How to Cite:
Al-Tamimi, K. H. S. S., Marni, N. B., & Shehab, A. (2022). Legal regulation of evidence in cybercrimes in UAE legislations. *International Journal of Health Sciences*, *6*(S1), 765-776. https://doi.org/10.53730/ijhs.v6nS1.4827

Legal Regulation of Evidence in Cybercrimes in UAE Legislations

Khalifa Hamed Saleh Shabal Al-Tamimi
Academy of Islamic Civilization, Faculty of Social Sciences and Humanities, UTM, Malaysia

Nurazmallail Bin Marni
Academy of Islamic Civilization, Faculty of Social Sciences and Humanities, UTM, Malaysia

Ahmed Shehab
Faculty of Sharia & Law, Islamic University of Gaza, Palestine

***Abstract*---**The study aims mainly to evaluate the legal regulation of evidence in cybercrime in the United Arab Emirates compared to the provisions of Islamic laws by explaining the concept of cybercrime, its types, elements, and ways to confront it. The study will examine the legal and judicial framework to combat cybercrime in the United Arab Emirates, and define the means, conditions, the evidentiary requirements of cybercrime in Islamic law and UAE legislation. The researcher has used the descriptive-analytical method in his research. The study concludes with several results. The most important of which is that cybercrime differs from its traditional counterpart in nature and methods of gathering evidence to prove it. The study also concludes that there are difficulties in proving electronic evidence, in addition to the fact that the UAE legislator did not provide for means of evidence for cybercrimes. The study also concludes with several recommendations. There is also a need to enact legislation that compels technical companies and social media platforms to ask users and customers to provide personal documents that prove their identities when registering on any platform on the Internet, these documents will serve as an "electronic fingerprint".

***Keywords*---**cybercrime, electronic fingerprint, evidence, legal regulation, UAE legislation.

International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696X © 2022.
***Corresponding author**: Al-Tamimi, K. H. S. S.; Email: uae.utm.students@hotmail.com*
Manuscript submitted: 27 Nov 2021, Manuscript revised: 18 Feb 2022, Accepted for publication: 09 March 2022

Introduction

Crimes have been evolving since long ago, and the forms and types of these crimes have begun to increase and multiply. There is no doubt that the protection of public interests and private interests in the state is one of the most important aspects contributing to the improvement, development, and preservation of societal security of countries. Moreover, the functions and roles of states have been expanding and developing. Nowadays, the functions and roles of the modern state are different from its functions and role in the past. The modern state is no longer limited to preserving public order. Indeed, the roles and functions of the state have changed in many different ways according to the requirements of our age.

The emergence of electronic crimes as a result of the tremendous technological and technical progress, the emergence of cyberspace and modern means of communication such as fax, the Internet, and other forms of electronic communication via satellites have enabled cybercriminals to exploit this scientific revolution in the implementation of their crimes that are no longer limited to the territory of one country but have exceeded the borders of countries. These crimes are innovative, novel, and highly intelligent so much so governments have not been able to include them within the traditional criminal descriptions in national and foreign criminal laws.

Besides, the procedural prosecution systems have also failed to absorb this new criminal phenomenon, whether at the level of criminal prosecution within the framework of national laws or the level of international criminal prosecution. This has necessitated the development of the national criminal legislative structure with the same level of intelligence of these crimes. This legislative structure is characterized by legal accuracy and the ability to keep in pace with the dimensions of these new technologies in a way that guarantees respect for the principle of the legality of crimes and penalties on the one hand, and the principle of procedural legality on the other hand. The objectives of this legislative structure have to correspond with the objectives of the national treaties (Al-Matradi, 2012).

Islamic Sharia has been a forerunner in achieving the interests of people in this world and the hereafter by establishing a righteous society that worships Allah, populates the earth, and uses the elements of the universe in building a human civilization in which every human being lives in an environment of justice, security and peace while fully fulfilling his/her spiritual and material requirements and not neglecting any element of their personality, spirit, mind, and body. Islamic Sharia prohibits harming people and society. Those who read biographies about the life of the Prophet Muhammad, the lives of his Companions, the lives of Caliphs, and Islamic history will find hundreds of evidences of the Muslim ruler's keenness to preserve the money, lives, and honor of Muslims. This indicates the commitment of Islamic law to protecting the Muslim community from crimes and their consequences.

