Ilkogretim Online - Elementary Education Online, 2024; Vol 24 (Issue 2): pp. 461-471
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2024.02.33

The Powers Of The Criminal Judge In The Evaluation Of Electronic Evidence Derived From Criminal Investigations

Laksaci Sidahmed Professor Lecturer A, Faculty of Law and Political Science, University of Adrar Ahmed Draia, Laboratory for the Study of Spatial Development and Entrepreneurial Development (Algeria). laksaci79@univ-adrar.edu.dz

Ben Abdelkabir Hassen Doctor of Law, Faculty of Law and Political Science, University of Adrar Ahmed Draia (Algeria). hba83114@gmail.com

Received: 14/02/2024 Published: 20/06/2024

Abstract:
The criminal judge has wide powers in evaluating evidence, as he can investigate the truth by various means and collect evidence without being obliged to prefer one piece of evidence over another. However, where certain types of evidence, such as electronic evidence, are prescribed as the only admissible forms, the criminal judge must comply with the conditions laid down by the legislature when accepting such evidence. These conditions serve as a safeguard against the criminal judge's deviation in relying on this type of evidence. The acceptance of electronic evidence is a relative matter that varies from one legal system to another, whether it is a Latin, Anglo-Saxon or mixed system.

Keywords: Evaluation Of Electronic Evidence, Criminal Investigation, Powers Of The Criminal Judge, Modern Forensic Evidence.

Introduction:
Criminal evidence is considered as a direct activity aimed at achieving legal certainty. Therefore, the aim of evidence is to demonstrate the degree of correspondence between the legal model of the crime and the presented event. In this field, certain means are used to provide evidence, and the means of evidence is any activity that is carried out to discover a state, a matter, a person or a thing. The issue of evidence in computer and Internet systems poses great difficulties for investigators for several reasons, including the invisibility of the data stored in the computer, the ease with which evidence can be erased in a short time, and other difficulties faced by investigators. In order for the criminal judge to accept electronic evidence, it must be based on a foundation and comply with the conditions laid down by law.
In the light of this introduction, we ask the following question:

What are the conditions that must be met in the electronic evidence derived from the criminal investigation and to what extent does the criminal judge have the authority to evaluate this evidence?

Based on this problematic issue, the study can be divided into two axes:

Axis One: Conditions for accepting electronic evidence derived from criminal investigation.

Axis Two: Bases for accepting electronic evidence in the light of criminal evidence systems.

Axis One: Conditions for the Acceptance of Electronic Evidence from Criminal Investigations

Electronic evidence may be paper outputs produced by printers or plotters, or non-paper outputs or electronic forms such as magnetic tapes, floppy disks, video discs and other non-traditional electronic forms, or it may be the display of computer processing outputs on its own screen or the Internet through screens or visual display units.Electronic evidence is invalid if it has been obtained in violation of the law.If the search of computer systems is faulty, it is invalid.Therefore, the criminal investigation of electronic crimes is subject to several conditions, as follows:

First: Conditions for the legality of electronic evidence.

One of the most important rights and freedoms protected by the Algerian Constitution is the right to respect for human dignity[1] and the protection of human rights. The State guarantees that the sanctity of the individual will not be violated and prohibits any physical or moral violence or any violation of dignity. The Constitution lays down provisions regulating the basic rules of searches, on the basis of which the State shall ensure that the inviolability of the home is not violated; no search shall be carried out except in accordance with the law and within the framework of respect for the law[2]. The fundamental freedoms and rights of citizens shall be guaranteed[3], and the sanctity of the private life of citizens and the inviolability of their honour shall be protected by law. The confidentiality of correspondence and private communications of all kinds is guaranteed, and these rights may not be violated in any way without a reasoned order from the judicial authority, the violation of which is punishable by law[4]. The protection of individuals with regard to the processing of personal data is a fundamental right guaranteed by law, the violation of which is punishable

