Egyptian Journal of Forensic Sciences

ORIGINAL ARTICLE Open Access

Electronic evidence and its authenticity in forensic evidence

Ahmad Fekry Moussa

Abstract

Background: The basis for criminal trials is the judge's conviction of the evidence presented in a case. His belief is based on the context or evidence he is satisfactory with and understands. However, the law may establish certain evidence for the judge to adhere to. This study aims to identify the extent of the authenticity and strength of digital or electronic evidence in criminal trials, by identifying legislative trends in the various legal systems, and examining what legal jurists have done to determine the extent of the authenticity of the electronic evidence of cybercrimes.

Results: This study will research the legitimacy of electronic evidence and the conditions for its verification, the extent of the authenticity of electronic evidence found during an investigation, the difficulties of obtaining electronic evidence that can be presented before the courts, and the extent of a presiding judge's freedom to determine if electronic materials presented in court should be used as evidence.

Conclusions: Two conditions must be met: first, the electronic evidence must be legally obtained based on written permission from the competent investigation authorities; second, it must be verified as valid by computer science and information technology experts. If those two conditions are not met, the evidence is invalid.
The study gives reason to talk about the need for the adoption of international agreements on cooperation in the development and exchange of computer and information technologies, aimed at preserving electronic evidence from destruction and oblige countries to implement and comply with these agreements.

Keywords: Authentic electronic evidence, Computer technology and Internet crimes, Criminal evidence, Criminal judge, Digital evidence, Legitimacy of electronic evidence

Background

Computer and information technology crimes are varied and there are numerous ways to perpetrate them, which makes it difficult for investigators to provide evidence of these crimes. Legal authorities must search for new evidence from crime scenes, especially electronic evidence, and prove its authenticity in the criminal evidence in order to reach the perpetrators of the crime (Biasiotti et al. 2018).

Cybercrimes are among the most serious criminal activity of the present day; they threaten the progress that the world has reached using the Internet in all areas of life, and they weaken confidence in its use as a quick, easy, and safe tool. It can be difficult to prove when a cybercrime is committed, making it difficult for investigators to find evidence through which the crime can be proven and its perpetrators can be convicted. This research looks at the authenticity of forensic electronic evidence in criminal cases (Wu and Zheng 2020).

This research is necessary due to the extent to which laws recognize electronic evidence, especially since these crimes are of a special nature (Shestak et al. 2020). The field of computer forensics is still new, and challenging, and cybercrime requires specialized technical expertise in order to search for evidence (Biasiotti et al. 2018; Welch 1997). It is very difficult for investigators to prove these crimes because the evidence is quickly and easily erased. Delays caused by the authorities' lack of

Correspondence: ahmed.moussa@aau.ac.ae
College of Law, Al Ain University, Abu Dhabi, United Arab Emirates

experience collecting cyber evidence, investigating, and bringing suspects to trial may result in the loss of evidence. Several points must be discussed to define the authenticity of the electronic evidence in the evidence in order to prove the crime was committed.

Modern researches concerning the issues of electronic evidence in forensic science and criminal procedure are devoted to such issues as the preservation of digital evidence and its admissibility in the court (Bilal 1994; Granja and Rafael 2017), legal aspects of electronic evidence and issues relating to legal-technical compliance (Losavio et al. 2019; Schloss 1976), the role of electronic evidence in the detection and investigation of cybercrimes (Matchanov 2020), classification and evaluation of digital forensic tools (Parveen et al. 2020), opportunities and challenges for electronic evidence (Biasiotti et al. 2018), and problems and prospects of legal regulation of issues of obtaining electronic evidences associated with the use of blockchain technologies (Wu and Zheng 2020).

The goals of this research imply to identify and analyze the difficulty of obtaining evidence that proves the perpetration of electronic crimes, as they are of a special nature that requires obtaining evidence from the same environment in which it was committed. This requires addressing and identifying types of electronic evidence, as well as the legitimacy of the electronic evidence, the condition it is in, and the extent of the authenticity of the electronic evidence in proof.

The challenges encountered are the nature of information technology crimes represented in computers and the Internet (Biasiotti et al. 2018), the procedures for proving them (Wu and Zheng 2020), the validity and integrity of the electronic evidence, and the validity of the evidence extracted from the electronic tool in criminal evidence. Electronic crimes have a special nature due to the gravity of their offense, the enormity of their losses, their increasing numbers, and how easy it is to commit them. There is also a problem related to the extent of the judge's discretionary powers in assessing the evidence extracted from electronic means (Losavio et al. 2019; Mason and Seng 2017). The study gives reason to talk about the need for the adoption of international agreements on cooperation in the development and exchange of computer and information technologies, aimed at preserving electronic evidence from destruction and oblige countries to implement and comply with these agreements. In relation to all countries of the world, the development and adoption of legislation regulating the scope of application of electronic evidence should become an urgent response to the emerging challenges in the field of criminal law and forensics, caused by the transition of the world to the digital age. In particular, the relevance of this issue is typical for the UAE, requiring the adoption of a law related to electronic evidence.

