American Journal of Social and Humanitarian Research

Vol. 5 Issue 10 | **pp.** 310-313 | **e-ISSN:** 2690-9626
Available online @ https://www.globalresearchnetwork.us/index.php/ajshr

The Role of Judicial Expertise in Cybercrimes

Dr. Rifea Abdullah Hameed [1]

[1] Assistant Lecturer mustafa kamil majeed, Samarra University - Faculty of Law

Abstract:

The role of scientific proof of evidence has increased with the emergence of electronic crimes and the necessity of deriving the digital evidence required to prove these crimes and revealing patterns of crimes committed using computers, a role played by judicial experts. The establishment of digital forensic laboratories has become an urgent requirement for examining digital evidence and evaluating the digital proof process. And the analysis of crimes within the scope of what is known as security expert systems , and despite the fact that the Egyptian Code of Criminal Procedure has set out the rules of criminal proof, criminal law jurists have elaborated and explained these rules in detail, and the Court of Cassation has established many legal principles since its inception to collect evidence and for the validity of the evidence, but crimes Due to its relative newness, electronic crimes did not receive sufficient explanation and codification of the procedures for proving them, whether from a legal or technical perspective, which placed a heavy burden on those concerned with detecting and investigating these crimes, as judicial expertise plays an important role at that stage.

Therefore, in this research, we will address the role of judicial expertise in the process of criminal proof of electronic crimes, with a focus on the field of electronic judicial expertise in particular

This research is divided into two sections as follows:

requirement: the legal rules that govern judicial expertise in cybercrimes.

requirement: The technical rules that govern the work of the expert in the field of cybercrime.

Finally, we concluded the research with a conclusion, in which we reached a number of conclusions and recommendations, and we ask God that we have succeeded in reaching them.

Citation: Hameed , D. R. A. . (2024). The Role of Judicial Expertise in Cybercrimes. American Journal of Social and Humanitarian Research, 5(10), 301–313. Retrieved from https://globalresearchnetwork.us/index.php/ajshr/article/view/2983

Received: 21 Aug 2024
Revised: 12 Sep 2024
Accepted: 20 Sep 2024
Published: 18 Oct 2024

First: Introduction:

There is no doubt that the theory of evidence is the basis on which the rules of criminal procedure are based from the moment the crime occurs until the ruling is issued by the judicial authority in accordance with the powers granted to it. Scientific evidence is defined as evidence taken from computers and is in the form of magnetic or electrical fields or pulses. They can be collected and analyzed using special programs, applications and technology. The expert's report, with the skills he possesses, makes the criminal judge more convinced, more decisive, and more certain, which helps

reduce judicial errors, approach justice with broader steps, and reach a greater degree towards the truth. The criminal judge, with the authority he possesses. It is discretionary and does not deal with material evidence. This is because the value of the evidence is based on scientific foundations, principles and facts that are characterized by consistency and stability. Modern scientific evidence requires examination and evaluation, which makes it difficult or even impossible for the judge to address it alone through examination and evaluation. Therefore, the role of technical judicial expertise from an expert specializing in the issues increases. Technically, the expert does not replace the judge in assessing the evidence. On the contrary, the criminal judge has complete freedom to be convinced by the expert's report, and he has the right to submit it if it becomes clear to him that it does not agree with the circumstances and circumstances of the incident.

Second: The importance of research:

The importance of this research is to identify the importance of technical expertise in cybercrimes, clarify the laws to which the perpetrator of this new type of crime will be subject, and the provisions that apply to it, and the increasing role of resorting to specialized experts in the technical fields in order to extract evidence from computers and provide specialized experts in order to ensure Preventing criminals from escaping punishment in electronic crimes and enhancing the conviction of the criminal judge by informing him of all legal and technical issues to reach a fair ruling.

Third: Research hypotheses/questions:

This topic raises a number of questions: What is the role of experience in convincing the criminal judge to evaluate the evidence for electronic crimes? What distinguishes technical expertise in cybercrime? How can we imagine this type of crime occurring between people who do not know each other? What is the role of the Internet in committing this type of crime? Are the punitive legal texts that regulate cybercrimes contained in the special section of the penal legislation sufficient for the important role played by judicial expertise in cybercrimes and the increasing role of the expert therein for this type of new cybercrimes?

In view of the great importance of this topic, and the abundance of this type of crime on the Internet and using modern technologies, there appeared to be an urgent need for legislative intervention to address and combat this type of crime, and from here we chose to study and research this type.

Fourth: Research methodology:

In this research, I used the inductive, analytical, and comparative method. The texts of criminal laws were analyzed, taking into account in this regard some Arab criminal legislation that codified the role of technical expertise in cybercrime in its legislation.