These constitutional provisions impose an obligation on the legislator, when establishing the rules of criminal procedure, to comply with them and not to deviate from them. The procedures for obtaining criminal evidence must fall within the general framework established by the Constitution, otherwise evidence obtained in violation of the provisions of the Constitution is absolutely null and void by virtue of its connection with public order and may be invoked by any interested party, and the court may rule on it of its own motion. It is therefore necessary for the Algerian legislator to adopt procedural rules that

guarantee the protection of private life stored on computers and the Internet, by prohibiting the intrusion into personal files without a legal basis, in order to protect the individual rights and freedoms guaranteed by the Algerian Constitution, in addition to the international covenants.

The penalty for violating the law in obtaining evidence includes criminal or administrative sanctions, as well as the payment of compensation. The official to whom the law entrusts a task and who acts in a manner contrary to the law is considered to have failed in his duties and to have violated his obligations[5], and therefore deserves to be held accountable. Article 107 of the Algerian Penal Code stipulates that "a public official shall be punished by imprisonment for a term ranging from five to ten years if he orders an arbitrary act or a violation of the personal freedom of an individual or of the national rights of one or more citizens"[6]. Similarly, article 85 of the Code of Criminal Procedure stipulates that "anyone who discloses or distributes a document obtained from a search of a person who is not legally entitled to see it, without the permission of the accused or his successor or the person who signed the document or the addressee, as well as anyone who uses the information obtained from it, unless this is necessary for the purposes of the judicial investigation[7], shall be punished by imprisonment from two months to two years and a fine of 2,000 to 20,000 Algerian dinars". In all cases, an act contrary to the law entails, in addition to the right of the perpetrator to be punished, the right of the person against whom this unlawful act has been committed to compensation, with the nullity of this act, since it is born of a crime, and consequently the nullity of the evidence derived from this act.

In the case of witnesses to a cybercrime, the question arises as to whether they are obliged to print out the files stored in the computer's memory, thereby revealing the secret, or to disclose the secret passwords, or to reveal the codes in which the specific programme execution commands are recorded. It should be noted that comparative jurisprudence has answered this question differently, with both proponents and opponents, which can be crystallised into two main trends as follows:

1- The first approach:

Its proponents argue that it is not the duty of the witness, according to the traditional obligations of testimony, to print files stored in computer memory, to disclose secret passwords or to reveal encoded codes. In Luxembourg, the witness is not obliged to cooperate with everything he knows when questioned in court, and it is therefore difficult to compel him to provide data he does not know and did not enter into the computer memory, even if he has access to it through his knowledge of the secret passwords[8]. If the witness cooperates in this way, his role would be closer to that of an expert than to that of a witness.

2- The second approach:

According to its proponents, the obligations to be fulfilled by the witness include printing files, disclosing passwords or codes for various programmes. For example, in France, in the absence of a legal text, a part of the doctrine considers that the witness is obliged to

disclose the secret passwords known to him and the operating codes of the programmes, except in cases of professional secrecy[9].

With regard to the legitimacy of electronic evidence, although the French Code of Criminal Procedure does not contain any provisions relating to the principle of good faith or integrity in the search for the truth, the doctrine and the judiciary are in favour of this principle, whether in the field of traditional crime investigation or in the field of computer and Internet crime investigation, for example when judicial police officers use computer methods to intercept telephone conversations. According to a French legal opinion, the judiciary has accepted, with reservations, the use of modern scientific means in the investigation and detection of crimes by obtaining criminal evidence, including evidence obtained from computers and the Internet, in a lawful and impartial manner. The same is true in Switzerland and Belgium[10].

In the UK, the police installed a listening device on the telephone line of one of the complainants with her consent. The complainant had several telephone conversations with the person the police suspected of committing the crime, and the conversations implicating the defendant were recorded. However, the judge excluded these recordings on the grounds that they had been obtained by entrapment[11].