Methods

The research is based on the study of international (Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, The Council of Europe Recommendation No. R (95) 13, Appendix, IV. Electronic evidence) and national acts (in particular Egyptian Law No. 175 of 2018, regarding combating information technology crimes, UAE Federal Law No. (35) of 1992 Concerning The Criminal Procedural Law) in the field of regulation of obtaining evidence from information technology systems (United Arab Emirates State 1992). This research uses the descriptive and analytical approach to describe, analyze, and diagnose the subject in its various aspects and dimensions, to realize the extent of the authenticity of electronic evidence in forensic evidence, through acquiring knowledge related to the subject from its public sources and through books and legal literature and across the Internet. This research uses the comparative approach to compare between United Arab Emirates (UAE) legislation and what it has achieved related to cybercrime.

The authenticity of electronic evidence in forensic evidence will be examined in two aspects. The first topic is the definition of the electronic evidence, and its legitimacy. The first requirement is the definition of the electronic evidence. The second requirement focuses on the legitimacy of the electronic evidence, and the conditions for its verification. The second topic is the authenticity of electronic evidence in the evidence arising from the inspection. The first requirement focuses on the difficulties in adopting the electronic evidence arising from the inspection in the courts. The second requirement examines the trends of the UAE's legal systems to validate the authenticity of electronic evidence before the courts.

Results

Evidence has been found to uncover the crime and find its perpetrator, as it is a meaning that is understood through evidence of reality, and this event succeeded in clarifying or determining the condemnation or innocence, and this is realized when using the scientific method, applying logic in estimating these until the meaning derived from its content becomes clear and becomes more accurate in its evidence of conviction or innocence (Matchanov 2020).

Kinds of forensic evidence are many including physical or documentary, or eyewitness testimony (Mason and Seng 2017). Forensic electronic evidence is submitted to prove a crime occurred using a computer and the Internet. This evidence is retrieved using information technology (Losavio et al. 2019).

Electronic crimes are committed in a space that has no use for papers or hard copies, but rather a virtual world related to computer technology and the Internet. This makes it easier for a perpetrator to tamper with data and programs moments after committing a crime, thus obliterating any evidence. This makes it difficult for investigators to collect proof. This research will expose in detail what the electronic evidence is and then examine its legitimacy as proof in a court of law.

Due to the great and rapid development of computer technology and the Internet, new types of crime have emerged. Such crimes are diverse and criminals use various methods to commit them. Then, due to the speed electronic crimes are committed, and the easy erasure of their evidence, it has become difficult to obtain, identify, and classify evidence. This makes it difficult for investigators to prove crimes were committed, and take the accused to trial.

The general rule in criminal cases pending before the courts is that they may be proven by all legally acceptable methods of evidence. This research finds the evidence of cybercrime is different from the evidence for other types of crime. One result of the development in methods for collecting evidence may be impunity of the perpetrators if evidence for the commission is not found (Hammouda 2003).

Obtaining evidence from information technology systems raises many difficulties for investigators for several reasons (Biasiotti et al. 2018). Electronic tools may be used to commit crimes; they are thus evidence of these crimes. Additionally, there is the ease of quickly erasing or manipulating digital evidence. Before the introduction of digital technologies into widespread use, forensic tactics, techniques, and methods were based on previous developments based on the study of the material world. The authorities in charge of the investigation were accustomed to evidence being tangible and perceptible, but the virtual world is different, and the investigator cannot apply traditional evidence procedures to crimes committed in that world. Rather, investigators need specialized technical expertise and training to search for evidence, such as examining hard drives and other electronic tools and systems.

An example that illustrates the difficulties that investigators face when solving cybercrimes is when a computer operator threatens their employer, demanding the company implement several of their demands. When the organization refused to capitulate, the operator committed suicide after deleting all the data on the main device of the institution. The institution tried to recover this data but found it very difficult, and expensive, to retrieve (Hegazy 2001; Rostom 1994, 1997, 2019).

Many researchers have defined electronic evidence or digital evidence as "information acceptable to reason and logic, obtained by legal and scientific procedures by translating the mathematical data stored in computers, its accessories and communication networks, and it can be used in the investigation or trial stage to prove that it has achieved an action or thing or a person connected to a crime, a criminal or a victim" (Al-Bushra 2004).

As defined by the Council of Europe, "electronic evidence" means any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system or network (Council of Europe 2019).

In scientific sources, this definition is considered in a similar way. In a broad sense, electronic evidence is any evidential information stored electronically on any type of electronic device that can be used as evidence in a lawsuit (Casey 2000; Volonino 2003).

Egyptian Law No. 175 of 2018, regarding combating information technology crimes, defines electronic evidence as "any electronic information that has a strength or proven value stored, transmitted, extracted, or acquired from computers, information networks, and the like, and that can be collected and analyzed by using special hardware, software, or technological applications" (Abdel-Muttalib 2006).

Some have defined electronic evidence as "evidence taken from computers in the form of magnetic or electrical fields or pulses that are collected and analyzed by special programs, applications, and technology to be presented in the form of evidence that can be adopted in front of the investigation authorities or before the court. And it has importance to look at the means by which the crime of destruction is committed. Hence, any action that reduces the value of something or completely loses it, and thus the crime of destruction will be realized. The object of the crime of destruction must be something of value and gain the characteristic of money, whether it is movable or real estate" (ILO 2018).

