THE AUTHORITY OF THE CRIMINAL JUDGE TO ASSESS DIGITAL (ELECTRONIC) EVIDENCE IN JORDANIAN, EGYPTIAN, AND FRENCH LEGISLATION □□□□□□□□□□□□□□□□□□□□□□(□□)□□□□□

Article *in* Journal of Southwest Jiaotong University · October 2022

DOI: 10.35741/issn.0258-2724.57.5.51

3 authors, including:

Hamzeh Abu Issa
Applied Science Private University
45 PUBLICATIONS **78** CITATIONS

SEE PROFILE

西 南 交 通 大 学 学 报

第 57 卷 第 5 期
2022 年 10 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol. 57 No. 5
Oct. 2022

ISSN: 0258-2724 **DOI：10.35741/issn.0258-2724.57.5.51**

Research article

Social Sciences

THE AUTHORITY OF THE CRIMINAL JUDGE TO ASSESS DIGITAL (ELECTRONIC) EVIDENCE IN JORDANIAN, EGYPTIAN, AND FRENCH LEGISLATION

刑事法官在约旦、埃及和法国立法中评估数字（电子）证据的权力

Tawfiq Khashashneh*, Tareq Al-Billeh, Hamzeh Abu Issa
Applied Science Private University
Amman, Jordan, t_khashashneh@yahoo.com

Received: June 18, 2022 ▪ Review: July 14, 2022
▪ Accepted: August 11, 2022 ▪ Published: October 30, 2022

Abstract

The interest that the digital (electronic) evidence enjoys has become great compared to other evidence. In fact, this is due to the spread of the use of digital information technology which role has increased with the entry of the Internet and computers into various areas of life. So, the research issue lies in that this virtual medium has become a hotbed for a range of perpetrators called information criminals. Actually, the crimes they perpetrate are located in the virtual medium, or what can be called the digital or electronic world. In fact, several results and recommendations were reached in this research, the most important of which is that the digital (electronic) evidence is the best evidence to prove this type of crime because it is of the nature of the medium in which the crime was committed. Hence, from here, the interest in this type of evidence began, bearing in mind that the proof of the digital (electronic) crime is not limited to digital (electronic) evidence as it is possible to prove by traditional evidence such as testimony, confession, and others. Therefore, the issue of accepting digital evidence (electronic) is affected only by the extent of the criminal judge's conviction of it if such type of evidence can be subjected to the discretion of the judiciary.

Keywords: Criminal Judge, Discretion, Digital Evidence, Information Systems, Electronic Crimes

摘要 与其他证据相比，数字（电子）证据的兴趣已经变得很大。事实上，这是由于数字信息技术的普及，随着互联网和计算机进入生活的各个领域，数字信息技术的作用越来越大。因此，研究问题在于，这种虚拟媒体已成为一系列犯罪者的温床，称为信息罪犯。实际上，他们所犯的罪行都存在于虚拟媒体中，也就是所谓的数字或电子世界。事实上，这项研究得出了几个结果和建议，其中最重要的是，数字（电子）证据是证明此类犯罪的最佳证据，因为它具有犯罪媒介的性质

。坚定的。因此，从这里开始，对这类证据的兴趣开始了，要记住，数字（电子）犯罪的证据并不局限于数字（电子）证据，因为可以通过证词、供词等传统证据来证明， 和别的。因此，接受数字证据（电子）的问题仅受刑事法官对其定罪程度的影响，如果此类证据可以服从司法机构的自由裁量权。

关键词: 刑事法官、自由裁量权、数字证据、信息系统、电子犯罪

I. INTRODUCTION

The criminal judge assesses the evidence and conducts investigation as well as verification to be convinced of the same [1]. In fact, before issuing his ruling, the criminal judge conducts research and verification until the aspect of the right in the case becomes clear [2]. Yet, and to that effect, he examines the various evidence and presents it in the session for the litigants to examine and refute to reach the truth that satisfies his conscience and to form his personal conviction to achieve justice [3]. Therefore, the authority of the criminal judge toward the evidence is determined within the scope of what the law has specified for him based on legal rules that the judge does not deviate from, otherwise his judgment will be invalid [4].

A. Importance and Objectives of the Study

Accordingly, and from this viewpoint, the judge's work is governed by two systems: First: the legal proof system, in which the legislator restricts the authority of the criminal judge to accept evidence, as the latter does not have the power to deviate from it [3]. Hence, and in case of satisfying the required elements of the evidence as established by the law, then the judge shall be bound to build up his conviction and base his judgment on the basis of this evidence, even if he is not personally convinced of the same. In fact, this system finds a wide scope in civil proof as it prevailed in the past in some systems of criminal proof in the old days. Secondly, a legal evidence system that is closer to the Anglo-Saxon system of evidence, or what is known as the general law system [5], [6].