The use of deception, fraud or trickery to obtain electronic evidence is also considered an illegal method. The legality of electronic evidence is an important guarantee of individual liberty, since the use of unlawful means to obtain digital evidence renders the proceedings invalid and inadmissible as evidence in criminal cases. Examples of unlawful methods include the use of physical or moral coercion or fraud against the perpetrator of computer crime in order to decipher the access code to the system and access the evidence obtained by electronic means[12].

Secondly, the requirement to discuss the electronic evidence:

The judge must base his judgement on the evidence presented to him for discussion in court. This is one of the most important rules of criminal procedure. Accordingly, the evidence must have a fixed origin in the case file and the parties must be given the opportunity to examine and discuss it. Article 212(2) of the Code of Criminal Procedure stipulates that "the judge may base his decision only on the evidence presented to him in the course of the pleadings and discussed orally before him"[13].

Therefore, electronic evidence, in whatever form it takes, whether data displayed on a computer screen, information stored on discs, magnetic tapes or extracted in printed form, must be discussed if it is to be accepted as evidence in court. The discussion of digital evidence is based on the following two main elements:

1- The first element:

The first element consists of giving the adversaries the opportunity to access the electronic evidence and to respond to it, thus respecting the principle of the right of defence, which is considered one of the fundamental principles of the Algerian judicial system. The requirement to discuss the electronic evidence also allows for the application of the principle of confrontation, which is also considered one of the fundamental

principles of the Algerian judicial system. It also lays down guarantees, including the need to inform the accused of the charges against him, to give him sufficient time to prepare his defence and to allow him to be assisted by a lawyer. It also allows each party to the dispute to submit its documents and to question witnesses and experts during the trial.

2- The second element:

The second element is that the electronic evidence must have an original in the case file, so that the judge's conviction is based on a foundation. Consequently, the legislator has made it compulsory to draw up a transcript of the hearing in which the facts of the criminal case and the evidence were established, so that the judge in question or any of the parties to the dispute can refer to this transcript in order to clarify any of the facts established[14]. Accordingly, the requirement to discuss the electronic evidence means that the judge's conviction at the time of sentencing must be based on his or her own conviction and not on the conviction of others. The judge's conviction must not be based on his personal information or the opinion of others, because the conviction generated in the judge's mind is part of the discussion of the evidence, which reveals the strength or weakness of the evidence and forms the judge's conviction on the basis of which he accepts or rejects the evidence[15].

Thirdly, the requirement that the judicial conviction reach the level of certainty.

It is necessary for the evidence obtained from the computer and the Internet to be free of doubt in order to be able to convict, since there is no room for rebutting the presumption of innocence and presuming the contrary, unless the judge's conviction reaches the degree of certainty and certainty. Thus, the judge can determine, on the basis of the electronic evidence presented to him and the impressions and probabilities he forms about it, its probative value with regard to the truthfulness of the attribution of the computer crime to a particular person or not. Therefore, the electronic evidence must be beyond doubt, since the latter is interpreted in favour of the accused, based on the rule that a person is presumed innocent until proven guilty. It is sufficient for the judge to have doubts as to the correctness of the attribution of the charge to the accused in order to rule in favour of acquittal, in application of a constitutional rule laid down in Article 56 of the Algerian Constitution[16].

If the criminal judge can reach certainty through sensory or rational knowledge through analysis and inference, then convicting the perpetrator of the electronic crime and attributing it to the accused requires another type of knowledge from the judge, namely scientific knowledge of information and electronic matters, especially since the criminal judge plays a positive role in the evidence. Ignorance of these matters leads to doubts about the value of electronic evidence, and these doubts lead to the acquittal of the accused who actually committed the electronic crime and benefits from these doubts. In this way, criminals escape the application of justice and the law.Therefore, the judge's conviction of guilt must reach the level of certainty, since conviction is the fruit of certainty[17].

