Legality of Electronic Evidence in Criminal Evidence

Ameel Jabbar Ashour¹, Hayder Ars Afan²

¹College of Law, University of Misan - Ministry of Higher Education and Scientific Research, Iraq, ameelashour@uomisan.edu.iq
²College of Law, University of Misan - Ministry of Higher Education and Scientific Research, Iraq, ms.haidr2015@uomisan.edu.iq

Abstract
With the great and accelerated development witnessed by various aspects of life, and the use of technological techniques in all areas of work from the use of computers and the Internet, the crime is no longer committed in its traditional form, but has gone beyond the use of the information network using computers and information systems as a tool in committing the crime, which necessitated the provision of legal protection and the creation of a punitive system for the perpetrator of computer crimes and the information network that accompanied the emergence, growth and development of computer systems and networks and the information technology revolution because of its many risks and Great losses to institutions and individuals as they target the attack on data and information that affect the private lives of individuals, as well as threatening national security and national sovereignty. The study found that there is a clear deficiency in many arab substantive and procedural criminal legislations in confronting the phenomenon of crimes that occur by electronic means or on these means, for the seriousness of this crime recommended this study need for Arab legislation to speed up the pace of amending its punitive laws in order to keep pace with the revolution in remote communications, so that there is no separation between reality and law in a way that harms society and its individuals.

Keywords: Electronic Evidence, Criminal Evidence, Technical Development, Criminal Law.

1. Introduction
The scientific and technological progress in the field of electronic devices and the information revolution has taken a privileged position in human life, but it has become one of the basics of human life because of its association with various aspects of life from economic, cultural, social, political, and health, and crime is only one of the manifestations of human life that is affected by the new discoveries and scientific innovations to harness it for its benefit, whether by using
it as a means or tool or the emergence of new crimes, the evidence of a person’s guilt or innocence may be derived or is derived from this virtual environment. Where ordinary evidence does not work, then electronic evidence must be used.

2. Statement of the Problem:

The electronic evidence is not only related to information technology crimes, as there may be a regular crime, such as killing, smuggling or others, but the evidence that convicts criminals is digital evidence. It was necessary to draw the parameters of the electronic evidence, whether in terms of its usefulness or in terms of its legal value, as the courts relied on it based on a legislative text at one time. It is decided that the obstacles and difficulties facing the digital evidencende do not stop at how to obtain it and the procedures for preserving it, but rather extend to the extent of the evidentiary strength that this evidence enjoys and the extent of the trial judge’s freedom to convince him to base a verdict of innocence or conviction on its basis. In view of the above, the following research problems will be addressed in this study:

1. The insufficiency of Iraqi legislation, like other legislations in Arab countries, to adopt modern scientific evidence as a method of proof, in addition to the traditional evidence mentioned in the texts of these laws.

2. Deficiency of readiness of the judges’ cadres to deal with this evidence, due to the stagnation of the rehabilitation programs for these judges.

3. Acute shortage of modern technologies, and the possibilities to address the adoption of this evidence.

3. Research Objectives.

1. Clarification of the legality of criminal evidence using modern scientific means in Iraqi criminal law and contemporary jurisprudence.

2. Statement of the obstacles facing the investigation and evidence of electronic crimes.

3. To study the the legality of the electronic evidence in the Iraqi criminal evidence.
4. Importance of Study.

The emergence of modern criminal acts, their multiplicity and spread, these crimes do not accept proof by traditional evidence because of the medium in which they originate, which is the virtual world, where electronic evidence is the only evidence stemming from the environment of committing the crime itself. Thus, the study helps in crystallizing the academic understanding of the electronic guide provided to law enforcement and law enforcement agencies to support the authenticity of electronic outputs in criminal matters.

5. Study Methodology.

The study took the analytical approach by referring to the texts of the legal articles that regulate and govern the subject to identify the research problem and its dimensions by linking the technical and legal aspects of the problem at hand in order to reach a standard that the judiciary can rely on.


Evidence is defined as the fact from which the judge derives proof of his conviction of the judgment that ends with him (Abdul Muttalib, 2006). In the sense that it is the means that contribute to achieving certainty for the judge in a way that reassures it and that leads to proving the validity or invalidity of the fact. It is known that the evidence stems from the environment in which the crime is committed, whether the crime is traditional or electronic. Cybercrime in particular does not benefit ordinary evidence because, as we mentioned, it arises only in a technical virtual medium with which ordinary evidence is unable to prove it, and from its association with electronic crime, the name was taken from it, and therefore it was called electronic evidence or digital evidence (Ali, 2016).