Based on the foregoing, and in the persuasive evidence system, the legislator allows the judge wide freedom to accept the digital (electronic) evidence according to his personal conviction without imposing a specific evidence of the same whereby he is recognized with a discretionary authority to evaluate the evidence presented to him in the criminal case. This system is one of the most common systems in various procedural legislation as it allows the acceptance of physical evidence and other evidence, such as digital (electronic) evidence resulting from the commission of a digital (electronic) crime because it gives the criminal judge flexibility in accepting evidence extracted from computers based on what is reassuring to him [7], [8].

Yet, in addition to these two systems referred to, a third system appeared, which is the system of scientific evidence that is based on the use of technical methods revealed by modern science in proving the crime and attributing it to the accused person. Actually, and the main role in proving the crime is given to the expert in addition to making the most important evidence as being the presumptions subject to rigorous scientific examination from which evidence of guilt or innocence is extracted [4]. In fact, this system has been particularly popular and well received by the proponents of the positivist school, who predicted a great future for it in that it would replace the system of judicial conviction [9].

Hence, it follows that this restricted system of evidence contradicts proofs in the field of computers and the Internet, which calls for the introduction of amendments to suit these crimes, for which this has led some to call for the acceptance of evidence derived from computers as an exception to the legal evidence system, and hence, the authority of the criminal judge to accept informational evidence in proving a digital (electronic) crime should depend on the flexibility of the criminal judge in accepting the evidence presented to him [10], [11].

B. Materials and Methods

In this research, the comparative applied approach will be followed due to the diversity of legislation that differed in dealing with sections and topics within this topic, in addition to indicating the differences between them and to know the strengths and weaknesses of these various trends as well as the extent of their adoption. Further, this research required to come to the analytical method to analyze all the texts of legislation related to the topic of this research to identify its contents, implications and goals and to criticize and comment on them. Further, the critical approach will also be followed to highlight the views and trends of jurisprudence in

the issues adopted and to highlight the critical aspects of the researcher for each aspect adopted by the jurisprudential trend, for which this research necessitated the use of several approaches due to its complex nature between the texts of legislation, opinions and jurisprudence trends [12].

II. The System of Judicial Conviction and Its Value in Proof with Digital (Electronic) Evidence and Its Limits

Note that, to prove the accusation against the accused, the judge must reach certainty in terms of verifying that the accused committed that crime. In fact, certainty in this case is judicial, not personal certainty and that certainty is reached by the soundness of the evidence that contains persuasion but not extracted from the imagination [13]. Yet, the knowledge required to be available to the judge in the digital (electronic) crime requires familiarity with some scientific rules that help him understand how the crime was committed to reach complete conviction without swinging between innocence and conviction toward the accused, otherwise innocence is the applicable ruling [14].

A. What Is a Judicial Conviction System of the Digital (Electronic) Evidence?

The principle of judicial conviction means that the judge may accept all the evidence presented to him by the parties to the case, as there is no evidence that the law prohibits him from accepting in advance [3], [15]. Further, he may exclude any evidence that does not reassure him, as there is no evidence imposed on him, while he has full discretion in weighing the value of each evidence separately at the end of which he has the power to coordinate between the evidence presented to him and to draw a logical conclusion from this combined and mutually supportive evidence represented by the innocence or conviction ruling [8].

In fact, this principle has been approved by Article 302 of the Egyptian Code of Criminal Procedures, which states that the judge shall rule in the case according to the belief that he has formed with complete freedom and in accordance with the provisions of Article 427 of the French Code of Criminal Procedures, which indicated that, except for cases regulated by law in another way, crimes may be proven by all Methods of Evidence. In fact, the judge shall rule according to his pure conviction and in accordance with the provisions of Article 147/2 of the Jordanian Code of Criminal Procedures, which stipulates that the evidence shall be established in felonies, misdemeanors and violations by all means of proof while the judge shall rule according to his personal conviction.

Hence, and in conclusion to the above, and in the judicial conviction system, judges are not entitled to exclude any means of evidence while they have the right to determine the extent of the evidence found in the digital (electronic) evidence that was collected from the computer container system [9]. However, in this context, all information recorded on the system can be restored before the courts, based on the fact that this information is subject to the rights of the defense (the principle of adversarial judgment) [4].