Fifth: Research objectives:

The research aims to the following :

1. Explaining the concept of judicial expertise in cybercrimes

2. A statement of the legal rules governing judicial expertise in cybercrimes

3. Knowledge of the provisions of Arab criminal laws regarding judicial experience in cybercrimes

4. Drawing the attention of the judiciary and the legislative authority to the emergence of new crimes committed daily against others and society by means of electronic computers and through the Internet, which requires confronting them through the use of specialized experts to uncover the perpetrators of this new type of crime.

5. Spreading awareness among the investigative and judicial authorities, raising their level of competence, and informing them of everything new in the world of cybercrime.

Sixth: Research plan:

In this research, we will study the role of judicial expertise in the process of criminal proof of electronic crimes, with a focus on the field of electronic judicial expertise, in particular. This research is divided into two requirements as follows:

requirement : the legal rules that govern judicial expertise in cybercrimes.

requirement : the technical rules that govern the work of the expert in the field of cybercrime

Accordingly, the plan for researching the topic was divided into two requirements. In the first requirement, it was addressed to determine the nature of expertise and the extent of the authority of the expert's report and the evidence obtained by electronic means through technical expertise in the first, second and third sections. In the fourth and fifth sections we address the role of acknowledging the authority of electronic means of proof and the areas of expertise. Regarding electronic crimes, in the second section we addressed the difficulties faced by the expert in collecting electronic evidence, in the second section we discussed the requirements for judicial expertise in the field of cybercrimes, and in the third and final section we discussed the process of extracting evidence.

We concluded the research with a set of results and recommendations. We ask God (Y) that we have succeeded in studying this topic and becoming familiar with everything that surrounds it, and God is the Granter of success.

first requirement

Legal rules governing judicial expertise in cybercrimes.

Legal principles require that the judge not resort to technical expertise except with regard to facts whose knowledge or interpretation requires special knowledge that is not available in him, and which are not proven or clear from the documents and documents, or the evidence contained in the case, or those facts that cannot be proven by other means. Such as testimony, evidence, or inspection, so he seeks the help of an expert or technician to clarify them and provide the technical advice he needs to decide the case[(1)]

Therefore, in this requirement, we will address the subject of expertise as follows:

First: What is experience:

Expertise is defined as: "a procedure related to a subject that requires familiarity with technical information in order to extract evidence from ita , [(2)] ". nd some jurists have defined judicial technical expertise as: "technical advice that the judge uses in the field of proof to help him evaluate some issues whose evaluation requires special information." And scientific or artistic competence that he does not have by virtue of his work and culture. [(3)] "

[(1)] Garraud (R.), Traite Theorique et Pratique d'instruction Crime and Procédure Penale , I. Sirez 1907, n. 317, p. 592. Merle (R.) & Vitu (A.), Traite de droit Penal and criminological , II, 2nd edition ., Dalloz , 1970, n. 1193, p. 1138. Merle (R.) & Vitu (A.), Traite de droit criminelle , problems Generaux de la science criminalelle , Droit penal General 6th edition , 1984, Cujas n. 164, p. 211.

[2]Dr. Maamoun Muhammad Salama, Criminal Procedures in Egyptian Legislation, Dar Al-Fikr Al-Arabi for Printing and .Publishing, Cairo, 2001, p. 645

[3]Dr . Amal Othman, Technical Expertise, Criminal Matters, A Comparative Legal Study, PhD thesis, Faculty of Law, Cairo .University, 1964, p. 19

Experience, as evidence in proof, refers to the expert's opinion, which he confirms in his report . [4] Since the expert's report is considered technical evidence, the procedure for delegating an expert is one of the procedures for collecting evidence. The investigator may seek the assistance of experts to seek their opinion on some of the matters that were exposed to him during his mission in the investigation, which ends with issuing a A decision that there is no reason to file a case or to refer it to the trial court. As for experience at the trial stage, it helps the judge in forming his belief to decide the case . [5] The facts on which expertise can be determined are limited to the material facts, not the legal issues that remain within the jurisdiction of the judge alone, as it is not permissible The judge has the right to delegate this authority to another person, and the judge in charge of deciding the case may resort to judicial technical expertise whenever he encounters a technical issue on which the decision of the case depends, as it is inconceivable that the judge will understand all the technical issues that are presented to him and be able to decide on them in a complete and comfortable manner. His conscience and achieves justice. [6]

An expert is every person who has special knowledge of an issue, and the investigation may require examining an issue whose examination requires special technical or scientific competence that the investigator does not feel possesses in himself, so he may consult an expert regarding it, as is the case in determining the anatomical characteristics in murder crimes or analyzing the material grafted into a crime. Poisoning or examination of allegedly forged handwriting. [7]

The legislator has permitted investigative authorities to assign experts if the nature of the crime under investigation requires the assistance of the expert to resolve a specific technical issue, or to search for and seize evidence of the crime. The court may also take whatever means it deems appropriate - including assigning experts - to research and understand any technical fact. I intercepted her.