Electronic evidence is defined as: "data that can prove that a crime has been committed or that there is a relationship between the crime and the perpetrator, or that there is a relationship between the crime and the victim of it. Digital data is the set of numbers that represent various information including written texts, drawings, audio and video maps" (Al-Bashir, 2004). It was also defined as "the set of magnetic or electrical fields or pulses that can be collected and analyzed using special programs and applications to appear in the form of images or audio or video recordings (Ahmed, 2015) and defined as: "evidence resulting from the use of electronic means in committing illegal acts that occur on the information means themselves" (Ali Al-Masri, 2012).
The electronic directory was defined by the American report submitted to the Interpol Scientific Symposium on Digital Directory in 2001 as "data that can be prepared, communicated and stored digitally so that a computer can perform a task" (Abdul Muttalib, 2006). While the Scientific Working Group on Digital Evidence prepared several definitions of electronic evidence, including "digital evidence: information of evidentiary value stored or transmitted in digital form", "physical elements that can be stored and transmitted, such as data or information, and can be relied upon in court", "original digital evidence is the physical elements and data associated with these elements at the time of acquisition or seizure", "Duplicate digital evidence: Accurate digital reproduction of all data elements on an original physical element." (Khindeel, 2015)

The International Computer Evidence Organization also provided a definition of electronic directory in general. 2000 as "information stored or transmitted that can be relied upon before the court", followed by a second definition in the following year 2001 as "information of potential value, stored or transferred" (Al-Bashir, 2004). In this regard, we refer to the definitions provided by special laws concerned with electronic transactions, including: the Federal Electronic Transactions Act of the United States of America (1999) that electronic information is: data, text, images, sounds, symbols, computer programs, software, databases or the like" (Al-Halabi, 2011). The Information Technology and Labor Legal Framework Act of the Province of Quebec, Canada (2005) in Article 3 of the electronic document is "a document consisting of the information transmitted and organized by physical means and in accordance with the media, and is a clear form of words, sounds, images and information that can be made in any written way, including a system of symbols or any other form of symbol system" (Ibrahim, 2007).

While others defined it as: "evidence derived from or by computer information software systems, computer devices, equipment and tools, or communication networks through legal and technical procedures, to be submitted to the judiciary after analysis and interpretation in the form of written texts, drawings or pictures to prove the occurrence of the crime and to determine innocence or conviction in it" (Kindeeel, 2015), as well as defined as a digital component to provide information in various forms such as written texts or images, sounds, shapes and drawings, in order to link between the crime, the criminal and the victim, and legally it can be taken before law enforcement and enforcement agencies" (Ali, 2016).
**7. Characteristics of the Electronic Directory.**

Electronic forensics is distinguished from traditional evidence by the following characteristics:

A. The technical nature of electronic forensics. Electronic evidence is of a technical and technical nature and how intangible moral is not perceived by the ordinary senses and requires the realization of the use of devices, equipment and tools of the automatic calculator (HARD WARE) and the use of computer software systems (SOFTWARE), the electronic directory - as mentioned above is a magnetic-electric fields and then the translation of the electronic directory and output in a tangible physical form does not mean that this gathering is considered the evidence, but that this process is nothing more than a transfer of those areas of their digital nature to the body that it can be inferred from a certain piece of information (Abdul Muttalib, 2006).

B. Digital Evidence Scientific Evidence. Electronic forensic evidence is scientific evidence due to the fact that it is derived from what is manufactured from science and scientific opinions in the light of which technical programs and devices are innovated, and electronic evidence is from the category of what is known as evidence derived from the machine (Al-Halabi, 2011).

C. Difficulty blurring or deleting electronic evidence. Electronic evidence can be retrieved after erasing, repaired after destruction, and shown after hiding, which leads to the difficulty of getting rid of it, which is one of the most important characteristics of the electronic directory compared to the traditional directory, there are many computer programs whose function is to recover data that has been deleted or canceled, whether this is done by the command (delete), or even if the hard disk is reformatted or configured using the command (format) and programs that have been destroyed or hidden, whether they were pictures, drawings, writings, or others (the file that has been deleted can be recovered using a recovery tool for deleted files (undeleted tool), which means that it is difficult for the offender to hide his crime or hide it from the eyes of security and justice as long as the knowledge of the research and criminal investigation men reached the occurrence of the crime, but the offender's attempt to erase the electronic evidence itself is recorded as evidence, as doing so is recorded in the machine's memory, which can be extracted and used as evidence against him. The difficulty of getting rid of electronic evidence increases that it is possible to extract identical copies of the original and have the same value and evidentiary authenticity, which is not available in other types of evidence (traditional), which constitutes a very effective guarantee to preserve the evidence against loss, damage or change from making true copies of the evidence, which made the Belgian legislator under the law of November 28, 2000
AD amend the Criminal Investigation Law (Code Destruction Criminal) by adding Article (BIS) (3), which allowed the seizure of digital evidence such as copies Materials stored in automated data processing systems with the intention of presenting them to the judicial authorities (Abdullah, 2016).