For this matter, the judge rules according to the principle of his judicial conviction while all elements of the evidence present are subject to his free personal judgment, as in the matter of confession – set in Article 428 of the Egyptian Penal Code as it is permissible to consider that the judicial conviction is the complete equivalent of the concept (without any doubt) and to obtain a high degree of probability but not to reach a definitive confirmation and therefore, the judicial conviction intended here, which stands in a middle position between certainty and belief, and in both cases the judge's decision must be based on certainty and belief, not on conjecture and possibility. Hence, the evidence in criminal matters is characterized as being supportive, i.e., supporting each other as well as being characterized by its finality and dependence on certainty and doubtlessness, meaning the necessity to recognize the crime and the validity of its attribution to the accused on an unquestionable basis [16].

Additionally, according to Articles 1316–2 and 1316–3 of the French Civil Code, electronic writing has the same strength as paper writing while the criminal judge may determine in various ways the most correct decision, whatever he relied upon. Hence, by this method, the judges are responsible for assessing the power of the digital (electronic) evidence submitted to them freely, while the courts have the right to issue highly contradictory decisions, especially in the commercial field [2].

B. Limits of the Principle of Judicial Conviction in the Proof by Digital (Electronic) Evidence

Note that, according to the provisions of Article 427 of the French Code of Procedures, the

judge may base his decision only on the evidence presented to him during the discussion of the criminal case. However, Article 302 of the Egyptian Code of Criminal Procedures states that the criminal judge must rule on the case according to the belief he freely formed. However, he may not base his judgment on any evidence that was not presented to him in the session, which is also consistent with the provisions of Article 148 of the Jordanian Criminal Procedures Code, which states that the judge may not depend except on evidence submitted during the trial, which was discussed openly by the opponents.

Hence, the Jordanian Court of Cassation ruled, in its judgment No. (22/2022) issued on March 30, 2022, that: "In this regard, we find that Article 147 of the Code of Criminal Procedures has given the trial court in criminal matters a wide authority to be convinced of the evidence presented to it and that it has the right to extract what it is satisfied with of the same and to exclude what it is not convinced of fort which the Court of Cassation has no control over the trial court in its assessment of the evidence as long as the judgment was based on foundations derived from established elements in the case papers that lead to the conclusion it reached. Hence, and since the Major Criminal Court, and by its contested decision, has thoroughly discussed the evidence of the case and referred to the evidence on which it relied in forming its conviction in its challenged decision, which is a legal evidence that has a firm origin in the case that leads to the conclusion it reached in addition to having set the legal articles that govern the incidents while its decision included the causes and reasons, which fulfills the purposes of Article (237) of the Code of Criminal Procedures, then the same necessitates refuting these reasons."

Accordingly, and in accordance with the principle of freedom of evidence found in the above-mentioned articles, the complainant has the right to present, before the criminal judge, the physical evidence of the digital (electronic) crime [3], [17]. In this context, all information recorded on the system can be restored before the judiciary, based on the fact that this information is subject to the rights of the defense (the principle of adversarial judgment) and if the outputs of the digital (electronic) means are considered proving evidence in the case papers entertained by the judge, they must be discussed before the litigants, and it follows that these outputs, whether printed or data displayed on a computer screen, or whether being statements included in carriers or in the form of tapes, magnetic or optical disks, or film thumbnails, are subject to discussion when relied upon as evidence before the court [16].

Hence, and if the judge judges by his own conviction and not by the conviction of others, then he must re-check all the evidence in the papers in order to be able to form a conviction that will bring him closer to the realistic truth that every just and diligent judge aspires to [18], and it follows from this principle that the judge cannot rule in digital (electronic) crimes based on his personal knowledge or based on the opinion of others unless the third party is an expert and his conscience is comfortable with the report made before him, so that the conviction on the basis of which he has issued his judgment is generated from his belief and not from the expert's report [11].

III. Power of Digital (Electronic) Documents and Papers before the Criminal Court

Computer outputs mean not only the papers that come out of the printer, but also the data that the computer records on various supports, e.g., disks, magnetic disks, or the device's memory itself [19]. In fact, the problem with digital (electronic) documents is that the information that is recorded on electronic media cannot be read with the naked eye, thus it is considered invisible evidence, and therefore, this recorded information can only be extracted by special spinning devices and with the help of a computer called a spinning device for information storage media [20]. Furthermore, the tapes and connected supports can also be read only by using a computer [2].