The prevailing opinion in Canadian jurisprudence considers the output of the computer or the computer to be among the evidence that has the desired certainty in criminal judgments, and therefore it is one of the best and most appropriate evidence. Some American laws have also established that the best evidence granted to prove data and information are the copies extracted from the data stored in the computer, and therefore it is considered the best evidence and the principle of certainty is achieved in it[18].

The Second Axis: Basis for the Acceptance of Digital Evidence in the Light of Criminal Evidence Systems

The evidentiary value of electronic output from a computer lies in its inferential power to prove the truth of the accusation against the suspect. Evidence systems have differed in their assessment of the probative value of such output as follows:

First: The Anglo-Saxon system

This system is known as the system of defined evidence or the system of legal evidence, where the evidence is predetermined and specified by the legislator. The judge is not allowed to deviate from this evidence or to base his judgement on evidence that contradicts it. In a case where the conditions of the evidence defined by the legislator are met, the criminal judge is obliged to base his judgement on this evidence, even if he is not convinced by it. If the statutory conditions are not met, the criminal judge is obliged to base his conviction and sentence on the lack of proof of the accusation, even if the judge is convinced of the validity of the accusation[19].

It should be noted that among the countries that use this system are England, the United States, Australia and South Africa[20]. Evidence in the Anglo-Saxon system is subject to specific rules for its admissibility in court, whether these rules relate to the content of the evidence, such as the exclusion of hearsay testimony, or to the manner in which the evidence is presented, known as the "best evidence rule"[21]. Electronic evidence is considered to be a type of evidence that requires hearsay testimony because it may contain statements or materials created by a particular person on a computer or the Internet. So what is the position of electronic evidence in relation to the rule of exclusion of hearsay evidence? Is it rejected and therefore excluded as criminal evidence, or is it accepted and on what basis?

Hearsay testimony is rejected in criminal evidence in jurisdictions based on the Anglo-Saxon system. However, a list of exceptions to the hearsay rule has been established, including data and information extracted from a computer[22].

The experience of the English judiciary has been that even when electronic evidence is admitted in criminal proceedings as an exception to the hearsay rule, it has been accepted as direct testimony. One of the cases that illustrates this is R v Wood. The events of this case revolve around the theft of some metals by an individual which were later found in the possession of another individual who became the defendant. The chemical composition of these metals was recorded on the victim's computer and the printout from the computer was produced as evidence. The court ruled that the printout from the

victim's computer was admissible as evidence under general law, as it was not hearsay but direct testimony[23].

Another example of the judiciary considering electronic evidence as direct evidence rather than hearsay is the case of R v Pettingreme. The facts of the case are that a person robbed a bank and was arrested some time later. The serial numbers of the banknotes were recorded on the bank's computer in England, and the court accepted the computer printout as direct evidence, not hearsay[24].

As for the United States, some laws have addressed the probative value of electronic evidence. For example, the Iowa Computer Act of 1984 states that computer media is admissible in evidence as to the programs and data stored therein under section 716(a)(16). Similarly, the Evidence Code of 1983 in the State of California states that copies of computer data are admissible as the best evidence available to prove such data[25].

In Canada, computer-generated records may be admissible as evidence if certain conditions are met. Section 29 of the Canadian Evidence Act sets out a number of requirements that must be met before a copy or extract of a record can be admitted as evidence. The Ontario Court of Appeal in the McMullen case held that for computer records to be accepted as true copies of electronic records, there must be a complete description of the records management system in place at the financial institution, which may include details of the procedures and processes related to data entry, storage and retrieval, in order to establish the reliability of the computer-generated output[26].

Second, the Latin system

also known as the system of free proof or the system of convincing evidence, is based on the freedom of conviction. In this system, the legislator does not define the means of proof, but leaves the judge free to base his judgement on his personal conviction regarding any of the available evidence, without imposing a particular type of evidence. The criminal judge may decide to accept or reject any evidence, provided that his conclusion is consistent with the truth and does not depart from the requirements of reason and logic[27].