Criminal evidence is generally required to be accepted as evidence to be obtained in a legitimate manner, and this requires that the competent authority for collecting evidence has adhered to the conditions set by law in this regard (Arhouma, 1999). The principle of the legality of electronic evidence means that the procedure must be consistent with the legal rules and regulations in the conscience of civilized society, that is, the rule of legality of criminal evidence is not limited only to mere conformity with the legal rule stipulated by the legislator, but must also be taken into account Human rights declarations, international charters and agreements, the rules of public order and good morals in society in addition to the principles settled by the courts (Alhasoon, 1979).

The legitimacy of the procedure is the ring that ensures respect for the personal freedom of the accused by requiring that the law is the source of procedural organization and that the innocence of the accused is assumed in each of the procedures taken before him and that the judicial guarantee is available in the proceedings, the procedural legitimacy is a natural extension of the legitimacy of crimes and penalties, but it is in fact more serious and greater, it serves as an external framework that can not be properly applied objective rule except through it, and it is clear from Procedural legitimacy is based on three elements (Abdullah, 2010).

The first element is the original in the accused innocence so that his freedom may not be restricted except within the framework of the constitutional guarantees necessary to protect it and based on a provision in the Code of Procedure or the principles of criminal trials, as it is fixed in the Penal Code that there is no crime and no punishment except by text, the constant in the laws of criminal procedure that there is no procedure except by text and this is the second element of criminal legitimacy, either the third element is the need to supervise the judiciary of all Procedures as the natural guardian of rights and freedoms. We are here as we discuss the legitimacy of the electronic evidence, we will limit ourselves to what raises the collection of this evidence of legal problems given its special nature, and therefore we can say that what raises the electronic evidence in terms of the legality of obtaining it is mainly concentrated in the inspection procedures to
search for this evidence. This raises an important point, which is the legality of searching for electronic evidence and controlling it in the virtual environment. (Arhuma, 1999), and the reason for this problem is related to the inspection procedure, which must be exercised by a member of the judicial control or the investigation body, as the case may be, do these have the ability to search the virtual medium (the Internet and seize the evidence from it?)

9. The Authority of the Criminal Judge to Accept Electronic Evidence.

The rule that prevails in criminal legislation in evidence is that the court rules on this case based on its conviction that it has of the advanced evidence in any role of investigation or trial. It has no authority in this except for the conscience of the judges and does not demand except to indicate the reason for its conviction with evidence without another, as it is not bound by a decision issued by the accused or a certificate of proof that the crime resulted in him or a defense certificate that denied the charge about him or an opinion presented by an expert, Unless convinced of it as the criminal evidence from which the courts derive their conviction is not exclusively specific, but the law mentioned some of them, which are often common and represented in (acknowledgment, testimony, investigation minutes, minutes of other official statements, reports of experts and technicians) and then the law came with a general text to include other evidence by saying ((and other evidence and evidence prescribed by law)). This evidence takes what he is satisfied with of the evidence and presents what he is not assured of other evidence (Alhaason, 1979).

With the issuance of the Electronic Signature Law of 2012, we find that the legislator has approved for electronic evidence the authenticity prescribed for traditional evidence, and thus electronic evidence can be considered acceptable evidence if certain conditions are met. The criminal judge is free to estimate the collection of evidence of the criminal case, regardless of its source, from which it was derived, as long as it is legitimate and equal in that traditional criminal evidence and electronic criminal evidence, the door of evidence is wide open in front of him, he takes any evidence that reassures him and his conscience and puts forward every evidence that revolves around doubt in order to reach the truth, as the judge's belief and conviction of the evidence must have been derived from electronic outputs presented in the session because the rule is that he should not rule except based on Investigations that take place by legal methods and conditions and not based on his personal information or on what he may have seen himself or a fact in other than the Judicial Council (Ahmed, 2006), as the criminal judge should base his judgment on evidence resulting from the computer for a reason that invalidates
it and executes its effect, and in order to achieve certainty and oral legitimacy in the evidence, the overall conditions for accepting electronic outputs are summarized in the following three principles:

A. The principle of certainty of electronic criminal evidence.
B. The principle that electronic forensic evidence should be discussed.
C. The principle of the legality of electronic criminal evidence.


