into the computer is not the maker of such document, or in most cases the person through whom the document is sought to be tendered is no the maker or has no knowledge of how such document is made.

Key words :- The Electronic Document, evidence, lawyers, document, customer, legitimate, Electronic signature, liability,.

I. INTRODUCTION

Information networks and EDI systems are an application of modern technological use in communications. Transactions made by electronic means are characterized by many advantages, which is easy to complete the business process with less effort and costs and shorter time. Online dealers are able to enter into various contracts as soon as possible and electronically execute them immediately. In addition, dealing with electronic media led to the abandonment of the traditional means of document paper after replacing electronic documents, adding another positive character to deal with electronic means, paper is characterized by the problem of conservation, as this process requires a lot of effort as the amount of documents to the extent that it weighs weight and Is a number, and the electronic document is easy to save because it is done in a modern electronic and easy. That the electronic document is the main tool to implement the idea of electronic management, commonly called e-government, as it requires the use of digital information systems in the completion of administrative transactions and the provision of services and facilities and communicate with citizens. The electronic document is the tool through which electronic commerce achieves its objectives. Through this document, it is possible to complete transactions and conclude transactions and legal actions easily, thus saving expenses. These transactions are concluded by electronic means without the need for an intermediary whether this broker is an individual or a company.

II. ELECTRONIC EVIDENCE

The information society and its services are becoming more and more pervasive and are growing both quantitatively and qualitatively. Many of these services relate to transactions and electronic commerce in an electronic marketplace. The security of these services is a major issue which requires generally trusted solutions to attract potential users and customers. At the present state of the art public cryptography techniques are widely recognized as one of the main security means.

The present study will specifically focus on the issues of evidence in electronic transactions and liability of in electronic transactions to create a level playing field in this domain as well as to assure the balancing of legitimate interests.(Lutfi. M: 27).

1. Electronic Contracts

Electronic transactions and contractual agreements take place in a virtual environment and are virtual themselves. Nevertheless they represent real values, monetary or not, and proof has to be retained on its content and on the parties in the transaction. These electronic transactions are depersonalized both in the negotiation and in the conclusion phase and therefore the certification of the status of the parties (in particular of their real existence and of their legal capacity) as well as the certification of the transactions and the establishment of legally valid evidence are particularly important in order to assure the balancing of legitimate interests of all the players, to resolve disputes, as well as to promote trust. Electronic transactions and electronic contracts must relate on a set of certain rules for the establishment of evidence and, equally important, for keeping up this evidence and making it available as necessary. These rules must take into account that a large part of this evidence is produced and stored electronically and that it has to stand in litigation and most probably in court.

2. Electronic signatures

An electronic signature is generally any electronic process that indicates acceptance of an agreement or form. A range of methods can be used to authenticate the identity of participants, including email addresses, Enterprise IDs, phone authentication, knowledge-based authentication and passwords. In addition, many electronic signature solutions offer workflows that track every step in the signature process, such as when the agreement was sent, opened, and signed, as well as the IP and email address of each signer or approver. The best of these solutions capture this additional data in a secured audit trail, which provides clear, easily producible evidence of each party's signature. Digital signatures A digital signature is a specific type of electronic signature that requires the signer to authenticate their identity using a certificate-based digital ID. The digital certificate is generally issued by an independent Certificate Authority (CA), which verifies the identity of the signer before issuing the certificate. In some jurisdictions, like the European Union, a distinction is made between two types of electronic signatures that are typically implemented using certificates: Advanced Electronic Signatures (AdES) and Qualified Electronic Signatures (QES). While both are uniquely linked to the signer, the latter requires that participants use Qualified Certificates issued by accredited CA's as well as a qualified signature creation device (QSCD) signature creation device, such as a smart card, USB token, or cloud-based trust service. In addition to providing audit trails, solutions that work with digital signatures rely on the fact that the signed document itself can produce evidence of each participant's signature. During the signing process, the signer's certificate is bound to the document using the private key uniquely held by the signer. During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signer's identity through the trusted CA and to confirm that no changes were made to the document since it was signed.[1]

3. E-mail

The use of computer networks in the transfer of messages instead of the traditional means, each person is allocated to their own mailbox, and this box is a file and the unit of magnetic disks used to receive messages.(Al-Alaq. B. 2001:20).