One of the most meaningful definitions of "electronic evidence" was given by the Evidence project, which operates under the auspices of USAID, according to which electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential value that are generated, processed, stored, or transmitted using any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format. This definition is important because it clarifies the various definitions previously proposed and removes as well some of their ambiguities. It takes into account the concreteness of electronic evidence and demonstrates the deep interdisciplinary nature behind this issue. The above definition of electronic evidence has broader applicability than other proposed descriptions, such as by the Standard Working Group

on Digital Evidence or the International Computer Evidence Organization, as it includes both digitally born evidence and that which in the course of its life is transformed and then stored or exchanged in electronic form (Biasiotti et al. 2018).

Electronic evidence is an informative digital component that takes many forms, such as writing, pictures, audio, and photographs, through which the crime, perpetrator, and victim can be linked.

One of the most famous definitions of electronic evidence is "all digital data through which the crime can be proven, or the relationship between the crime and its perpetrator and the victim is proven." Numeric data is a set of numbers from various texts that include writing as well as graphics, maps, audio, and drawing (Casey 2000).

Through the above definitions, electronic evidence can be categorized into several divisions and classifications according to various criteria.

First, electronic evidence can be classified by type (form of electronic data) (Warken 2018). This includes writing such as documents written on a computer, messages written and sent via e-mail, and texts sent by mobile phone. It also includes voice recordings. These can be recorded and stored on a cell phone or on an app. Digital photos are the embodiment of the visual facts of the crime, either as hard copies printed out or stored digitally (Mason and Seng 2017).

Electronic evidence can also be classified according to the method established by the US Department of Justice in 2002: Records created with computer software, known as outputs, such as log files, ATM bills, and mobile phone records, are one such classification. This classification can be defined as classification by method of data creating. Another way to classify evidence is by records saved by plugging data, part of which was created by computer programs and software. This includes securities which contain inputs processed by Excel calculations. Another classification would be records kept on computer, such as written documents, and saved as word processing files. This also includes chat room messages, and saved e-mails (Abdel-Muttalib 2006).

The third way of classifying electronic evidence is according to the purpose for which it was created (classification that can be defined as classification by purpose). According to this standard, the electronic evidence is subdivided into two categories. The first is evidence fit to be means of proof (Ibrahim 2020). This includes records created by the machine automatically outputs, such as phone bills and computer records. It also includes records, part of which has been saved in the machine and processed by software. The second subdivision is evidence not prepared as a means of proof. This type of digital evidence is unintentionally left behind by the perpetrator (Abdul-Muttalib et al. 2003).

Electronic evidence has characteristics that distinguish it from other traditional forensic evidence, and the most prominent are as follows: electronic evidence is scientific (Biasiotti et al. 2018). Scientific evidence is the result of practical experiments using the scientific method. It is used to provide valid data and facts that have been presented for proving or denying crimes, and this requires using high-quality science and data from technicians to make sure that the evidence is correct (Mason and Seng 2017). Therefore, what applies to scientific evidence applies to electronic evidence. Each type of evidence is subjected to a test of its validity. This is an implementation of the rule that the law seeks justice or knowledge aiming at the truth; electronic evidence presented in courts should be based on scientific logic, and its validity should not be in question (Al-Hamdani and Al-Mousawi 2016; Golubtsov 2019).

The use of information systems leaves evidence that includes data sent or received, and every communication made by the communications network. The data on the computer is translated by a system using two numbers, zero and one (Naim 2013). This data is available as digital evidence.

The digital evidence is diverse and is rapidly improving. Electronic evidence varies in form and type and may include raw data, monitoring systems across networks and servers, or electronic documents and digital signatures, or audiovisual recordings or attachments stored in e-mail. The diversity of the electronic guide leads to the breadth of its network. The development of multiple types of digital evidence is characteristic of the virtual world. This diversity has prompted legislators to draft laws to accommodate the various forms of computer output, including electronic evidence.

Information technology includes many types of digital data that can be transmitted electronically. Electronic evidence is a link between that data and the crime, and also a link between the victim and the perpetrator (Losavio et al. 2019). Electronic evidence is analytical. Electronic evidence can monitor important information about the perpetrator and allow forensic specialists to analyze their electronic footprints. It is possible through electronic evidence to know the movements, habits, and electronic behaviors of a perpetrator, as well as a great deal of personal information. Therefore, dealing with electronic evidence in a criminal investigation can be easier than dealing with traditional physical evidence (Mason and Seng 2017). The abovementioned characteristics distinguish electronic evidence from traditional evidence and helped solve crimes committed by computer technology and the Internet.

It is required for forensic evidence to be accepted as evidence if it is obtained legally. Investigators are required to collect evidence according to the policies and

procedures set by law (Rajan et al. 2017). If these policies and procedures are violated during the inspection of computer systems and evidence collection the inspection becomes null and void. It is not permissible to adhere to what is not in the violated inspection record, and the court cannot rely on it in its ruling (Al-Tamimi et al. 2020). There are many legal trends concerning the validity of the electronic evidence. Opinions differ regarding the evidence upon which a judge bases their conviction. These legal trends can be divided into two main schools of thought: the free proof system, and the legal evidence system.