The most correct in contemporary criminal jurisprudence is the division of certainty in terms of its source into legal certainty and moral certainty, legal certainty: means that situation resulting from the value that the law adds to the evidence and imposes on the judge under the limited legal evidence it is a kind of certainty received by the judge willingly and this type of certainty is prevalent in English law (alhaason, 1979).

However, the common law in England no longer takes the theory of legal evidence at all, but began to accept the principle of free appreciation of evidence, so it has become talk about conviction without any reasonable doubt or conviction without any doubt is prevalent in English law currently, and from this point of view, the English judiciary has the freedom to rule on conviction based on, on the testimony of one person as long as this testimony achieves certainty if the general rule in England that the criminal court should not Convict the defendant only when the elements of the crime have been proven and far from anything reasonable (Abdullah, 2010).

If we move on to discuss the certainty of electronic outputs, we find that the Police or Criminal Evidence Act in Britain requires that the data be accurate and resulting from a properly functioning computer (Abdul Muttalib, 2006). In France, there is no place to refute the origin of innocence and presume the opposite, except when the judge's conviction reaches the point of certainty and certainty, and the matter is no different for computer outputs, as French law requires electronic outputs to be certain so that the conviction can be judged, so that there is no place to refute the presumption of innocence and presume its opposite, except when the judge's conviction reaches the point of certainty and certainty, and this is reached through what is deduced by the various means of perception of the judge from Through the computer outputs presented to it, whether they are paperless or electronic outputs such as tapes, magnetic disks, film works and other non-traditional electronic forms of technology that are available through direct access, or finally it is just a display of these outputs processed by electronic on its own screen or on terminals (Abdullah, 2010).
In order to be certain criminal evidence, some legislation, as in Greece, Austria, Suez or Norway, have gone to the need for electronic evidence to be legible, whether printed on paper after leaving the computer or read on the computer screen itself, and in the same direction the Iraqi legislator walked as it stipulated in Article (2/26) of the draft Iraqi Information Crimes Law: ((The body collecting evidence shall do the following: Provide electronic or paper copies of the evidence ..)) Thus, the legislator allowed the evidence submitted to be in the form of electronic or paper copies (Abdul Muttalib, 2006).

9.2. The Principle that Electronic Forensic Evidence should be Discussed.

The principle that governs the trial proceedings is that the pleading is oral and in the presence and what is meant by pleading here is all the procedures of the final investigation conducted by the court, and the concept of the principle that electronic evidence must be discussed in general that the judge can not base his conviction only on the evidentiary elements that were put forward in the trial sessions and were subject to the freedom to discuss the parties to the lawsuit and it is no different for electronic evidence as evidence as it should be put forward in the session and be discussed in the face of the parties (Qindeel, 2015).

Based on this, electronic evidence, whether printed or data displayed on the computer screen or data included in data carriers, must be discussed and analyzed. The rule that criminal evidence must be discussed, whether it is traditional evidence or computer-generated evidence, is an important and definite guarantee of justice so that the criminal judge in information crimes does not rule on his personal information or based on the opinion of others (Al-Haason, 1979).

The idea that it is not permissible for the judge to rule on cybercrimes based on his personal information is one of the most important consequences of the rule that criminal evidence must be discussed or presented, whether it is traditional or electronic evidence in the session, because it does not justify the judge to rule according to his personal information in the case or on what he saw himself or achieved in the Judicial Council without the presence of the litigants. This is because this information was not presented at the hearing, discussed and evaluated, and therefore reliance on it is contrary to the rules of orality and confrontation that prevail in the trial phase (Abdul Muttalib, 2006).

There is also a contradiction between the qualities of the judge and the witness, as the testimony requires awareness of the facts and then transferred to the case and in this process intervene several
considerations, including the element of appreciation of the witness and his awareness and memory to other factors and influences that have a great involvement in the assessment of the testimony and this needs on the part of the judge to estimate and scrutinize his statements and is worthy of that because of his two faculties of criticism and interpretation, but if the source of this testimony is the judge himself, he cannot conduct censorship required as he then falls into conflict with himself because the information he gives must be free from bias and personal influences (Al-Haason, 1979).