Among the legal systems that follow this approach are those of France, Egypt and Algeria[28]. If we examine Algerian legislation, we find that it has enshrined the principle of conviction as a general rule through the provisions of article 212, paragraph 1, which states that "crimes may be proved by any means of evidence, except where the law provides otherwise, and the judge shall pronounce his judgement according to his personal conviction"[29].

This article makes it clear that the principle of freedom of evidence is a general rule and that an exception applies only if the law provides otherwise, in which case the judge is bound by the legal provision. The Algerian legislator has thus recognised this freedom to choose the appropriate method of proof in order to deal with emerging crimes such as cybercrime.

Therefore, the criminal judge is obliged to deal with the emerging evidence as necessary and leading to the revelation of new types of crimes, given the judges' lack of familiarity with all informational aspects.

The results of the application of this principle (the principle of freedom of evidence) include the following:
1- The criminal judge has a positive role in providing, accepting and evaluating criminal evidence, including electronic evidence.
2- The criminal judge can order the Internet service provider to search for and reveal the truth, such as the websites and pages accessed by the accused, the dialogues and files in which they participated, and the messages they sent or received.
3- The criminal court may order the system operator to provide the information necessary to penetrate and access the system, as well as the secret passwords and codes used to operate the various programmes.
4- The criminal court judge may order the search of computer systems by examining the Internet connection system and the components of the computer and its accessories.

Thirdly, the mixed system.
The mixed system is the system that combines the two previous systems, the Anglo-Saxon system and the Latin system. Therefore, the mixed system relies on the law to establish certain evidence to prove some facts but not others, or it establishes conditions for the evidence in some cases, or it gives the judge freedom to evaluate the legal evidence. An example of this is the Japanese procedural law, which has limited the accepted means of proof to the following (the defendant's statements, witness statements, presumptions and expert opinions). Regarding computer and Internet evidence, Japanese jurisprudence states that electromagnetic records are inherently invisible and therefore cannot be used as evidence in court, provided that they are converted into a visible and readable form through printer output for such records. In this case, evidence produced by computers and the Internet is accepted, whether it is the original or a copy of the original[30].
It is worth noting that the Algerian legislator has also adopted the mixed system alongside the Latin system, adopting freedom of proof as a general principle through the text of article 212 of the Algerian Code of Criminal Procedure, which we mentioned earlier, and exceptionally through the law, which adopts the principle of legal proof through the phrase "except in cases where the law provides otherwise". It should be noted that there are some crimes for which the Algerian legislator has limited the means of proof, such as the crime of adultery, punishable under article 339 of the Algerian Penal Code[31], which can only be proved by the means exhaustively listed by the Algerian legislator in article 341 of the Algerian Penal Code[32], which states that the proof of the commission of the offence punishable under Article 339 is either a judicial report drawn up by a judicial police officer on a flagrante delicto situation, or an admission contained in letters or documents issued by the accused, or a judicial confession.
As for electronic evidence, it is characterised by the fact that it is invisible in itself and therefore cannot be presented as evidence in court unless it is converted into visible and readable evidence by means of printouts. In this case, it becomes admissible whether it is the original or a copy of the original[33]. This is what the Algerian legislator has chosen, accepting the method of written evidence regardless of the means it contains and the methods of its transmission[34]. It has also stipulated that written evidence in electronic

form is considered equivalent to written evidence on paper, provided that the identity of the person who issued it can be verified and that it has been prepared and stored under conditions that guarantee its integrity[35].

Accordingly, the advent of electronic evidence has significantly changed the methods of criminal proof for crimes that occur in electronic files and documents, especially since electronic evidence is technical in nature and difficult to prove. On the other hand, the subject of electronic evidence, i.e. cybercrime, sometimes transcends the borders of a single state or even an entire continent, which raises problems in the rules of criminal law in terms of conflicts of jurisdiction, whether internal or international. Cybercrime is thus beyond the control or supervision of any specific authority, which makes it impossible to subject it to a specific criminal law. Consequently, the matter requires the conclusion of international agreements aimed at promoting international judicial cooperation in order to resolve the jurisdictional problems arising from cybercrime.