Unrestricted evidence and free proof system gives the judge the freedom to accept the facts presented without requiring them to rely on specific evidence when forming their convictions. They are free to build their convictions on any evidence, even if it was not stipulated. Besides, all evidence is equal for the legislator in the evidence, and the judge determines what they consider to be valid (Hammouda 2003). In the free proof system, there is no problem regarding the legality of the existence of digital evidence, because the existence of the evidence proves its legitimacy.

According to legal evidence system the judge's role is confined to examining the evidence and ensuring that the conditions set by law for the validity of the work are fulfilled (Ahmed 1999).

The law allows a list of evidence for the judge, after determining its value in court. This system is called a restricted evidence system, drawing its culture from the Anglo-Saxon systems. The legal systems of the Anglo-Saxon culture stipulate that electronic evidence cannot be recognized unless the law includes it in the list of evidence. An example of this is the British Evidence Act, which defines the evidentiary value of the digital evidence (Akhihiero 2013). Based on the proceeding facts, questions arise about the legitimacy of obtaining electronic evidence and the conditions for its verification.

Considering the issue of legitimacy of accessing digital evidence, it should be noted that the possibility of obtaining electronic evidence raises several legal challenges due to the special nature of such evidence. The source of the data, and the hardware that can be searched related to collecting evidence that requires the assistance of technical experts in this field, are just some of the challenges that arise when handling digital evidence.

For legitimacy to be obtained in obtaining the digital evidence, there are several formal conditions that must be met, in addition to objective conditions discussed by the court through its delegated experts.

The formal conditions required include the following: the digital evidence must be obtained in a manner consistent with the controls and procedures established by the laws related thereto (Mason and Seng 2017). Additionally, a permit must be obtained from the Public Prosecution, or the authority competent to investigate the inspection, to obtain the evidence required. Finally, the judicial arrest officer should have the technical expertise to facilitate the inspection process and reveal the digital evidence.

One of the most important processes for ensuring the legitimacy of digital evidence is that the authorization for inspection issued for cybercrime must be written, dated, and signed by the representative of the authority competent to issue it. Likewise, it must include notes about the type of crime of which evidence is to be collected, determine the place of inspection, and the time allowed to conduct the inspection. Additionally, the authorization to inspect must be explicit in indicating who is responsible for conducting the inspection (Mason and Seng 2017).

The aforementioned raises another question concerning witnesses. Witnesses called to testify regarding cybercrime are, by virtue of their work, employed in the field of information technology, or in adjacent profession. Care must be taken to ensure such witnesses are competent enough to testify. Should they be tasked with cyber forensic duties they should be trained to handle the evidence responsibly, and according to law, computers which is required to be searched to print data files stored in the computer memory under inspection, which entails the disclosure of the password to open the computer, as well as codes for implementing programs?

There are two schools of thought regarding witnesses. Supporters of the first school, notably one aspect of jurisprudence in the State of France, believe that witnesses are responsible for printing the data files, as well as disclosing passwords and codes for running various programs, except in certain cases where they testify to release themselves from this commitment due to their adherence to respecting the professional secret. This research finds that the judiciary in France accepts the use of modern scientific methods and means in order to obtain forensic evidence for cybercrimes, especially in the field of computer technology and information technology (Le-Khac and Choo 2020).

Supporters of the second school of thought argue that the witness does not have an obligation to print data files stored in the computer, disclose passwords, or reveal codes for implementing programs. In Luxembourg, the witness is not obligated to reveal everything they know when asked before a court (Ligeti and Robinson 2017).

Special attention should be given to the questions of definition of electronic evidence. A judge must, when viewing the electronic evidence extracted from the computer and the Internet, make sure that it is correct and unquestionable. Valid evidence ensures a judge can rely

on it to preside over a case. The presumption of innocence until a guilt is proven based on evidence accepted by a judge means that judges have the responsibility to ensure all evidence presented in a trail is high quality and valid.

To ensure that, judges are required to seek the assistance of technical experts in the fields of computer technology, and information technology. These technical experts should present and explain electronic evidence gathered from computers, and the judge should examine electronic outputs to determine the evidentiary power to reach the perpetrator of the crime and determine their guilt (Tawalbeh 2019).

In the USA, research finds that some state laws have a stipulation that copies of data extracted from a computer are one of the best evidence, and the certainty of this evidence is verified. Federal rules also state that "it is a prerequisite for documentation or verification of the validity of the evidence, as a precondition for acceptance, that it meets sufficient evidence to support the discovery of matters related to the matter in support of the claims claimed by the plaintiff" (Hassan 1999). In Britain, the Police and Evidence Act of 1984 stipulates that in order for the electronic evidence to be certain, the data must be accurate and properly issued by the computer (Bevan and Lidstone 1985; Mason and Seng 2017).