The rule is that the court is the supreme expert, and therefore expert reports are always subject to its discretion. It has the right to reject them completely and to take the opinion of one expert rather than the other. The court also has the authority to decide on issues that are consistent with the facts of the case, even if the expert's report is not decisive in their opinion, and if two experts disagree. In the opinion, the court is not obligated to confront them, but rather it has the right to give preference to one over the other according to its conviction and what it sees as supported by the facts of the case. In doing so, it is not obligated to state the reasons for the preference, nor is it obligated to discuss other reports as long as it sees no issue and the opponents do not ask it for anything of that, and the court has the authority. Discretionary also takes some of what was stated in the expert's report and leaves out the other part without any reasons for that, except in technical issues, as it is not permissible to refute them except with technical supports. [8]

If the assignment of experts is important in traditional crimes, its importance is more important and its necessity is more important in the procedures for collecting evidence of the moral components in all storage units, analyzing it, and detecting any tampering with programs and information. However, this does not mean

(4) .Dr. Mamoun Muhammad Salama, previous reference, p. 645

(5) .Dr. Fawzia Abdel Sattar, Explanation of the Code of Criminal Procedure, Dar Al Nahda Al Arabiya, Cairo, 1986, p. 322

(6) Dr. Essam Mahmoud Abdel Halim Youssef, Criminal Liability for People Suffering from Neurological and Psychological .Diseases, PhD thesis, Faculty of Law, Cairo University, 2014, p. 374

(7) Dr. Ahmed Fathi Sorour, Mediator in the Code of Criminal Procedure, Book One, Dar Al-Nahda Al-Arabiya, Cairo, 2016 .edition, pp. 457 et seq

[8]Dr. Ali Mahmoud Hamouda, Evidence obtained from electronic means within the framework of the theory of criminal proof, research presented to the first scientific conference on the legal and security aspects of electronic operations, Dubai Police .Academy, Research and Studies Center, held from April 26 to 27, 2003, Dubai, United Arab Emirates , p. 6

indifference to the issue of qualifying the prosecuting authorities and providing their members with scientific and technical knowledge to be knowledgeable. This requires recruiting experts and understanding the opinions they provide. Therefore, we find that many developed countries have paid attention to training investigators in electronic crimes, and the European Council, in one of its recommendations in 1999, called for the necessity of training the police and justice agencies in a manner that keeps pace with the rapid development of information technology and its use to achieve a balance between... The means of committing crime and ways to confront it. The International Police Organization also held many training courses for computer crime investigators.

Second: The validity period of the expert's report

Experience, like the rest of the evidential evidence, is subject to its validity at the discretion of the judge and the extent of the influence of the work of expertise on the subjective conviction of the judge. In this article, we will present the importance of the expert's report and the extent of its influence on the subjective conviction of the judge, since the court is obliged to refer to the opinion of technical expertise and take an opinion regarding a technical issue. However, the court The subject has full authority in assessing the evidentiary force of the elements of the call at hand, and she is the supreme expert in everything that she can decide on her own, as long as the issue at hand is not one of the purely technical issues on which the court itself cannot make its way to express an opinion. What it concluded When the court examines the contract that is the subject of the accusation, it does not require experience to evaluate it because the difference in materials can be seen with the naked eye. (9)

It should be noted that although it is established that the court has discretionary authority regarding the assessment of the expert who comes to it, this does not extend to technical issues, so it is not permissible for it to refute them except with technical supports . (10) It is subject to the absolute discretion of the trial court, and therefore the court cannot refute it and respond to it except with technical supports that may be difficult for it to make its way through except through other technical expertise, and if the court has the discretionary power to decide whether the evidence in the case is sufficient and can be dispensed with. As for appointing an expert or not, this is conditional on not being exposed to purely technical issues that are within the scope of investigating the accused's defense. (11)

The Court of Cassation ruled to establish the limits of the discretionary authority of the trial court. .. The court may not replace itself with the technical expert in a technical matter, if the ruling was based - among what it was based on - in convicting the accused - on the fact that the victim had spoken after his injury and disclosed the names of the perpetrators to the witnesses and the defense had challenged the validity of their narrative Witnesses and there is a dispute about the victim's ability to distinguish and understand after his injury, for the judge should have verified it through a technical specialist, which is the forensic doctor, but if she did not do so, then her ruling would be flawed because it violated the right of defense, which must be overturned. (12) "...