4. website

The website consists of a set of pages that enable the user to perform many activities in different fields such as communications and customer services, marketing and sales, and other services offered in the network. The site provides contact with people and offers information, , And away from traditional methods of supply and demand.(El-Khail. M. 1998:135).

5. Conversation programs

Several chat programs have emerged that enable both parties to the web contract to speak directly through writing, audio, or audio and video together. If the device has a digital camera, each side can see the other. Here, the will can be expressed by a word, a letter, or a sign. This method achieves timeliness between the parties to the contract.(Al Ajarmeh. M. 2010:171).

[1] https://www.google.iq/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwifpv3-1KvTAhVFwxQKHTtnCCMQFggkMAE&url=https%3A%2F%2Facrobat.adobe.com%2Fcontent%2Fdam%2Fdoc-cloud%2Fen%2Fpdfs%2Fadobe-global-overview-of-electronic-signatures.pdf&usg=AFQjCNF8XG2M-3fdHINO5LJqa_NRIh1hSQ

i. Conditions for recognition of electronic extracts

1. Writing in an electronic document

The written evidence shall indicate the content of the legal disposition or the data recorded in the editor and that such writing shall be continuous. This means that the writing must be recorded as evidence of a foundation that ensures the consistency of this writing so that the parties can act or Stakeholders refer to them, and finally requires the stability of the manual, whether not add or delete until the evidence of confidence and security.(Lutfi. M:27).

2. The electronic editor should be readable

In order for the written editor to be traditional or electronic, as proof of proof, it must be readable, in the sense that the content of the written document is known and understood by the parties, which may remain in the form of documenting. The many possibilities offered by high technology and information technology for electronic document reading are vastly beyond reading on a traditional platform. Contracts, messages, data and everything that has been introduced, transferred or stored via electronic support has become available in more than one of the world's languages. Often written in one language. Moreover, the ordinary document, which is not read to any party because of the language in which it is written, must be translated into the language to which it becomes read until it performs its function of proof, with the costs and transfers required and time wasted. The electronic document, which allows the high technology included in the support to provide more than one copy in a different language and one-click interpretation of the document quickly and quickly, which saves a lot of time and money.

3. Automation in electronic document

Financial transactions on the Internet have demonstrated the need to protect electronic transactions and nominal data by means of a third party who is not a party to the contract to authenticate the exchanged data, in particular the electronic signature, and certify his or her health without having a personal interest in such data.(Ramadan. M:22). Therefore, encryption is a means of preserving and confidentiality of information in the scope of electronic systems, especially in e-government and its applications, such as electronic commerce, which requires maintaining the data and transactions of the parties and the volume and type of transactions and the protection of money traded within the scope of this trade.(Hijazi. A. 2007:260).

III. THE STRENGTH OF THE DOCUMENTARY IN IRAQ

There is a trend in Iraq to the equality of electronic writing with Paper writing, and gives them the same legal authority in evidence, in the sense of Article (104) of the Law of Evidence(107) for the year 1979, which stipulates that "the judge may benefit from the means of scientific progress in The development of judicial evidence. The document should therefore be understood to include a paper document and an electronic document, in particular the Transport Act(No. 80) of 1983, has allowed the signing of the bill of lading by manual signature or any other acceptable method. the remarkable development of international trade at the present time has forced the conclusion of transactions. And trade, making reliance on the traditional means that dominated commercial transactions at the turn of the century Past, one of which is a manual signature, is impossible.