Yet, and if the rule in criminal cases is the permissibility of proof by all means of legal proof, then the evidence must be one of the evidence accepted by the law, and therefore the importance of the law's recognition of evidence of a digital (electronic) nature emerges, especially since informatics is almost the only evidence tool that is used to search for evidence regarding the crimes committed by computer, such as cases of money seizure by manipulating information stored in the memory of the computer and its programs, to transfer all or some of the balances of others to the offender's account, and therefore the digital (electronic) evidence revealed by the computer is what helps to reveal the truth, and then the evidence revealed by the computer is a necessary and sufficient method of proof [6].

In fact, and if the general principle is the

freedom of the criminal judge to form conviction from any evidence he deems appropriate, including written evidence and the written document as a proof that is subject to the principle of (judicial conviction), then every value derived from the judge's conviction of the validity and truthfulness of the data contained in it shall be considered while the judge must derive this conviction in accordance with the general rules of criminal evidence, so that the new digital (electronic) documents stored on new media such as microfilm and perforated supports of all kinds, as one of the computer outputs, connected paper supports and outputs on tapes and CDs, do not easily adapt to the traditional rules of evidence, especially in terms of the availability of the elements of written evidence, the concept of the image or copy and its authenticity [4], as well as the difference in the system and form of storage, preservation and retrieval, because the only recognized method so far to prove legal actions in civil matters and mixed works is writing [19]. In fact, the legal system of civil proof is based mainly, in Jordan, Egypt and France, on a written a paper document signed by hand from whom the writing was issued. Therefore, writing on the one hand and a written signature on the other hand are the two elements of complete written evidence in the traditional systems of proof [6].

Hence, the Irbid Court of First Instance, in its appellate capacity, ruled, in its judgment No. (2426/2022), issued on May 16, 2022, that: "As for the first and second reasons for the appeal, the effect of which that the court erred when it issued a verdict of conviction, as this case needs technical expertise or technical experts to download the voice recordings "WhatsApp message" and then preparing a detailed experience report while the expert's testimony will be the final decision in the case - as the cybercrime law has drawn new ways for the legislator to prove - which is the informational or digital evidence – which the Jordanian legislator calls the electronic evidence - and the proof of electronic crimes depends on the electronic evidence being the only way to prove this type of crime, and since the complainant's attorney dismissed this evidence "experience", as it is the basis evidence in this case, and therefore, the court had to declare innocence and/or lack of responsibility because the WhatsApp message was not downloaded by a specialized expert or experts in addition to that the court erred when it relied on contradictory and faltering traditional testimonies and evidence that are not suitable for conviction, as these evidence are not suitable for conviction - as electronic evidence is the product of modern technology which gathering and extraction is made by special and technical programs of high technique- being an intangible evidence which turns to be a material evidence when preparing the experience report with its content through an expert whose testimony shall be heard by the prosecution or the court which the court did not do, as the complainant's attorney dismissed the technical expertise .. Since the statements of the defendant who appealed to the public prosecutor, which is a confession to be considered, in which she mentioned that she sent the audio message, the subject matter of this case on February 25, 2021, and the content of this audio message is a threat, then there is no need to conduct technical expertise, especially since the defendant did not submit any evidence refuting the evidence of the prosecution, and therefore these reasons do not refute the appealed decision and requires dismissal."

Yet, and in another ruling, the Amman Criminal Court of First Instance - Misdemeanors of First Instance, ruled, in its judgment No. (2298/2018) issued on November 19, 2018 that: "With regard to the offense of slander and contempt through the information network, the impersonation of an electronic account and the impersonation of the account owner without permission, then the court finds that the Facebook site named (h h), which is the site that was used to send messages of defamation, slander and contempt to the complainant while the evidence was not presented by the Public Prosecution that the suspect was the one who used that account, created it, or impersonated it for him but, on the contrary, the expert report made on 31 January 2016, on the suspect's cell phone and number, stated that it was found that an account on the Facebook site (h h) was not used in addition to the fact that the complainant, the prosecution's witness mentioned in his testimony that he asserted that the suspect had nothing to do with those messages and that they were sent to him from Iraq while the suspect resides in Jordan, which necessitates in this situation, and for not presenting sufficient evidence to link the suspect to these two crimes, declaring his innocence from them.

A. Criminal Courts Follow the Methods for Proving Established in the Special Law Regarding Digital (Electronic) Evidence

The criminal courts follow the methods for proving established in the special law, but the problem is mainly limited to civil articles in the extent to which these new technical means agree in completing transactions with the legal

requirements to prove legal actions on the one hand, and the extent to which the new media is accepted as convincing evidence in criminal proof on the other hand [9].