Scientific reality shows that the judge often accepts what the expert has stated in his report, and bases his ruling on its basis, and this behavior is logical on the part of the

[9].Appeal No. 145 of Judicial Year 42, session 1/34/1972 AD (

[10]Cassation session of 5/29/1967 AD, Collection of Cassation Rulings, Year 18, p. 143, Cassation session of 11/27/1967 AD, .Year 18, p. 251

[11]Dr. Saad Hammad Saleh Al-Qabaili, The right of the accused to seek assistance from a lawyer, a comparative study, Dar Al-.Nahda Al-Arabiya, Cairo, 2005, p. 89

.Appeal No. 486 of 34 BC, session 6/29/1964 AD, Appeal No. 2397 of 33 AD, session 1/27/1964 AD, p. 384 [12]

judge. There is no doubt that if the expert's opinion is stated on a technical subject, the judge has no jurisdiction over it, and it is not the business of his culture or judicial experience to It allows him to decide on it - in addition to that, he is the one who assigned the expert and trusted him - and he saw that it was appropriate for his mission , [13] so he must take his opinion.

Some jurisprudence sees [14] the necessity of giving compulsory force to the expert's report, on the basis that if the judge rejects the expert's opinion, he has contradicted himself, as this means that he wanted to decide for himself a matter in which he had initially admitted that the expert had knowledge and expertise that exceeded his own. Personal.

Third: Evidence obtained by electronic means through technical expertise

Technical expertise is the investigation of material or technical issues that are difficult for the investigator to find his way into and for which he is unable to collect evidence through traditional means of proof, such as confirming the truth of images that have been modified, or attributing votes to their owners, or verifying the truth of a scene that has been manipulated or not.

In order to determine the truth in such scientific and technical issues, the law permits the investigator to seek the assistance of an expert who specializes in the matter subject of the expertise. The investigator's assignment of the expert is considered one of the investigation procedures that interrupts the statute of limitations. The same applies to filing the expert report, but the expert work itself has no effect on the statute of limitations. Because they are material works. [15]

In view of the revolution that has occurred in the world of remote communications technology, we find that it has brought scientific techniques of an advanced technical nature, and these technologies have produced crimes of a complex technical and scientific nature, for which collecting evidence requires examining scientific and technical issues, as the evidence may be invisible and it is necessary to Converting them into readable evidence, and they may be the result of tampering with certain accounts or certain electronic accounts, such that their detection requires specialists to prove this tampering.

It may require precise technical operations to gain access to electronic means systems as a result of using secret codes and passwords. If the goal of the expertise is to reach the truth in scientific, technical, and material issues, it is not limited to the investigating authority, but rather the court has the right to order it.

As for electronic crimes, and given their specific nature, discovering them and revealing their truth may require technical expertise, which may be needed from the beginning of the investigation phase for these crimes , and then the need for it will continue in the investigation and trial phases due to the technical nature of the methods of committing them and the moral nature of the site of the attack. [16]

Fourth: Acknowledging the validity of electronic means of proof

Almost all legal systems, such as French law and American law, currently agree on the authenticity of files stored in computer systems and extracts and data retrieved from

[13] Radel J: The books respectifs juge and technicien _ dans The pre- administration , Colloque institutes _ d'études judiciaires (Poitiers, 26 February - 2 March 1975) Publications of the Faculté de droit et de sciences sociales , Poitiers, PUF, Paris, 1976, p.67.

[14] Dr. Amal Othman, Technical Expertise, Criminal Matters, A Comparative Legal Study, previous reference, p. 307 et seq.

[15] Dr. Mahmoud Naguib Hosni, Explanation of the Code of Criminal Procedure, third edition, Dar Al-Nahda Al-Arabiya, Cairo 1996, p. 162.,

[16] Dr. Muftah Boubakar Al-Mutradi , paper presented to the Third Conference of Presidents of Supreme Courts in the Arab Countries in the Republic of Sudan, held from September 23 to 25, 2012, p. 32.

microfilm and microfiche systems, the authenticity of files with a purely technical meaning, acknowledging the validity of the electronic signature and its equality in argument with the traditional signature, and gradually abandoning it. About any restrictions that limit proof in the technical environment , and the few years will also witness a development in the trend towards accepting audio and analog files, files with visual content, and others. (17)

Fifth: Areas of expertise regarding electronic crimes

The tremendous development in the field of information and communications technology - the digital or electronic age - has produced many innovative activities that are carried out using electronic means, which are based on computer systems and programs, and global communications networks , such as e-commerce, banking, e-banking, e-management, and e-government. As a result, the crimes committed by these operations vary according to the type of electronic means used to commit them, and examples of these crimes include: (18)

1. Forging documents entered into computer systems or resulting after processing .

2. Data manipulation.

3. Manipulating basic programs or application programs .

4. Fraud while transferring and broadcasting data .

second requirement

Difficulties facing the expert and his requirements in electronic crimes

Electronic forensic evidence has great importance and a fundamental role in knowing how the crime occurred. To confirm this, the digital forensic investigation must contain this evidence, and the facility must be prepared and prepared for such unusual matters, and the people responsible for dealing with these matters must have a great understanding Undertaking technical matters, their tricks, and how to deal with them.

