Proving electronic the crime with judicial and technical expertise

debabeche rahmouna

University Hajj Lakhdar, Batna 1.rahmouna.debabeche@univ-batna.dz

Received: 01/06/2024 Accepted: 10/06/2024 Published:30/06/2024

Abstract

Proving cybercrime is a complex process that requires combined efforts between judicial and technical expertise. The role of experts in this field is to collect and analyze digital evidence with high accuracy to ensure reliable information is presented before the courts. The challenges faced by this field, such as the rapid development of technology and legal complexities, require constant preparation and constant updating of knowledge and tools. Through cooperation between judicial and technical authorities at the national and international levels, the effectiveness of combating cybercrime and protecting the rights of individuals and communities can be enhanced. The balance between collecting digital evidence and respecting privacy remains essential to ensuring justice. In the end, judicial and technical expertise are essential pillars for achieving a judicial system capable of meeting the challenges of the digital age efficiently and effectively, which contributes to achieving digital security and justice in society that reflects the due accuracy On the legal level, means of proof, techniques, and developing expertise and competencies in this field

The first axis The importance of using judicial expertise in cybercrime

Expertise is a procedure related to a subject that requires the imam to have technical information in order to extract digital evidence, or it is the technical advice that the investigator or judge uses in the field of proof to help him assess the technical issues whose assessment requires technical or administrative assistance that is not available to the member of the judicial authority who is competent by virtue of his work and culture. (Al Baqi, 1992)

Experience as evidence of proof is the opinion of the expert that he confirms in his report, and since the expert's report is considered technical evidence, the procedure for delegating the expert is one of the procedures for gathering evidence. The investigator may seek the assistance of experts to seek their opinion on some of the matters that were exposed to him while performing his task in the investigation, which ends with issuing a decision that there is no basis. To file a lawsuit or refer it to the subject court, or experience in the trial phase helps the judge in forming his belief to decide the case. (Mohamed, 2007)

An expert is a person who has special knowledge of an issue or a technical specialty. The investigation may be able to examine an issue that requires special scientific or technical competence that is beyond the competence of the investigator or judge through which the expert is consulted, as is the case in autopsies during murder crimes or examining handwriting to detect forgery and more. The importance of judicial experience in criminal proof is to witness the era of scientific and technological development to the extent that it is described as the information age.

Islamic law has established controls and rules in the field of transactions and investigation and management systems that have been characterized by flexibility so that they become valid for every place and time. Islamic law has confirmed the idea of seeking assistance from experience as a type of testimony or consultation,

Because Islamic law permits the assistance of experts in order to determine how to reach the truth. Islamic history has known the so-called expert who evaluates the fruits and crops that are still on the trees or in the ground to know the amount of zakat to be imposed on them. The Prophet, may God bless him and grant him peace, was Abdullah bin Rawaha sends an expert to a Jew to examine the palm trees for them to estimate the size of the roots. (Ali, 2004)

These are diamonds on the path of positive laws throughout the ages

First: The role of technical expertise in proving cybercrime

From this, it can be said that the importance of experience lies in the fact that it is the lamp that illuminates the judiciary's path to justice, especially in the criminal field, and this is what legislation has unanimously agreed upon regarding the use of experience in all laws and courts, whether an expert is appointed at the request of the opponents or the court appoints him on its own initiative, while maintaining that it is not Rejecting the expertise if it was requested by the opponent, this is related to preserving the right of the accused to defend himself, and the fact that appointing an expert is a permissible method of proof. For opponents, it is not permissible to deprive them of benefiting from it and supporting their requests. Therefore, experience has been of such importance in traditional crimes, so how can it not increase its importance, necessity, and even inevitability in proving cybercrime? Experience is a means of proof that aims to uncover some evidence and determine its meaning by using scientific information, which is research into material or material issues. It is an art with which it is difficult for the investigator to make his way through it, and he is unable to collect evidence regarding it through other means of proof Since the emergence of cybercrime, judicial authorities have been staffed with distinguished technical expertise in the field of computers, with the aim of uncovering the ambiguity of the entire crime, or helping to clear up the ambiguities in the delicate electronic operations related to the crime, as the investigation was solved. Therefore, the success of inference and carrying out the investigation in cybercrime depends on efficiency and specialization. These reports are B. It is permissible for the investigator to seek assistance from experts and to waive their oath if there is a fear that he will not be able to hear their testimony later. The importance of seeking assistance from an expert in the field of floating traction appears when he is absent in uncovering a mystery. It or the investigating authority may be unable to collect evidence about the crime, and evidence may be destroyed or erased due to ignorance or negligence. When dealing

Secondly, extracting evidence to prove the electronic crime using technical expertise

The process of obtaining digital evidence is characterized by difficulty and accuracy because it requires great experience and skill in the field of computers. This is due to the diversity and multiplicity of forms and forms of cybercrime, which may be related to attacking information for the purpose of destroying it, or on electronic accounts, or spreading viruses to damage main units, or it may be limited to hacking a password. Especially for a bank or a large institution for the purpose of fraud and obtaining money, and it may be just to prove and demonstrate high ability in the field of computers, and since the process of collecting criminal digital evidence in electronic crimes is one of the most important and difficult matters faced in criminal proof, which led to resorting to an information forensic expert to derive scientific and technical evidence. Criminal Some specialists believe that the process of collecting digital evidence in digital crimes that take place via the World Wide Web takes place in three stages. (Saleh, 2012)

The first stage: information stored by the service provider

The second stage: the monitoring stage. There is an assumption that the criminal must return to the scene of his crime, and there are many ways to monitor computers, including the following: the suspect, recording my data upon entry, and Exit use of computer screen surveillance cameras To monitor

The third stage: tracking and examining it, both technically and forensically. Here, the work of the information expert begins by examining the computer system according to the generally accepted technical rules to determine the guilt or innocence of an accused.