Conclusion

In summary, the search is considered one of the investigative measures with the greatest impact on individual freedom. Therefore, before the criminal judge begins to evaluate the electronic evidence derived from the criminal search, it is necessary to first ensure its validity and suitability as criminal evidence, as well as the existence of the legally established conditions for the acceptance of such evidence. These conditions include the legality of the electronic evidence, the requirement to hear it and the achievement of a degree of certainty in obtaining a judicial conviction. If one of these conditions is not met, the evidence obtained from the search is invalid. It should be noted that the acceptance of electronic evidence varies from one legal system to another, as discussed in the second section.

Finally, we make two important recommendations:

1. The need to focus on training experts, investigators and judges to deal with cybercrime, as well as the continuous development of analysis tools, such as tools for copying disk contents and data storage.
2. The need for international cooperation in the fight against cybercrime, through the conclusion of agreements and treaties criminalising the various forms of such crime. Countries that have not yet criminalised the illegal use of computers should expedite the enactment of the necessary legislation to criminalise this type of transnational crime.

Footnotes:

[1]- Article 40 of the Algerian Constitution of 28 November 1996, Official Journal of the Algerian Republic No. 76 of 8 December 1996, as amended and supplemented by Law No. 02-03 of 10 April 2002, Official Journal of the Algerian Republic No. 25 of 14 April 2002, as amended and supplemented by Law No. 08-19 of 15 November 2008, Official Journal of the Algerian Republic No. 63 of 16 November 2008, as amended and supplemented by Law No. 16-01 of 6 March 2016, Official Journal of the Algerian Republic No. 14 of 7 March 2016.

[2]- Article 47 of the Algerian Constitution of 28 November 1996, ibid.