In fact, it is legally established that the criminal courts are competent to adjudicate civil matters, on which the decision in the criminal case depends, as Article 225 of the Egyptian Code of Criminal Procedures stipulates that the criminal courts shall follow, in non-criminal matters which are decided according to the criminal case, the methods for proving established in the law related to those issues.

Hence, and based on the foregoing, the problem appears here if the civil issues to be decided upon are recorded in a microfilm or in an electronic document, as it is required in this case to follow the rules of civil proof, whether concerning the elements required in these documents or concerning the extent of their power in proving [2].

But we do should note that in this case, and in order that the evidence stored electronically can be considered conclusive evidence, this depends on the accuracy of the devices used to detect fraud. So, and if these devices are accurate and detect fraud by an expert, then they are conclusive evidence [11]. Therefore, digital (electronic) evidence can be used as conclusive legal evidence when the legislature states that digital (electronic) information is evidence to prove civil and commercial actions [16], [21].

In fact, some comparative legislation accepts the sources of information related to the computer or obtained from its systems, such as the outputs of the automated data processing system, the data written on its screen, and the data recorded on magnetic supports or stored within the processing system as evidence on which the criminal proof is based and that this evidence obtained from digital means (electronic) is subject to the discretionary power of the criminal judge [14], [22].

However, this problem does not appear in the Latin system, where the principle of the criminal judge's freedom to be convinced of the outputs obtained from digital (electronic) means prevails [9]. As for the problem in systems that adopt the legal evidence system or the system of (general Sharia), according to which it is permissible to accept any evidence of proof [3], [23].

Hence, the Zarqa Court of First Instance ruled, in its appeal capacity, issued the judgment No. (176/2021) on January 26, 2021 to the effect that: "In this, we find that proving in criminal matters is permissible by all means of proof, and that the criminal judge rules according to the evidence presented and his sentimental conviction derived from the evidence submitted by the Public Prosecution or the defense's evidence based on the text of Article (147) of the Code of Criminal Procedures as the criminal legislator did not restrict the criminal judge to evidence of itself without another except for specific crimes exclusively. Further, that the legislator, in the Code of Criminal Procedures, has approached tangible evidence and did but has not caused the electronic evidence to be covered singly by any provisions in the aforementioned law. Furthermore, the cybercrime law did not specify how to access the electronic evidence, but the law gave authority to the electronic evidence if it was obtained according to the technical basis in collecting the electronic evidence and provided that the access to it is legitimate. In fact, note that, in electronic crimes, in most cases, it is reached through technical electronic means according to equations and means of research related to the electronic evidence, and that the electronic evidence is of power in proving the electronic crime and the extent to which it is related to the perpetrator (the cybercriminal). Yet, and as we find, with reference to Report No. (4371/2003) dated 4 March 2020 issued by the Department of Laboratories and Criminal Evidence/Electronic Forensic Evidence Department, Digital Evidences Branch/Criminal Investigation Department, kept in the investigative file, from which it is found that after examining the mobile device of the model (Samsung Grand) of the black color, and after retrieving all existing and deleted photos and videos on the device to search for traces of the use of an account on the Instagram website (C), the account (C), the Instagram account (C) and the account (C), then the same was not found regarding the effects of using the Instagram account referred to above or the account that bears the identifier referred to above, with which we find that the digital (electronic) evidence contained within the evidence of the Public Prosecution does not refer to the appellant's use of any of the accounts that were examined on the seized device that is the subject of the case, meaning that the evidence submitted did not prove the issuance of any insulting or slanderous expressions towards the complainant in this case on the one hand, and on the other hand, and with reference to the evidence of the person (witnesses) of the Public Prosecution represented by the testimony of the complainant, then what was mentioned in these testimonies regarding the use of any Instagram accounts by the defendant is just a statement that lacks technical evidence for which it has been

proven through the report issued by the Electronic Evidence Department/in the Investigation Department that there are no traces of using any Instagram accounts or any websites by the defendant that offend the complainant in any way since the focus of cybercrime is the extracts written on an electronic support, from which evidence is obtained electronically and by means of technical means to obtain digital evidence to prove electronic crimes for which we find that what was referred to in these reasons is relative and refutes the appealed decision for which the judgment must be annulled and the appellant declared innocent of the crime ascribed to her due to the lack of legal and convincing evidence against her".

B. The Digital (Electronic) Evidence Must Be Related to the Incident in Question Being Entertained before the Court

Based on the foregoing, the digital (electronic) evidence must have significance so that it exceeds or clearly exceeds its harmful impact on the criminal case [8].