Ensure that the contents of the CD label are identical to what is written on them, while ensuring that the system units are operable and recording the data of the seized component units such as type, model, model and serial number.

Complete the recording of the rest of the unit data by reading the device

Make a copy or identical copies of the original of all the seized storage media, especially the hard disk. Thanks to starting with that, to perform the basic examination process on the copies to protect the assets from loss, damage, or destruction, whether from malicious traps or software bomb traps.

Determine the types and names of software, system programs, application programs, and communications programs

Whether there are programs, files, data, or information of significance related to the subject of the crime, such as pictures of currencies, security tape, and serial numbers in crimes of counterfeiting currency, and documents, signatures, seal prints, and fingerprints in crimes of forgery.

Show hidden files and hidden texts inside images

Convert digital evidence into a physical form This is done by printing the files, photocopying their contents if they are images or texts, or placing them in another container according to the type of data and information that constitutes the evidence from the investigating authorities. There is nothing in the law that obliges him to respond to the accused or to other opponents. The expert investigator determines his mission and the date in which he submits his report. The original is that he proceeds. The expert works in the presence of the investigator and under his supervision. The exception is that this is done in his absence. The opponents have the right to be present while the expert is working. However, it is permissible for the expert to carry out his work in the absence of the opponents and also prevent them from attending if the prevention has a reason. Obtaining documents during the inspection process is considered an easy matter as it is possible to identify them. And by clarifying the role of technical expertise in proving electronic crime, searching for information inside the computer itself is a very complex matter and requires the presence of an expert. The most important issues to be used are It has experience in the field of electronic crimes

the second:

The second axis : requirements for implementing technical expertise to prove cybercrimes

First: Areas of technical expertise in proving electronic crime

1-: Description of computers and their impact. The description of computers and their impact includes the following

The installation of the computers, their make and model, the type of operating system, the importance of the subsystems it uses, in addition to the peripheral devices attached to them, the password or bios, and the encryption system, the possible location of the evidentiary evidence, and the form or form that the investigation will have, economically and financially, on those involved in using the system.

2- Some information and techniques related to computers, including McKayli

Explain how, if necessary, the information system can be isolated without damaging or destroying evidence or causing damage to equipment.

Explaining how, when necessary, it is possible to transfer the evidentiary evidence to appropriate containers without causing it damage. How to embody the evidence in a physical form so as to transfer it, as far as possible, to paper containers that are available to the judge to view and understand, while proving that what is hidden on the paper is identical to what is recorded on the computer, system, network, or magnetic support.

Secondly, the most important requirements for judicial expertise to prove cybercrime

The electronic means and devices that are used in the computer system 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 the investigation and trial authorities to be careful when selecting the expert and the scientific and technical capabilities in the field of the precise specialization of the right that is asked of him to research, and it is not enough. In this case, the expert must obtain a certain academic degree, but he must also have the scientific experience that enables him to acquire high technical competence. Given the technical and scientific nature of the expertise in the field of cybercrime, this experience, which helps in proving cybercrime, can be identified in the following topics:

- Familiarity with computer installation, make, model, main and secondary operating type, devices attached to it, password and code, in addition to proficiency in working with it.

- The expert's ability to master his tasks without resulting in any problems or destruction of the evidence obtained from electronic means.

- Being able to transfer invisible evidence of proof and transform it into readable evidence or maintain its support until the work of the expert is carried out without causing it to be destroyed or destroyed, while proving that the paper outputs of this evidence match what is recorded in its magnetic supports.

Conclusion

One of the first methods of combating cybercrime in inference is to resort to expertise, which, given the specificity of cybercrime, the diversity of its methods, and the multiplicity of its forms, is why international and domestic efforts have focused on embodying a law to prevent this new crime. It has been represented by the efforts of international bodies and organizations to raise people's awareness of the concept of cybercrime, its danger, and the necessity of being careful of it. It is necessary to verify electronic addresses that require passwords on a regular basis, so I worked to form an organization to combat electronic crime with the expertise, means, and equipment to combat it.

However, the most important factor is the difficulty of discovering the crime primarily due to the lack of experience of investigators, which puts us in front of an unequal equation on one side of which is the investigation agencies with their lack of experience in the field of computers and the Internet, and on the other side are occupiers and immoral hackers who enjoy high skills and keep up with everything new in the world of information.

The most important factors contributing to the lack of experience in information crimes are:

- Not allocating specialized training for judges and members of the judicial police in technical fields, which made them inadequate in dealing with them.

Bibliography

– Thunayan Nasser Al Thunayan. Proving electronic crime. Native University of Security Sciences. Riyadh 2012.

– Farghali Abdel Nasser Muhammad and Al-Mismari Muhammad Obaid. Criminal proof with digital evidence from both the legal and technical aspects. The First Arab Conference on Forensic and Forensic Sciences. Naif Arab University for Security Sciences 2007

– Saghir Jamil Abdel Baqi. Criminal Law and Modern Technology. Cairo, Dar Al Nahda Al Arabiya. 1992

–Wasel Muhammad and Al-Hilali Hussein bin Ali. Technical experience. Imam of the Judiciary. Amman, Ministry of Justice. 2004.