IV. LEGAL RISKS ASSOCIATED WITH ELECTRONIC DISCOVERY UNDER CURRENT DISCOVERY PRACTICE.

The discovery obligation triggered by these rules carry substantial consequences for their breach. Inadequate or improper data preservation and deletion practices can amount to spoliation, contempt or obstruction of justice, each carrying with it potentially severe consequences. In an age that equates emptying the recycling bin with burning documents, it is especially important to comply with the rules of discovery.

1. Destruction of information

Inadequate or inconsistent record keeping can lead to a claim of spoliation, which is the negligent or "intentional destruction, mutilation, alteration, or concealment of evidence." This includes, "the failure to preserve [the records] for another's use as evidence in pending or reasonably foreseeable litigation." Spoliation not only sounds unpleasant, it is a particularly nasty outcome. The act of spoliation gives rise to a new affirmative claim that may be asserted by one's opponent, even if the opponent's underlying claim ultimately is found meritless.(Watson. L.2004:34).

2. Delete information

If there are no institutional policies in place to deal with electronic records when litigation or a formal investigation is pending, discoverable information may be lost, or purposefully deleted by members of the

organization. If electronic record storage policies exist they must be amended, from the IT department down to the individual user, to comply with the rules of discovery. Certain features of email clients, such as auto-delete or routine purges of data from a storage server, can result in spoliation. It is often in the failure to preserve electronic evidence that parties inadvertently violate the rules of discovery.(Wechsler.M&Lange.M. 2004:18-19).

3. The size of the large electronic records

With this background on applicable discovery rules, let us drill down a little further into the real world of public sector electronic records management. In a manner not anticipated by the text of these rules, the widespread propagation of electronic records complicates their discovery. With paper records, the amount of discoverable information is limited in a practical sense by the physical limitation on their storage: one can only maintain a given volume of pager records in the physical space actually available to one's organization: These locations are, by their nature, known and readily identifiable. Electronic records, on the other hand, may be stored in multiple locations simultaneously. Simply by sending an email, a record is created in (among other places) the outbox of the sender's computer, the recipient's inbox and on both servers housing the underlying systems, in addition to the storage media of intermediate transmission service providers. Factoring in replies, carbon copies and the ever-elusive blind carbon copy, a single email can result in a huge amount of discoverable information. Preserving the chain of evidence has become even more increasingly difficult due to "reply to all," "forward" and other features of email systems that create strings of email. The mere existence of an email in an employee's inbox, or a name on an email distribution list, can create a legal presumption of access or knowledge, "time stamped" for the opposing party's convenience, even if the employee has not actually read it.[2]

4. Electronic directory submission expenses

The expenses associated with electronic discovery, and thus the costs to be apportioned in an ideal system, may seem obvious to anyone with legal experience whether as a lawyer, as a computer forensics specialist or for some information technology personnel. Even assuming a responsible and appropriately restricted request for documents (that is, properly "balanced" as described in *The Sedona Principle*s), proper response to discovery including electronic materials will require some, if not all, of the following:

- Identifying, isolating and securing the requested electronic record: This entails finding the definitive version of an electronic record, "the official version," the "final revision," or the entire series of records, as with an exchange of emails between specified parties on particular dates. Isolating the files, once located, may require hundreds of gigabits of data and the duplication of operating systems and applications so that files may be viewed separate from systems and equipment of origin. Stand alone computers and related equipment may be required for the duration of litigation to ensure the security of the electronic records.
- Authenticating the records' source, content, revision and generation: The process of authentication is referred to broadly here. Specific requirements vary widely, depending on the source and location of the electronic records. Without retention schedules and formal procedures and policies defining the "office of record" or custodian of a type of file, authentication can be extremely difficult to establish.
- Initiating a process of documenting the locations of the record: From the receipt of the discovery order, someone or some division within the producing organization should be tracking all the players, their work, time, materials cost and the line. Tracking costs is an expense itself, but to determine equity during e-discovery, new records must be created and maintained.
- Documenting chain of custody: You find it, you track it. The complexities of tracking an electronic record from identification through to presentation in court have led to the existence of a growing number of firms specializing in "computer forensics" and electronic discovery services. The *Zubulake* decision was made on the basis of this concept.
- Producing an admissible version for court: Whatever version of the records is agreed upon for delivery, must be prepared and distributed.
- Preparing sufficient supporting media and testimony to ensure that the records will be comprehensible to the court: your IT manager, the database administrator, the systems analyst or other specialist who will (and hopefully can) explain the electronic environment of the record at issue.
- Matching the request to ability to produce, in terms of technical feasibility, timeliness, and cost: Is responding to the order resulting in costs that exceed a reasonable expense to the producing side relative to the severity of the issue being argued?