[3]- Article 38 of the Algerian Constitution of 28 November 1996, ibid.
[4]- Article 46 of the Algerian Constitution of 28 November 1996, ibid.
[5]- Ali Hassan Al-Tawalbeh, Criminal Inspection of Computer and Internet Systems, a Comparative Study, First Edition, Alam Al-Kutub Al-Hadith, Irbid, 2004, p. 179.
[6]- Article 107 of Decree No. 66-156 of 8 June 1966, Official Journal of the Republic of Algeria No. 49 of 1966, containing the Penal Code, as amended and supplemented by Law No. 16-02 of 19 June 2016, Official Journal of the Republic of Algeria No. 37 of 22 June 2016.
[7]- Article 85 of Decree No. 66-155 of 8 June 1966, Official Journal of the Algerian Republic No. 48 of 1966, establishing the Code of Criminal Procedure, as amended and supplemented by Law No. 17-07 of 27 March 2017, Official Journal of the Algerian Republic No. 20 of 29 March 2017.
[8]- Council of Europe activities related to information technology, data protection and computer crime, Asonka, Peter - Information and Communication Technology Law - Oat 19 96.Vol.5.Issue 3.P177.
[9]- Hichem Mohamed Farid Rustom, Computer Crimes as a Form of Emerging Economic Crimes, Journal of Legal Studies, Assiut University, Issue No. 17, 1995, p. 117
[10]- Abdel-Aal Hilali Abdel-Allah Ahmed, The Witness's Obligation to Inform in Cybercrime, a Comparative Study, Al-Nasr Al-Dhahabi, Cairo, Egypt, 2000, pp. 121-122.
[11]- Abd Al-Aal Hilali Abd Al-Ilah Ahmad, The Witness's Commitment to Informing in Cybercrimes, Previous Reference, p. 132.
[12]- Ali Mahmoud Ali Hammoudah, Evidence Obtained from Electronic Means within the Framework of the Theory of Criminal Proof, The First Scientific Conference on the Legal and Security Aspects of Electronic Operations, Organized by the Dubai Police Academy, Research and Studies Center, Issue No. 1 Dubai, United Arab Emirates, 26-27-28 April 2003, p. 38.
[13]- Article 212 of Decree No. 66-155, cited above.
[14]- Aisha Bin Qara Mustafa, The Validity of Electronic Evidence in Criminal Proof in Algerian Law and Comparative Law, Dar Al-Jami'a Al-Jadidah, Alexandria, Egypt, 2010, pp. 271-272-273.
[15]- Fayez Mohammad Rajeh Ghulab, Cybercrimes in Algerian and Yemeni Law, a thesis to fulfil the requirements of a doctorate, Speciality of Criminal Law and Criminal Sciences, University of Algiers 1, Algeria, 2010-2011, p. 413.
[16]- Article 56 of the Algerian Constitution of 28 November 1996, cited above.
[17]- Aisha Bin Qara Moustafa, The Validity of Electronic Evidence in Criminal Proof in Algerian Law and Comparative Law, Previous Reference, pp. 278-279.
[18]- Ali Hassan Al-Tawalbeh, Criminal Search on Computer Systems and the Internet, previous reference, p. 8.
[19]- Labsher Sidi Muhammad, The Role of Digital Evidence in Proving Cybercrimes, Master's Thesis, Specialty of Investigation and Criminal Research, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2010, p. 88.
[20]- Chaima Abdel Ghani Muhammad Attallah, Criminal Protection of Electronic Transactions, Dar Al-Jami'a Al-Jadidah, Alexandria, Egypt, 2007, p. 387.
[21]- Aisha Bin Karrah Mustafa, The Probative Force of Electronic Evidence in Criminal Proceedings in Algerian Law and Comparative Law, op. cit. p. 196.
[22]- Aisha Bin Karrah Mustafa, The Probative Force of Electronic Evidence in Criminal Proceedings in Algerian Law and Comparative Law, op. cit. p. 198.
[23]- chaima Abdel Ghani Mohamed Attallah, Criminal Protection of Electronic Transactions, supra, at 391.
[24]- Aisha Bin Karrah Mustafa, The Probative Force of Electronic Evidence in Criminal Proceedings in Algerian Law and Comparative Law, op. cit., p. 204.
[25]- Esonka, Peter, op. cit., pp. 176-177.

[26]- Abdel-Aal Hilali Abdel-Hah Ahmed, The Probative Force of Computer Outputs in Criminal Evidence, First Edition, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 1997, pp. 55-56-57.
[27]- Lbechir Sidi Mohamed, The Role of Digital Evidence in Proving Cyber Crimes, op. cit., pp. 88-89.
[28]- Aisha Bin Karrah Mustafa, The Probative Force of Electronic Evidence in Criminal Proceedings in Algerian Law and Comparative Law, op. cit. p. 181.
[29]- Article 212(1) of Decree No. 66-155, op. cit.
[30]- Abdel-Aal Hilali Abdel-Hah Ahmed, The Probative Force of Computer Outputs in Criminal Evidence, op. cit., p. 62.
[31]- Article 339 of Decree No. 66-156, op. cit.
[32]- Article 341 of Decree No. 66-156, op. cit.
[33]- Fayez Mohamed Rajeh Ghulam, Cybercrime in Algerian and Yemeni Law, op. cit., p. 405.
[34]- Article 323 bis of Order No. 75-58 of 26 September 1975, Official Journal of the People's Democratic Republic of Algeria No. 78 of 30 September 1975, containing the Civil Code, as amended and supplemented by Law No. 07-05 of 13 May 2007, Official Journal of the People's Democratic Republic of Algeria No. 31 of 13 May 2007.
[35]- Article 323 bis 1 of Decree No. 75-58, op. cit.