In fact, although the penal legislation set these conditions for accepting proving evidence, this legislation excluded some of the evidence despite the availability of legal conditions in it. Such evidence includes auditory testimony, i.e., the testimony based on indirect knowledge (derived from secondary sources such as other people, books, or records) and that the matter is also related to the testimony that would disclose the secret of the profession, although the countries of the general sharia differ in this matter in terms of its extent or scope [3], [24].

Therefore, it must be emphasized that the restrictions set by general sharia in accepting evidence would reduce the importance of evidence derived from the computer as evidence in computer crimes, if we take the rule of original evidence or the rule of original writing in this system, as this rule requires that the evidence presented in the criminal case is the best that can be obtained in relation to the nature and circumstances of the case, which requires that this evidence be primary and not secondary [4]. However, this raises a problem when proving evidence extracted from the computer, considering that they are electronic signals or electronic impulses that can only be viewed through the computer as they are not seen with the naked eye [11], [25].

In fact, since the objective of the evidentiary process is to establish valid evidence on which the criminal judge relies in his rulings, so the extent of the power of these outputs is searched according to what the legislator decided in the field of proof whereby the legislations, the subject of the study, adopted the method of the Latin legislations and relied upon the free proving system or the system of the artificial evidence in which system the law does not draw specific ways of proof that the criminal judge is bound by, but rather the freedom of proof is generated for the parties to the litigation to present what they deem appropriate to persuade the judge to form his belief based on any evidence presented before him, while he has the right to assess the persuasive value of each of them according to what unfolds in his conscience, as there is no authority over him except his conscience [2], [26].

In fact, it is clear from this that the judge is absolutely free to use all methods of proof to search for the truth and reveal it as long as these methods are legitimate and he evaluates every evidence presented before him because the principle of freedom and conviction of the criminal judge in assessing the value of evidence exists while he may derive it from any source that reassures him which is without the legislator dictating to him a specific authority or obligating him to follow specific means to reveal the truth as a general rule [16], [27]. In fact, the most probable justification for the emergence of this principle, established by the law for the criminal judges, is the emergence of the scientific evidence [6], [28].

Yet, perhaps it is useful to confirm that the criminal judge decides in the case he is entertaining based on the conviction that he derives from the evidence of the case presented to him when it is being considered [8], [29].

Hence, the Jordanian Court of Cassation ruled, in its judgment No. (1303/2022) issued on July 17, 2022, that: "With regard to the felony of indecent assault of a female who has completed fifteen and has not completed eighteen years of age, in violation of the provisions of Article (298/1) Penal and as indicated by Article (15) of the Electronic Crimes Law, and where there was no evidence linking the accused to this crime or that he photographed the victim while she was naked, or otherwise asked her to take off her clothes and watched by him through the phone camera while they were communicating on her phone together and that the prosecution did not provide evidence that the accused committed this crime and that the victim did not mentioned this incident for the police's statements, especially since the accused denied committing this crime, as the penal judgments are based on certainty and belief, not on doubt and guesswork, for we which

should declare the accused's innocence of this crime".

IV. CONCLUSION

The outputs obtained from digital (electronic) means do not represent a problem in the Latin system where the principle of the criminal judge's freedom of conviction prevails. Hence, the French jurisprudence approaches the power of these outputs in the criminal articles within the matter of accepting the evidence obtained from tools or scientific evidence, which should not be accepted as a means of proving unless satisfying the conditions set for the same.

In fact, the acceptance of evidence obtained from digital (electronic) means raises many problems considering the Anglo-American rules of criminal proof, which embrace, as a basic principle, the proof by testimony related to the incident in question. Therefore, the acceptance of printed documents for the outputs of digital (electronic) media, which are electronic signals and magnetic pulses, represents a problem before the judiciary in this system as neither the jurors nor the judge can debate the evidence generated by them or put their hands on it and this makes the same as secondary and unoriginal evidence.

Hence, and from this viewpoint, it is necessary to develop special procedural texts regulating the use of modern technologies in the detection and use of digital evidence (electronic) as well as its use in the scene of electronic crime as well as extracting digital evidence and dealing with it to be evidence acceptable to the judiciary.

Additionally, attention must be paid to preparing experts and specialists based on the use of scientific means at the scene of electronic crime to deal with digital (electronic) evidence in an attempt to bring the real truth closer to the judicial truth.

Finally, the research revealed to us the importance of digital (electronic) evidence in criminal proof, especially if it was obtained within the stipulated legal controls. Therefore, we suggest that specialized experts be prepared to examine digital (electronic) evidence in high-tech digital forensic laboratories.