Computer crimes are characterized by difficulty in discovering and proving, as electronic crime takes place in an environment or framework that has nothing to do with papers or documents, but rather takes place via the computer or the global network, and the perpetrator can use electronic pulses that do not see tampering with the computer data or its programs, in record time. It may be a fraction of a second, and this data or information that has been tampered with can also be erased in record time before the hand of justice reaches it, especially since the control process is only carried out by the knowledge of a technical expert or specialist . (19) In this section, we will discuss the difficulties that the expert faces in Collecting electronic evidence and the requirements for judicial expertise in cybercrimes, as well as the process of extracting evidence from them.

First: The difficulties faced by the expert in collecting electronic evidence

The forensic expert faces many difficulties in collecting electronic evidence from computers or digital networks, including

(17) Dr. Hilali Abdullah Ahmed, Inspection of Computer Systems and Information Guarantees for the Defendant, a comparative .study, Dar Al-Nahda Al-Arabiya, Cairo, 2006, p. 27

(18) Dr. Hisham Muhammad Farid Rostom, Procedural Aspects of Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 1998, p. . 137

(19) Dr. Abdel Fattah Bayoumi Hegazy, Principles of Criminal Procedure in Computer and Internet Crimes , Dar Al-Kutub Al-Qaniya, .Mahalla Al-Kubra, 2007, p. 24

1. A large portion of the information and commands that constitute digital evidence is lost if the computer is shut down incorrectly, or in the event of a sudden disconnection of the power supply to the device. When the power supply to the computer is shut down or cut off, such an act may lead to the erasure of the information. From the device's memory or distorting important data, causing damage to the computer's hardware , or preventing rebooting , thus losing essential evidence.

2. The perpetrator prepared the computer to explode or destroy it by simply turning it on by pressing the Power button .

3. The nature of the crime scene in networks spread around the world, so it may not be possible to obtain evidence if the crime scene is distributed among more than one country due to the complexity of procedures or the existence of practical and legislative problems in some countries, which prevents obtaining electronic evidence, and the speed of traffic Digital data passes through networks for less than a fraction of a second, with criminals being skilled at destroying evidence, distorting, or modifying data to protect themselves, as well as the huge volume of data that passes through networks, which has the opposite effect when searching for evidence of guilt or innocence.

4. Identity concealment, when the user deliberately conceals his identity when using the Internet, whether by performing some actions or using some programs and applications that lead to the obliteration of identity, which constitutes an obstacle for the criminal investigator or technical expert.

5. Hiding information, or the existence of some special programs to hide information or data, in order to create what is known as a secure file system through the use of the World Wide Web, which makes the process of recovering or reassembling evidence extremely difficult for the criminal investigator or expert.

6. From this it is clear that obtaining digital forensic evidence is difficult to obtain because it requires great experience and skill in the field of computers .

Second: Requirements for judicial expertise in the field of electronic crimes

The electronic means and devices that use computer systems are diverse, as are the communication networks between them, and their technical characteristics are distinct, so they fall under precise technical and scientific specializations. This also requires investigation and trial authorities to be careful when selecting an expert. They must be certain that he or she has the scientific and technical capabilities and abilities in the field of precise specialization in the field he is asked to research. It is not sufficient for the expert to have a specific academic degree, but he must also have experience. Scientific knowledge that enables him to acquire high technical competence and given the technical and scientific nature of expertise in the field of cybercrime, this expertise can be defined in the following topics: [20]

1-Familiarity with computer installation, make, model, main and secondary operating systems, peripheral devices attached to it, passwords or secrets, and encryption codes.

2-The nature of the environment in which the computer operates in terms of organization and extent of concentration or distribution of automated processing work, and specifying storage locations and the means used in that.

3-The ability of the expert to master his task without resulting in damage or destruction of the instrument obtained from electronic means.

4-Being able to transfer invisible evidence and transform it into readable evidence, or maintain its supports until expert work is carried out without damaging or destroying it,

[20] .reference , pp. 142-143 Dr. Ahmed Fathi Saro, previous

while proving that the paper outputs of this evidence match what is recorded on the computer, system or network [21]

In addition, the electronic or information expert must have the knowledge, experience, and skill that enable him to perform his task optimally, so he must be familiar with the following:

1. Computer systems with their hardware and software components.

2. Means, programs, and methods for examining computer systems, such as programs for detecting and removing viruses, programs for retrieving data and information, repairing damaged ones , revealing hidden ones, programs for decoding codes and passwords,...etc.

3. Means and programs for copying programs and files, and making exact copies of the hard disk.

4. How to link physical evidence and digital evidence in the facts under investigation .

5. How to interpret observations, link things, and draw conclusions with scientific, technical, and judicial significance .