Discussing digital evidence produced by the computer and the Internet, it should be noted that it is the responsibility of a criminal judge to establish their evidentiary convictions by discussing the forensic evidence in the trial sessions with the parties of the lawsuit. A judge must discuss the digital evidence obtained from sources such as publications, data, audio files, or photographs, and hear the statements of witnesses who were previously heard in the preliminary investigation.

Inspection is a primary investigation procedure; it affects the personal freedom of citizens accused of crimes. Its purpose is to reveal facts related to felonies or misdemeanors. Regarding electronic crime, research shows that the lack of specialized information about these crimes is still the biggest challenge for criminal investigations (Matchanov 2020).

Research finds that investigations frequently focus on the place of employment of the accused, their home, or the homes of family and friends. Permission for a search must be specified in the inspection permit, which must include the location to be searched. The inspection process in the electronic system may produce evidence related to the crime, such as magnetic tapes, information stored inside the computer, and optical discs.

Part of the criminal jurisprudence holds that if the purpose of an inspection is to seize material evidence that is useful for the detection of the crime, then it extends to include electronic data in its various forms (Le-Khac and Choo 2020). This research will discuss the verification of authenticity of forensic electronic evidence.

Turning to the issue of difficulties in adopting electronic evidence in the courts, first, one should keep in mind that there is no doubt that data or information suitable to be electronic evidence can be tampered with and erased before it reaches the hand of justice. Search and seizure does not take place without the knowledge of technical experts or specialists. This is because security authorities, investigators, and trial agencies do not have sufficient knowledge of information technology in the field of cybercrime, which makes it difficult to control and find electronic evidence (Matchanov 2020).

The strength of the inferential authenticity of the outputs obtained from computer and information technology lies in the truthfulness of the attribution of the act to a specific person or its lie, or the value of the output generated from the computer in its multiple forms of electronic or paper outputs or movie thumbnails (Le-Khac and Choo 2020).

Specialists may encounter, when gathering evidence and after confirming its legitimacy, and the legitimacy of the procedure of obtaining it, other difficulties. These challenges are largely due to the technical nature of the electronic data, and from interference with the evidence. Non-specialists do not always have the ability to detect tampering, which affects the validity of the electronic data to the degree of certainty, and its adoption as forensic evidence in establishing the facts and reaching a conviction or innocence. Among the most prominent of these difficulties are the following:

Difficulties regarding the validity of digital evidence allowed before the courts are numerous. First, digital evidence can be manipulated to hide the truth, so it does not reflect the reality of the crime being investigated. This manipulation may affect in all other digital evidence presented before the judiciary, and it weakens its authenticity and taking it with certainty. The possibility of technical errors while obtaining the digital evidence is very rare, but it weakens the perception of the authenticity of the digital evidence. This is due to several reasons (Mason and Seng 2017). Making decisions using evidence whose validity is less than that usually required calls into question the validity of a court decision. Another difficulty that can arise is the use of an inappropriate tool for accessing digital evidence due to the reason for using the wrong specifications and the inconsistency of the code used.

Because of the difficulty of extracting digital evidence in such crimes, specialists in computer technology and information technology see that cybercrimes constitute a major challenge for computer forensic specialists (Biasiotti et al. 2018).

There is a belief that control and audit bodies in both the private and public sectors will lead to the disclosure of evidence, how the crime occurred, and the identification of the suspect (Le-Khac and Choo 2020).

It should be noted that the suspicion of electronic evidence is not related to it as evidence, but rather to other factors. The credibility of electronic evidence is diminished or supported depending or whether or not it can be verified, including computer science, which provides technical information to understand the content of the evidence and how to extract it (Abdel-Muttalib 2006).

Computer scientists and information technology specialists have an important role in detecting manipulation of digital evidence, by comparing the digital evidence presented to the judiciary with the original, uncorrupted data.

There is a type of electronic evidence called the neutral evidence, which is separate from the subject of the crime. It helps ensure the integrity of digital evidence by preventing any changes or modifications by the addition or removal of data (Abdel-Muttalib 2006).

Discussion

The difficulties raised about the extent of the authenticity of digital evidence presented in court cases, and the attempt to develop solutions to them, resulted in a procedure approved by law. The procedure is "before digital evidence is allowed as criminal evidence before the courts, technicians, specialists in computer technology and information technology, should verify its authenticity and its relation to the crime under trial."

Courts ruled based on facts proven by digital evidence, while considering it distinct from other types of evidence (Al-Bushra 2005). This is supported by some jurists referencing the necessity of help from specialists in computer technology and information technology when investigating electronic crimes. Highly trained computer forensic specialists are needed to reveal the perpetrators, obtain evidence, and explain it before the criminal courts entrusted with adjudication (Mason and Seng 2017).

Computer science specialists provide assistance by obtaining copies of the original evidence, and also by using scientific methods to procure electronic evidence that has not been manipulated. They make it more difficult to destroy digital forensic evidence by manipulating or erasing it.