[2]http://www.mass.gov/anf/docs/itd/guidance/legal/managing-the-discovery-of-electronic-recordsppt.doc

- Balancing legal requirements with proprietary and operational concerns and considerations: IT says its too much work, or, they say it can't be done when, in fact, to revive the files is "just" hugely time-consuming, not impossible.[3]

V. CONCLUSION

The rise and rapid evolution of electronic communication and social media has forever changed the way we communicate, and it has left many courts and lawyers unsure of how to deal with the resulting deluge of evidence from these mediums. The stereotypical technophobe lawyer should have at least a rudimentary understanding of these mediums and how people use them to understand how potentially valuable, or damaging, they can be in court. we must state that though the Evidence Act as it stands today does not expressly mention that computer print outs and other form of electronically generated evidence are admissible, the Act however creates allowance for admissibility of such evidence. The subject of the legal force of the electronic document is one of the modern topics related to the legal framework of transactions. Which is made by advanced means of communication using digital technology, is still the idea of the document To the present in many countries is not clear, as its final picture is not clear After that, and that the Iraqi legislator to the present did not regulate this idea legislation, and on the other hand the countries that codified. This idea has differed among themselves in the mechanism of organization and to unite among themselves in the text on the applications of the document Without a well-structured legal structure in the field of the composition of this document.

We ask the Iraqi legislator to organize a law on electronic transactions in general and to grant the electronic document In particular the legal force expressly to be trusted in electronic transactions.

REFERENCES

[1] Al Ajarmeh. Mustafa Mousa (2010). Legal Organization for Online Contracting, Legal Books House, Egypt.
[2] Al-Alaq. Basheer Abbas (2001). Internet Applications in Shopping, Dar Al-Mahaikh, Amman, Jordan.
[3] El-Khail. Mahmoud Abdel-Moati (1998). The Internet and Some Legal Aspects, Egypt.
[4] Hijazi. Abdul Fattah Bayoumi(2007). E-commerce in the Arab Model Law. Legal Book House. Egypt.
[5] Lutfi. Mohamed Hossam Mahmoud. Legal framework for electronic transactions. Arabic Renaissance House.
[6] Ramadan. Medhat Abdel Halim. Criminal Protection of Electronic Commerce. Arab Renaissance House.
[7] Watson. Linda (2004). Anticipating Electronic Discovery In Commercial Cases A Guide for Corporate and In-House Counsel, Michigan Bar Journal.
[8] Wechsler. Michael. & Lange. Michele(2004). Digging for Data: Today's Discovery Demands Require Proficiency In Searching Electronic Documents, New York State Bar Journal. https://www.google.iq/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwifpv3-1KvTAhVFwxQKHTtnCCMQFggkMAE&url=https%3A%2F%2Facrobat.adobe.com%2Fcontent%2Fdam%2Fdoc-cloud%2Fen%2Fpdfs%2Fadobe-global-overview-of-electronic-signatures.pdf&usg=AFQjCNF8XG2M-3fdHINO5LJqa_NRIh1hSQ
[9] http://www.mass.gov/anf/docs/itd/guidance/legal/managing-the-discovery-of-electronic-recordsppt.doc

[3] http://www.mass.gov/anf/docs/itd/guidance/legal/managing-the-discovery-of-electronic-recordsppt.doc