Third: The process of extracting evidence

The process of obtaining digital forensic evidence is difficult to achieve because it requires experience and great skill in the field of computers. This is due to the many forms and types of cybercrimes, ranging from attacking information for the purpose of destroying or seizing it, or the attack may be intended for devices, such as spreading a virus that works. To destroy its main units, for example, or it may be just hacking the password of a bank or a major institution for the purpose of fraud and obtaining money, or it may be just to prove oneself and demonstrate high ability in the field of computers, and since the process of compiling forensic scientific evidence in electronic or digital crimes It is considered one of the most important and difficult matters facing the criminal proof process, so it was necessary to resort to a specialized forensic information or digital expert to derive scientific and technical forensic evidence. He is the specialized expert and trained to process, evidence [22]. examine and analyze all types of digital

Some specialists believe that the process of collecting digital evidence in digital crimes that take place via the global network takes place through three stages: [23]

The first stage: collecting information stored by the third-party servers , where computers track the servers from which the criminal entered and try to find any trace of him.

The second stage: Prospective Surveillance stage . There is a hypothesis that the criminal must return or hover around the scene of his crime. There are many ways to monitor these computers, including:

Use monitoring programs that can be downloaded to search for suspicious information and inventory and record login and logout data on the site .

Using what are known as bugs, which are parts placed in the computer to monitor it.

Using cameras to monitor the computer screen is intended for commercial use, and the simplest way to monitor the computer is to enter its location and plant it.

---

[21] Dr. Abdel Fattah Bayoumi Hegazy, Principles of Forensic Evidence and Forgery in Computer and Internet Crimes, .an in-depth study in computer and Internet crimes, Bahjat Printing and Binding, 2009, p. 98

[22] Dr. Muhammad Al-Amin Al-Bishri, Investigation into New Crimes, first edition, Naif Arab University for Security Sciences, .Riyadh, 2004, p. 243

[23] Orin S. Kerr, Digital Evidence and the new criminal procedure, Columbia Law Review, Vol .105:279, 2005, p. 285.

There is another method, which is a little more difficult, which is to plant a computer virus or a Trojan horse-type worm. This method has the advantage that it can monitor more than one device, but the virus must not be allowed to spread, otherwise it will become a target for anti-virus defense programs.

The third stage: seizing the suspected devices and examining them through a forensic technical examination. In this stage, the work of the information expert begins to examine the suspected computer system with its hardware and software components, in an effort to derive physical evidence to be presented to the investigation or ruling body, to determine the extent of the crime occurring using the recognized system .

And practiced in the field of electronic expertise, taking into account the legal rules of the principle of legality.

The US Department of Justice has also developed a practical framework that defines several basic steps for collecting evidence, the information extracted from it, and the locations of this information in various devices and information systems. It also links each set of information to a specific type of cybercrime. For example, this model specifies a list of the usual places where it can be It finds hidden and deleted files, and it also identifies other types of information, such as pictures and passwords, and identifies ID cards such as the social security number, which is useful information in the process of investigating some types of cybercrimes, such as infringement on identities, and publishing scandalous images. Identifying the types of useful information The places where they are hidden are considered a positive step that helps provide reliable legal evidence when bringing the perpetrators to trial before the judiciary.

The electronic expert must coordinate with the criminal investigator before prosecuting the perpetrator for the committed electronic crime, provided that the meeting includes all the experts who contributed with the control or investigation authorities in receiving the report or the procedures for seizure and inspection or examining the programs and collecting forensic evidence, provided that this meeting is limited to The available evidence and its arrangement according to the importance of each piece of evidence or presumption. The criminal investigator must also explain to these experts the legal aspects of the nature of their work, with an emphasis on linking the evidence with scientific expertise to the elements and elements of the crime for which the criminal case is being brought against the accused [24]

It should also be noted that although it is established that the court has discretionary authority regarding the assessment of the expert who comes to it, this does not extend to technical issues, so it is not permissible for it to refute them except with technical evidence that is subject to the absolute discretion of the court of the matter, and therefore the court cannot refute it and reject it. It has only technical supports that may be difficult for it to make its way through except through other technical experience . [25]

Conclusion

The increasing role of scientific proof has obligated the criminal judge, whether an investigating judge or the court, to establish evidence against the accused. It is not permissible for the accused to be tried and convicted merely because there is evidence. Rather, this evidence must be complementary to the rest of the other material evidence, and the procedures for collecting evidence must be characterized by legitimacy. This is out of respect for the personal freedom of the accused, as the accused is considered

(24) Dr. Abdel Fattah Bayoumi Hegazy, Principles of Forensic Evidence and Forgery in Computer and Internet Crimes , an in-depth .study of computer crimes, previous reference, p. 99