Despite the lack of legislation in some countries and their lack of local and formal procedures regarding information technology and computer science crimes, the courts of other nations have not faced difficulties dealing with digital forensic evidence. This is largely due to the efficiency of computer systems and modern technology, and the ability to link digital forensic evidence and its effects to the crime pending before the court. The clarity of electronic evidence and its accuracy in establishing the relationship between the accused and the crime, and access to sources of digital evidence by tracking its effects, have also benefited other nations.

Legal systems overseas differ in their trends regarding the authenticity of digital evidence. This includes systems that adopted the principle of freedom of proof, such as the nation of France and many Arab countries like Egypt, Syria, and Lebanon. A judge presiding over a criminal case is given the freedom to estimate the evidence presented to him. This gives that judge the freedom to gauge evidence for computer technology and information technology.

That is what jurisprudence and statutory legal systems adopting the principle of freedom of proof do; they gave the presiding judge wide authority to assess evidence after confirming its validity and relevance to the case. The judge has the authority and capacity to consider digital evidence and ensure its authenticity (Mason and Seng 2017).

Jurisprudence in France considers that the validity of electronic evidence is not contrary to the law as the presiding judge is free to decide if this evidence should be presented in court (Meissonnier and Banat-Berger 2015).

Likewise, in Germany, Luxembourg, and Greece, judges are free to allow electronic evidence to be presented. This allows judges to decide when the digital evidence does not agree with the circumstances of the crime (European Judicial Network 2020; Insa 2007).

Courts are in dire need of computer science and information technology experts in the age of new, technologically advanced crimes. These experts will help investigators convict criminals by reviewing and implementing systems for processing data and programs. The competence and efficiency of such experts will help investigators access and organize electronic evidence (ILO 2018).

Egyptian Law Number 175 of 2018, passed to combat information technology crime, gave authority to judicial authorities to issue an order to search computer programs, databases, and other information devices and systems, to uncover evidence.

The UAE has adopted the principle of freedom of proof by giving judges freedom to gauge the evidence presented in terms of inference to find the accused. This is evident in Federal Penal Procedures Law Number 35 of 1992, which includes in its Articles expressions with the characteristic of publicity. Article 51 stipulates, "… the accused is searched for any effects or things related to the crime that are on their body, clothes, or baggage, or that are necessary to investigate it" (Antti 1994).

This Article clarifies the powers of the judicial arrest officer regarding the inspection process. This is especially true of the terms "baggage" and "things." These

terms are now understood to include digital evidence obtained from electronic crime scenes.

In restricted law systems, the Legislature frequently determines, in advance, the evidence and its persuasive value that the judge uses to try the accused. Among these systems is the British legal system, which issued in 1990 the Computer Misuse Act. This Act does not concern evidence resulting from computers and the Internet, leaving policy and procedure of such evidence to the Police and Criminal Evidence Law of 1984. The 1984 Act included a precise procedure of organizing outputs produced from the computer and the Internet, to process evidence (Hassan 1999).

In the USA, the State of California issued the Evidence Act in 1983, which included the acceptance of extracted copies of data contained in a computer, as the best available evidence to prove information and data (Csonka 1996). This is stipulated by the federal rules of proof by accepting copies of data that are identical to the original and adopting it as evidence without specifying a specific method for copying it. This is legal whether the copying was done by printing, photocopying, or recording electronically. The American judiciary system can rely on the evidence extracted from the computer's retained records (Hassan 1999).

In the State of Canada, Article 29 of the Canadian Evidence Act includes conditions for accepting computer-generated records that must be met before the copying process (Duranti et al. 2010). A judgment was issued by the Canadian Court of Appeal of Ontario on the occasion of an incident called the McMillan case, which includes a requirement that for computer records to be accepted as evidence of proof, as real copies of electronic records that they contain a full description of the system of record-keeping prevailing in financial institutions, which may include a description of the procedures and processes related to data entry, storing and retrieving it to ensure that the output obtained from the computer is certain (Ahmed 1999).

Studies find that the matter differs slightly in laws with a mixed direction, where the law determines in advance whether or not certain evidence is suitable to prove some facts. Sometimes, the law sets conditions for its acceptance of evidence; however, in other circumstances, a judge may be allowed to assess the material for its validity as evidence. An example of the former is the Japanese Legislature restricting acceptable evidence to the statements of the accused, witnesses, physical evidence, and testimony from subject matter experts.

Japanese jurists state that evidence derived from digital sources cannot be used to prove crimes before the courts unless they are converted into physical evidence, whether as an original, or a copy identical to the original. The reason for this is that the information and data resulting from computer technology and the Internet are invisible electronic pulses that flow through computer networks and may be encrypted. This makes it easier for criminals to obscure the evidence of the crime, making it difficult to convict them (Ahmed 1999).

This research aimed to define electronic evidence, the extent of the authenticity of electronic evidence in solving cybercrimes to the satisfaction of the courts, as well as to identify important legislation that addresses this type of forensic evidence. This study proves there are many challenges the courts face when accessing this kind of evidence. However, there is a great deal that has been learned that will help guide future research.