ACKNOWLEDGMENT

The authors would like to thank Applied Science Private University for their support of this research.

REFERENCES

[1] BAZIN, P. (2014) An outline of the French law on digital evidence. *Digital Evidence and Electronic Signature Law Review*, 5, pp. 179-182.

[2] HASSAN, S. (1999) *Proving Computer Crimes and Crimes Committed via the Internet*. Cairo: Dar Al-Nahda Al-Arabiya.

[3] HOSNI, M. (1997) *Explanation of the Code of Criminal Procedures*. Cairo: Dar Al-Nahda Al-Arabiya.

[4] ATALLAH, S. (2007) *Criminal Protection of Electronic Transactions*. Alexandria: New University House.

[5] LEACOCK, C. (2014) Search and seizure of digital evidence in criminal proceedings. *Digital Evidence and Electronic Signature Law Review*, 5, pp. 221-225.

[6] AL-SAGHIR, J. (2001) *Proof of Criminal Evidence and Modern Technology*: *A Comparative Study*. Cairo: Dar Al-Nahda Al-Arabiya.

[7] HANNON, M.J. (2012) *Digital evidence: computer forensics and legal issues arising from computer investigations*. Buffalo, New York: William S. Hein.

[8] AFIFI, A. and AL-SHAZLY, F. (2003) *Computer Crimes, Copyright, the Role of the Police and the Law: A Comparative Study*. Beirut: Al-Halabi Law Publications.

[9] AL-MASRI, A. (2004) *Internet Fraud Crimes*. PhD thesis, Cairo University.

[10] LEWULIS, P. (2021) Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics*, 13 (1), pp. 403-417.

[11] MUSTAFA, A. (2009) *Computer Crimes in Egyptian Legislation: A Comparative Study*. Cairo: Arab Renaissance House for Publishing and Distribution.

[12] MALKAWI, B. (2008) *The Scientific Origins of Writing Legal Research PhD and Master's Theses*. Jordan: Dar Wael for Publishing.

[13] LUND, P. (2014) An investigator's approach to digital evidence. *Digital Evidence and Electronic Signature Law Review*, 6, pp. 220-222.

[14] OMAR, N. (2000) *Criminal Protection of the Electronic Store in Information Crimes*. Alexandria: New University Publishing House.

[15] MANOLEA, B. (2014) The digital economy - where is the evidence? Theoretical and practical problems in understanding digital evidence in Romania. *Digital Evidence and Electronic Signature Law Review*, 5, pp. 226-230.
[16] SULEIMAN, A. (2005) *Strategy for Combating Crimes Arising from the Use of the Computer: A Comparative Study*. Ph.D thesis, Police Academy.
[17] MOORE, R. (2005) *Search and seizure of digital evidence*. LFB Scholarly Publishing.
[18] ABU ISSA, H., ISMAIL, M., and AAMAR, O. (2019) Unauthorized access crime in Jordanian law comparativestudy. *Digital Investigation*, 28 (1), pp. 104–111.
[19] AL-BILLEH, T. (2022) Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. *Pakistan Journal of Criminology*, 14 (1), pp. 1–14.
[20] ISSA, H.A. and ALKHSEILAT, A. (2022) The cyber espionage crimes in the Jordanian law. *International Journal of Electronic Security and Digital Forensics*, 14 (2), pp. 111-123.
[21] MARCELLA, A.J. and GUILLOSSOU, F. (2012) *Cyber forensics: from data to digital evidence*. Hoboken, New Jersey: Wiley.
[22] CHAN, G.J., MAGOTIAUX, S., GREENSPAN, B.H., and RONDINELLI, V. (2021) *Digital evidence*. Toronto: Emond Publishing.
[23] NILSSON, J.D. (2010) *Digital evidence in the courtroom*. Hauppauge, New York: Nova Science Publishers.
[24] SCHELLEKENS, M. (2014) Digital watermarks as legal evidence. *Digital Evidence and Electronic Signature Law Review*, 8, pp. 152-164.
[25] OPARNICA, G. (2016) Digital evidence and digital forensic education. *Digital Evidence and Electronic Signature Law Review*, 13, pp. 143-147.
[26] CASEY, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. Burlington, Massachusetts: Academic Press.
[27] DI CERBO, S. (2021) *Digital evidence changing the paradigm of human rights protection*. Oisterwijk: Wolf Legal Publishers.
[28] SCANLAN, T. (2014) Search and seizure of digital evidence: thresholds and minefields. *Digital Evidence and Electronic Signature Law Review*, 5, pp. 240-244.
[29] UMBERG, T. and WARDEN, C. (2014) Digital Evidence and Investigatory Protocols. *Digital Evidence and Electronic Signature Law Review*, 11, pp. 128-136.