(25) Dr. Ali Mahmoud Hamouda, Evidence Obtained from Electronic Means within the Framework of Criminal Evidence Theory, .op. cit., p. 12

innocent until proven guilty by a final judicial ruling, and the general rule in criminal proof is that crimes may be proven by all means, including judicial experience, which is the role played by judicial experts, as judicial experience plays an important role in the process of criminal proof of electronic crimes. The expert's report, with the skills he possesses, makes the criminal judge more convinced, more decisive, and more certain in reaching a just ruling, ensuring that the criminal does not escape punishment, inflicting the punishment he deserves, reducing errors in judicial rulings, getting closer to justice, and arriving at the truth in all its forms. From this we can say Judicial expertise has an important role in criminal proof, and the expert does not replace the judge. On the contrary, the role of the expert is to access digital evidence, thus taking advantage of his expertise in his field of specialization. This makes it easier for the judge to reveal the features of the crime. The judge has absolute freedom to accept the evidence extracted from computers if he is convinced of it and he has the right to do so. To raise it if he finds justifications that require it based on the circumstances and circumstances of the incident in order to ensure that criminals do not escape punishment in electronic crimes and to strengthen the judge's conviction by informing the criminal judge or court of all legal issues by virtue of his knowledge of them and the technical ones through the judicial expert's report in order to reach To reach a fair ruling on the issue at issue

Results:

1. The expert's report, with his experience and skill, makes the criminal judge more convinced, more decisive, and more certain, which helps reduce judicial errors and move closer to justice with greater steps.

2. Scientific evidence requires examination and evaluation, which makes it difficult or even impossible for the judge to examine and evaluate it alone. Therefore, scientific and practical necessity requires the assistance of specialized judicial experts in order to reach the truth in all its forms and manifestations.

3. The expert does not replace the judge in assessing the evidence. On the contrary, the expert facilitates the judge's access to the truth by convincing the judge of the evidence. The judge has complete freedom to accept the expert's report if he is reassured by it, and he has the right to submit it if it becomes clear to him that it does not agree with the circumstances and circumstances of the incident.

4. Practical reality and scientific progress have warned of the existence of new crimes committed daily against others and society by means of electronic calculators and through the Internet, which necessitated confronting them through the use of specialized experts to uncover this new type of crime.

5. The judge does not resort to technical expertise except in the presence of an incident that requires knowledge or interpretation of special knowledge that is not available in it and that is unclear or not proven through documents and documents and that cannot be reached and proven by other means such as testimony, evidence or inspection. Therefore, the technical expert is sought to clarify it and provide advice. The technical requirements needed to decide the case.

6. The expert's report is considered technical evidence. Therefore, assigning experts is one of the procedures for gathering evidence. Delegation of experts must be resorted to during the investigation stage by the competent investigating judge to seek their opinion on some of the technical matters required by the investigation. As for the role of expertise in the trial stage, it helps the judge in Forming his belief to decide the case before him.

7. Practical reality necessitates that expertise be limited to material issues rather than legal issues, which remain within the judge's authority alone, as the judge may not delegate his authority to another person.

8. The practical reality has proven that the judge often bases his judgment on the report of the expert in cybercrimes, and this behavior is logical on the part of the judge, as the judge is the one who appointed the expert, trusted him, and saw that he was suitable for his task, so he must base his judgment on it.

9. Cybercrimes, due to their special nature, require technical expertise to be discovered and revealed. The need for it may appear from the beginning of the investigation phase, and the need for it continues in the investigation and trial phases, as it is of a technical nature.

10. Electronic crime takes place in an environment that has nothing to do with papers or documents, but rather takes place via a computer or the global network, and the process of seizing evidence of this crime can only be achieved with the knowledge of a specialized technical expert.

Recommendations:

1. We recommend the creation of scientific departments in institutes and colleges in order to train judicial experts to prove these crimes, reveal patterns of crimes committed using computers, and develop their skills on a regular and continuous basis.

2. The report prepared by the judicial expert, using his skills, makes the criminal judge more convinced, more decisive, and more certain, which helps to reduce judicial errors, approach justice with broader steps, and reach a greater degree of truth.

3. We stress the need for legislative intervention in the Iraqi Code of Criminal Procedure and the Iraqi Penal Code to address and combat this type of crime.

4. We recommend that the judicial authority, represented by the Supreme Judicial Council, address the emergence of new crimes committed daily against others and society by means of computers and through the Internet, which requires confronting them by preparing judges, investigators, and specialized experts to uncover the perpetrators of this new type of crime.

5. We recommend that the procedures for assigning experts take place at the stage of collecting evidence and that the competent judge is the investigating judge with the powers he has in order to seek the assistance of experts to seek their opinions on some of the matters that were exposed to him during his mission in the investigation, which ends with issuing the decision that there is no basis for filing the case or referring it to the trial court. The expert's report shall be one of the main pieces of evidence in the case.