Evidence is considered the basis of the investigation work, and it starts from the occurrence of the crime until the end of the trial. The prosecution must transfer the case files to the presiding judge, including any legal evidence and documents indicating the incident at hand. Digital evidence is related to computer technology and the Internet, and the methods of collecting or extracting it are different from those of physical evidence. The programs, data, and information circulating over networks, or stored on computers, can be considered digital evidence. This evidence has a system of protection on the network where it originated, and it can be damaged via manipulation. That damage threatens the validity of the evidence.

Forensic evidence has an effective role in establishing objective law. It particularly affects the development of processes and procedures for gathering electronic evidence. This gives it special importance in solving cases of cybercrime, and convicting the guilty party. Electronic evidence is accepted as legal evidence when its conditions are met in most comparative legal rulings and laws, even with the malfunctions of their jurisprudential trends in establishing their acceptance of such evidence in a court of law.

Having access to experts in computer science and information technology helps investigators control cybercrime and access evidence that can be used as proof.

Conclusion

The study leads to the conclusion about the need for the adoption of international agreements on cooperation on the development and sharing of computer and information technology designed to preserve electronic evidence from destruction and vandalism, and obligate countries to implement and abide by these agreements. Sanctions should be imposed on countries that are not committed to aid-related agreements to control cybercrime and collecting related evidence. These countries should also be deprived of access to new developments in computer science and information technology. Such cooperation must be by international agreement.

Training and qualification of those responsible for investigating crime related to computer and information technology must be developed by preparing continuous training programs in that field. The training should focus on the technological aspects of electronic crime, thus allowing law and order professionals to find the perpetrators of cybercrime, and obtain evidence to convict them.

As the research shows, the adoption of legislation regulating the scope of application of electronic evidence is an urgent response to the emerging challenges in the field of criminal law and forensics, caused by the transition of the world to the digital age. In particular, the relevance of this issue is typical for the UAE, requiring the adoption of a law related to electronic evidence, which should include a definition of tools for extracting electronic evidence. It should also identify the authorities responsible for this jurisdiction, and specify the controls and conditions necessary to obtain electronic evidence.

Legislators in the United Arab Emirates must amend the UAE criminal procedures law and other legislation to comply with the development of electronic crime. The law should provide legal support obtaining electronic evidence of these crimes and tracking their perpetrators. It should also outline clear legal mechanisms to process with electronic evidence in the stages of tracking and prosecution, inspecting information technology systems, and controlling electronic devices.

Abbreviations

UAE: United Arab Emirates; USAID: United States Agency for International Development; ATM: Automatic Transaction Machine

Acknowledgements

Not applicable.

Author's contributions

Ahmad Fekry Moussa is the single author and the only one responsible for the content of the article. The author read and approved the final manuscript.

Funding

The research has no funding.

Availability of data and materials

Data will be available on request.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The research has no conflict of interests.

Received: 3 June 2021 Accepted: 19 August 2021
Published online: 27 August 2021

References

Abdel-Muttalib MAM (2006) Search and criminal investigation in the digital computer and Internet crimes. National Library.

Abdul-Muttalib MAH, Qasim ZM, Aziz AA (2003) A proposed model for the rules for adopting the digital evidence for evidence in computer crimes. Arab J 5: 2253–2238

Ahmed HAI (1999) Authoritative computer outputs in criminal matters: a comparative study. National Library.

Akhihiero HJP (2013) Admissibility of electronic evidence in criminal trials. How practicable? In: Being a paper presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State, from 23rd of July, p 1-29. http://nigerianlawguru.com/articles/practice%20and%20procedure/ADMISSIBILITY%20OF%20ELECTRONIC%20EVIDENCE%20IN%20CRIMINAL%20TRIALS.pdf. Accessed 15 Apr 2021

Al-Bushra MAA (2004) Investigating the new crimes. Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

Al-Bushra MAA (2005) Digital forensic evidence, its concept and its role in evidence. Arab J Secur Stud Train 1:112

Al-Hamdani MK, Al-Mousawi AMK (2016) The digital evidence and its relation to infringing the right to information privacy while proving crime. Al-Nahrain University, Baghdad, Irak.

Al-Tamimi KHSS, Marni NB, Shehab AA (2020) Evidence in cybercrimes: a comparative study between Islamic law and UAE legislations. J Crit Rev 7(14): 2778–2781

Antti A (1994) International review of penal law – Computer crime and other crimes against information technology. Comput Law Secur Rev 10(1):34

Bevan N, Lidstone K (1985). A guide to the police and criminal evidence act 1984. Bulterworthe.

Biasiotti MA, Cannataci JA, Bonnici JPM, Turchi F (2018) Introduction: opportunities and challenges for electronic evidence. In: Handling and exchanging electronic evidence across Europe. Springer, Cham, Switzerland, pp 3–12.

Bilal AA (1994) The evidence base obtained illegally in comparative criminal procedures. Dar Al-Nahda Al-Arabiya.

Casey E (2000) Digital evidence and computer crime: forensic science, computers and the Internet. Academic Press, Cambridge, USA.