The legitimacy of the electronic evidence means that it is based on legitimate procedures, whether those procedures have been issued by the judge directly or indirectly, or by the accused when interrogated and confessed, or by others after arresting him, interrogating him, searching his home, or practicing any work of technical expertise, and the judiciary's control is not limited to the original or exceptional inference work or to estimate the evidence only, but this control also extends to the legitimacy of the evidence and the method by which the investigation authorities obtained the evidence, and did it violate a procedural rule or not? The legitimacy of the evidence in general is a prerequisite for reaching judicial certainty upon conviction, and this does not prevent the incriminating evidence from being clear and blatant as long as this evidence is suspicious and its source is not characterized by integrity and respect for the law.

The criterion for the legality of evidence lies in respecting the guarantees of personal freedom stipulated by the law, not respecting the freedom of the individual as an innocent person until proven guilty by a final judgment (Ali, 2016), and therefore the criminal judge may not rely on invalid or abstract evidence of its legal value and derive his self-conviction from it and enter into the meaning of false evidence that evidence that did not meet one of the conditions required by law in order to have persuasive force for the judge, the conviction of the judge must be based on evidence derived from a valid and legitimate procedure, but if this conviction is based on invalid evidence or illegal procedures, it leads to the invalidity of the judgment, the application of the rule (what is built on nullity is invalid), and therefore these procedures must be in conformity with the law and not inconsistent with ethical and scientific principles (Al-Bashir, 2004).

Criminal procedures are legal and characterized by legitimacy when the criminal judge adheres to the provisions of the law does not stray or deviate from the path set by the law, but if ignorance or ignoring a legal rule, objective or formal, or the first or interpreted those rules interpretation or interpretation is not real or illogical, this ignorance or ignorance on the one hand or error in interpretation or
interpretation on the other hand reflects honestly on the conviction obtained because it is the fruit or outcome of the steps taken by it is the result of the operations conducted in a manner characterized by error or corruption, and in the field of cybercrime, we see the need to seek the help of judicial expertise to ensure the integrity of the electronic evidence from tampering or error, in addition to monitoring the judge the validity of the procedures for collecting electronic evidence, (Abdul Muttalib, 2006).

10. Conclusion

First: Results:

1. The study found that there is a clear deficiency in many arab substantive and procedural criminal legislations in confronting the phenomenon of crimes that occur by electronic means or on these means. Many of them are still subject to these crimes by traditional texts, which may result in an assault on the principle of legality of crimes and penalties, or the impunity of many perpetrators. Despite the proliferation of electronic means in these countries, many of their legislations have not been touched by the hand of amendment in order to be able to protect the emerging interests produced by these means.

2. The study also revealed that there is a difficulty in forensic evidence with regard to electronic crimes, whether in terms of methods of obtaining it or in terms of its nature. Obtaining it may require complex technical, scientific and mathematical operations. Just as its nature may be invisible, such as vibrations and pulses, and it is easy to use scientific technology to hide or destroy it. This may be done by encryption, secret passwords, and the use of destructive or damaged viruses.

3. The research showed that the criminal evidence, no matter how advanced it is in relation to electronic crimes, and the importance of scientific and technical evidence in this evidence, we must maintain the discretion of the judge in his assessment of this scientific and technical evidence, because we thus ensure that this evidence is purified from the impurities of the scientific truth, and the judge remains in control on this fact; Because through his discretion he can explain the doubt in favor of the accused, and exclude evidence obtained illegally.

Second: Recommendations:

1. The need for Arab legislation to speed up the pace of amending its punitive laws in order to keep pace with the revolution in remote communications, so that there is no separation between reality and
law in a way that harms society and its individuals, and in the way that many foreign and some Arab legislations have followed by explicitly stipulating the criminalization of illegal acts that produced by this revolution.

2. Paying attention to training experts, investigators and judges to deal with electronic crimes of a complex technical and scientific nature, so that it is possible to reach the truth and uncover these crimes in order to achieve the benefit of society and its members, for the benefit of the accused themselves so that only the offender is convicted.

3. Paying attention to evidence and scientific evidence so that judges can reach the truth through these modern means of criminal evidence.

4. Allowing the inspection authorities to control computer programs and information in the devices according to the same conditions for regular inspection procedures. The need to issue a technical and legal guide on images of computer crimes and scientific assets to detect and investigate them, and methods of dealing with electronic evidence, and to continue updating this guide periodically and whenever the need arises. Therefore, it should be circulated to those working in the field of investigation, and the judiciary should benefit from the guide issued by the International Criminal Police Organization, Interpol.

Bibliography