6. We recommend the need to train justice agencies periodically to keep pace with the rapid development of information technology in order to achieve a balance between the means of committing crime and the means of confronting it.

7. We recommend that the court itself does not replace the judicial expert in a technical matter, otherwise the ruling will be subject to invalidation by issuing it without a specialist and arranging indictment evidence against the accused without taking into account fairness in accessing the evidence of the crime by having the judge replace the expert in a matter that is not considered to be within his jurisdiction.

8. We recommend that the authority of the expert's report be as strong as the official evidence in terms of proof and the main case evidence on which it is based in justifying the ruling.

References

1. Dr.. Ahmed Fathi Sorour, Mediator in the Code of Criminal Procedure, Book One, Dar Al-Nahda Al-Arabiya, Cairo, 2016 edition, pp. 457 et seq.
2. Dr.. Amal Othman, Technical Expertise, Criminal Matters, A Comparative Legal Study, PhD thesis, Faculty of Law, Cairo University, 1964, p. 19.
3. Dr.. Saad Hammad Saleh Al-Qabaili, The right of the accused to seek assistance from a lawyer, a comparative study, Dar Al-Nahda Al-Arabiya, Cairo, 2005, p. 89.
4. Dr.. Abdel Fattah Bayoumi Hegazy, Principles of Criminal Procedure in Computer and Internet Crimes , Dar Al-Kutub Al-Qaniya, Mahalla Al-Kubra, 2007, p. 24.
5. Dr.. Abdel Fattah Bayoumi Hegazy, Principles of Forensic Evidence and Forgery in Computer and Internet Crimes , an in-depth study in computer and Internet crimes, Bahjat Printing and Binding, 2009, p. 98.
6. Dr.. Essam Mahmoud Abdel Halim Youssef, Criminal Liability for People Suffering from Neurological and Psychological Diseases, PhD thesis, Faculty of Law, Cairo University, 2014, p. 374.
7. Dr.. Ali Mahmoud Hamouda, Evidence obtained from electronic means within the framework of the theory of criminal proof, research presented to the first scientific conference on the legal and security aspects of electronic operations, Dubai Police Academy, Research and Studies Center, held from April 26 to 27, 2003, Dubai, United Arab Emirates , p. 6.
8. Dr.. Fawzia Abdel Sattar, Explanation of the Code of Criminal Procedure, Dar Al Nahda Al Arabiya, Cairo, 1986, p. 322.
9. Dr.. Maamoun Muhammad Salama, Criminal Procedures in Egyptian Legislation, Dar Al-Fikr Al-Arabi for Printing and Publishing, Cairo, 2001, p. 645.
10. Dr.. Mamoun Muhammad Salama, previous reference, p. 645.
11. Dr.. Muhammad Al-Amin Al-Bishri, Investigation into New Crimes, first edition, Naif Arab University for Security Sciences, Riyadh, 2004, p. 243.
12. Dr.. Mahmoud Naguib Hosni, Explanation of the Code of Criminal Procedure, third edition, Dar Al-Nahda Al-Arabiya, Cairo, 1996, p. 162.
13. Dr.. Muftah Boubakar Al-Mutradi , paper presented to the Third Conference of Presidents of Supreme Courts in the Arab Countries in the Republic of Sudan, held from September 23 to 25, 2012, p. 32.
14. Dr.. Mamdouh Abdel Hamid Abdel Muttalib, Digital Forensic Research and Investigation into Computer and Internet Crimes, Dar Al-Kutub Al-Qanuni, Egypt, Al-Mahalla Al-Kubra 2006, p. 9.
15. Dr.. Hisham Muhammad Farid Rostom, Procedural Aspects of Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 1998, p. 137 .
16. Dr.. Hilali Abdullah Ahmed, Inspection of Computer Systems and Information Guarantees for the Defendant, a comparative study, Dar Al-Nahda Al-Arabiya, Cairo, 2006, p. 27.
17. Garraud (R.), Traite Theorique et Pratique d'instruction Crime and Procédure Penale , I. Sirez , 1907, n. 317, p. 592. Merle (R.) & Vitu (A.), Traite de droit Penal and criminological , II, 2nd edition ., Dalloz , 1970, n. 1193, p. 1138. Merle (R.) & Vitu (A.), Traite de droit criminelle , problems Generaux de la science criminalelle , Droit penal General 6th edition , 1984, Cujas n. 164, p. 211.
18. Orin S. Kerr, Digital Evidence and the new criminal procedure, Columbia Law Review, Vol . 105:279, 2005 , p. 285.
19. Radel J: The books respectifs juge and technicien _ dans The pre- administration , Colloque institutes _ d'études judiciaires (Poitiers, 26 FebruaryMarch 1975) Publications of the Faculté de droit et de sciences sociales , Poitiers, PUF, Paris, 1976, p.67.