Council of Europe (2019) Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c. Accessed 15 Apr 2021

Csonka P (1996) Council of Europe activities related to information technology, data protection and computer crime. Inf Commun Technol Law 5(3):177–196. https://doi.org/10.1080/13600834.1996.9965744

Duranti L, Rogers CM, Sheppard AF (2010) Electronic records and the law of evidence in Canada: the uniform electronic evidence act twelve years later. Archivaria 70:95

European Judicial Network (2020) Transnational access to electronic evidence for criminal cases: trends and latest developments within the EU and beyond. https://www.ejn-crimjust.europa.eu/ejn/NewsDetail/EN/727. Accessed 15 Apr 2021

Golubtsov VG (2019) Electronic evidence in the context of e-justice. Civil Procedure Bull 9(1):170–188. https://doi.org/10.24031/2226-0781-2019-9-1-170-188

Granja FM, Rafael GDR (2017) The preservation of digital evidence and its admissibility in the court. Int J Electron Secur Digit Forensics 9(1):1–18. https://doi.org/10.1504/IJESDF.2017.081749

Hammouda AMA (2003) Evidence obtained from electronic means within the framework of criminal evidence theory, the first scientific conference on legal and security aspects of electronic operations. Dubai Police Academy, Research and Studies Center, Dubai, UAE.

Hassan SAL (1999) Proving computer crimes and crimes committed via the Internet. Dar Al-Nahda Al-Arabiya.

Hegazy AFB (2001) Forensic evidence and forgery in computer and internet crimes. El-Mahalla El-Kobra.

Ibrahim KM (2020) The electronic evidence in cybercrime from the website. National Library.

ILO (2018) Egyptian Law to Combat Information Technology Crimes No. 175, EGY-2018-L-108464. http://ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=108464&p_country=EGY&p_count=499. Accessed 15 Apr 2021
Insa F (2007) The admissibility of electronic evidence in court (AEEC): fighting against high-tech crime – results of a European study. J Digit Forensic Pract 1(4):285–289. https://doi.org/10.1080/15567280701418049
Le-Khac NA, Choo KKR (2020) Cyber and digital forensic investigations. Springer International Publishing, New York, USA. https://doi.org/10.1007/978-3-030-47131-6
Ligeti K, Robinson G (2017) The handling of digital evidence in Luxembourg. In: Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations. Wolters Kluwe, pp 123–162
Losavio MM, Pastukov P, Polyakova S, Zhang X, Chow KP, Koltay A, James J, Ortiz ME (2019) The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdiscip Rev Forensic Sci 1(5):e1337
Mason S, Seng D (2017) Electronic evidence. University of London Press. https://doi.org/10.14296/517.9781911507079
Matchanov A (2020) On the specific features of disclosure and investigation of cybercrimes. Soc Innov 1(1):155–165
Meissonnier A, Banat-Berger F (2015) French legal framework of digital evidence. Rec Manag J 25(1):96–106. https://doi.org/10.1108/RMJ-07-2014-0031
Naim S (2013) Research and investigation mechanisms for information crime in Algerian law. Master Thesis
Parveen A, Khan ZH, Ahmad SN (2020) Classification and evaluation of digital forensic tools. Telkomnika 18(6):3096–3106. https://doi.org/10.12928/telkomnika.v18i6.15295
Rajan AV, Ravikumar R, Al Shaer M (2017) UAE cybercrime law and cybercrimes – an analysis. In: 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, p 1-6.
Rostom HMF (1994) Procedural aspects of information crime: a comparative study of the modern machine library. Asyut University
Rostom HMF (1997) Computer crimes as a form of the new economic crimes. J Leg Stud 17:117
Rostom HMF (2019) Information crime - fundamentals of the technical criminal investigation and a proposal to establish a unified Arab mechanism for specialized training. In: Law, Computer and Internet Conference, United Arab Emirates University, Dubai, United Arab Emirates, pp. 1–7.
Schloss JD (1976) Evidence and its legal aspects. Merrell Publishers, London, UK.
Shestak V, Gura D, Khudyakova N, Shaikh ZA, Bokov Y (2020) Chatbot design issues: building intelligence with the Cartesian paradigm. Evol Intell:1–9
Tawalbeh AH (2019) The legality of the electronic evidence derived from the Criminal Inspection. Faculty of Law Forum, Mansoura University, Dakahlia, Egypt.
United Arab Emirates State (1992) United Arab Emirates Federal Criminal Procedures Law Number 35 of 1992. https://legaladviceme.com/legislation/156/uae-federal-law-35-of-1992-concerning-criminal-procedural-law#:~:text=Every%20person%2C%20accused%20of%20a,services%20as%20specified%20by%20law. Accessed 15 Apr 2021
Volonino L (2003) Electronic evidence and computer forensics. Commun Assoc Inf Syst 12(1):27 https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3193&context=cais
Warken C (2018) Classification of electronic data for criminal law purposes, vol 4. Eucrim: the European Criminal Law Associations' fórum, Freiburg, Germany, p. 3.
Welch T (1997) Computer crime investigation and computer forensics. Inf Syst Secur 6(2):56–80. https://doi.org/10.1080/10658989709342536
Wu H, Zheng G (2020) Electronic evidence in the blockchain era: new rules on authenticity and integrity. Comput Law Secur Rev 36:105401. https://doi.org/10.1016/j.clsr.2020.105401

Publisher's Note