参考文:

[1] BAZIN, P. (2014) 法国数字证据法概述。数字证据和电子签名法评论，5，第 179-182 页。
[2] HASSAN, S. (1999) 证明计算机犯罪和通过互联网实施的犯罪。开罗：达尔•纳赫达•阿拉比亚。
[3] HOSNI, M. (1997) 刑事诉讼法解释。开罗：达尔•纳赫达•阿拉比亚。
[4] ATALLAH, S. (2007) 电子交易的刑事保护。亚历山大：新大学大楼。
[5] LEACOCK, C. (2014) 在刑事诉讼中搜索和扣押数字证据。数字证据和电子签名法评论，5，第 221-225 页。
[6] AL-SAGHIR, J. (2001) 刑事证据证明与现代技术：比较研究。开罗：达尔•纳赫达•阿拉比亚。
[7] HANNON, M.J. (2012) 数字证据：计算机取证和计算机调查引起的法律问题。纽约布法罗：威廉•海因。
[8] AFIFI, A. 和 AL-SHAZLY, F. (2003) 计算机犯罪、版权、警察和法律的作用：一项比较研究。贝鲁特：哈拉比法律出版物。
[9] AL-MASRI, A. (2004) 互联网欺诈犯罪。博士论文，开罗大学。
[10] LEWULIS, P. (2021) 波兰刑事诉讼中的数字取证标准和数字证据。法医学中数字证据的更新定义。国际电子安全和数字取证杂志，13 (1)，第 403-417 页。
[11] MUSTAFA, A. (2009) 埃及立法中的计算机犯罪：一项比较研究。开罗：阿拉伯文艺复兴时期的出版发行公司。
[12] MALKAWI, B. (2008) 撰写法律研究博士和硕士论文的科学起源。约旦：达瓦尔出版。

[13] LUND, P. (2014) 调查人员处理数字证据的方法。数字证据和电子签名法评论，6，第 220-222 页。
[14] OMAR, N. (2000) 信息犯罪中电子商店的刑事保护。亚历山大：新大学出版社.
[15] MANOLEA, B. (2014) 数字经济——证据在哪里？罗马尼亚理解数字证据的理论和实践问题。数字证据和电子签名法评论，5，第 226-230 页。
[16] SULEIMAN, A. (2005) 打击使用计算机引起的犯罪的战略：一项比较研究。博士论文，警察学院。
[17] MOORE, R. (2005) 数字证据的搜索和扣押。LFB 学术出版。
[18] ABU ISSA, H.、ISMAIL, M. 和 AAMAR, O. (2019) 约旦法律比较研究中的未经授权访问犯罪。数字调查，28 (1)，第 104-111 页。
[19] AL-BILLEH, T. (2022) 约旦立法对在互联网上发布节目犯罪的法律控制。巴基斯坦犯罪学杂志，14 (1)，第 1-14 页。
[20] 国际社会保障协会，H.A. 和 ALKHSEILAT, A. (2022) 约旦法律中的网络间谍罪。国际电子安全和数字取证杂志，14 (2)，第 111-123 页。
[21] 马塞拉，A.J. 和 GUILLOSSOU, F. (2012) 网络取证：从数据到数字证据。新泽西州霍博肯：威利。
[22] CHAN, G.J.、MAGOTIAUX, S.、GREENSPAN, B.H. 和 RONDINELLI, V. (2021) 数字证据。多伦多：埃蒙德出版社.
[23] NILSSON, J.D. (2010) 法庭上的数字证据。哈帕克，纽约：新星科学出版社。
[24] SCHELLEKENS, M. (2014) 数字水印作为法律证据。数字证据和电子签名法评论，8，第 152-164 页。
[25] OPARNICA, G. (2016) 数字证据和数字法医教育。数字证据和电子签名法评论，13，第 143-147 页。
[26] CASEY, E. (2011) 数字证据和计算机犯罪：法医学、计算机和互联网。第三版。马萨诸塞州伯灵顿：学术出版社。
[27] DI CERBO, S. (2021) 改变人权保护范式的数字证据。奥斯特韦克：狼法律出版社。
[28] SCANLAN, T. (2014) 搜索和扣押数字证据：阈值和雷区。数字证据和电子签名法律评论，5，第 240-244 页。
[29] UMBERG, T. 和 WARDEN, C. (2014) 数字证据和调查协议。数字证据和电子签名法评论，11，第 128-136 页。