The United Arab Emirates is one of the Arab and Islamic countries whose legislation is based on the Islamic law given the development, multiplicity, and diversity of Emirati legislation in the last quarter of the twentieth century,

especially the criminal legislation including a set of deterrent provisions aimed at enhancing levels of protection for public and private interests. The Emirati legislator has not only enacted a set of laws on combating information technology crimes to preserve the rights and interests of the people but the UAE has also established a department known as the General Administration of Criminal Investigations and Intelligence. It has also worked on training specialized cadres and technical agencies to enhance protection from electronic crimes. It has also organized many conferences and workshops related to combating cybercrime.

In this study, we review the authenticity of evidence of the cybercrimes compared to the authenticity of evidence regulated under the provisions of Islamic law. We have developed a sequential methodology. First, we have explained what cybercrime is in terms of concept, types, subject matter, and nature of those crimes. Second, we have reviewed the forms of cybercrime and proceeded with the examination of the evidence of cybercrimes in terms of their nature and characteristics. Third, we have discussed the position of the Emirati legislator on cybercrimes and the most important obstacles preventing the capture of the perpetrators. Finally, we have concluded with a set of findings and recommendations

Literature review

Literature review is considered one of the most important pillars of scientific research in its theoretical framework. The importance of Literature Review in our study is that it helps in an in-depth understanding of the aspects of the subject matter by clarifying what cybercrime is. They also contribute to identifying the authenticity of evidence of cybercrimes. Also, Previous studies contribute to the subject of our study by providing a set of information helping in achieving the desired goals. This study differs from previous studies related to the subject of cybercrime in that it is the first study related to the topic of the authenticity of evidence in cybercrime in the United Arab Emirates. Here we review the most important previous studies related to the subject of our study:

- Abdul-Baqi Ahmed (2018), entitled: " The Authenticity of Modern Scientific Methods in Evidence from the Perspective of Sudanese Legislations". The researcher's goal, through his study, is to identify the concept of modern scientific methods, their importance, their sufficiency, and their validity in evidence.
- Mukhtari (2017), In his study entitled "Evidence in Cyber Crime" reviews the legal nature of evidence in cybercrime. The study reviews the various jurisprudential perspectives that have discussed the issue of evidence in cybercrime and the implications thereof.
- Al Thanayan (2012), in his study titled "Evidence of Electronic Crime" has tried to answer the following question: How can cybercrimes be proven? The researcher has used the inductive documentary analytical approach in his study.
- The most important finding of the study are: the nature of cybercrime generally requires unconventional methods of investigation to discover digital evidence and to prove it by specialized technicians since cybercrimes are difficult to detect. The investigation methods for proving cybercrimes

require some special procedures while taking into account the location of its occurrence

- Al-Hudairi (2016), explains in his study titled: "Forensic Evidence by Modern Scientific Methods" that his study aims to clarify the legality of criminal evidence through modern scientific methods in Libyan criminal law and contemporary jurisprudence and to clarify aspects of agreement and differences between them. The researcher uses the descriptive-analytical approach and the comparative approach for comparison between Libyan law and Islamic law in his study.

General provisions for cybercrimes

In this part of the study, we review the concept of Cybercrime, its types, characteristics, and natures.

The concept of cybercrime

There are many opinions regarding the definition of cybercrime, and each team of scholars has adopted its definition based on its perspective. Some scholars of jurisprudence have defined it from a technical and legal perspective, and there are some scholars of jurisprudence who have defined it based on the means of committing it, its types, or based on the extent to which the perpetrator of the crime possesses technical knowledge or based on other criteria (Hegazy, 2016). This is what prompted the United Nations not to reach an internationally agreed definition in its "code of information crime". However, despite the difficulty of establishing a single and specific definition of cybercrime, the Technology Evaluation Office in the United States of America has defined it based on computers as " crimes in which computer data and information programs play a major role ". Cybercrime has also been defined as "criminal activity constituting an assault on computer programs and data". Others have defined it as "every unlawful use of information technology, in the form of an act or omission, aimed at attacking any legitimate interest, whether material or moral" (Al-Mutradi, 2012). Based on the previous definitions, we can define cybercrime as unlawful acts that the computer is the subject of or a mean to commit it.

Types of cybercrime

Jurisprudence scholars have divided cybercrime into four types according to the definition adopted by each of them as follows:

- Computer Crimes: It refers to acts that constitute an assault on computers, whether on its physical components such as input and output units, flexible and solid storage devices or the monitor and printer or its intangible components such as data and information stored in the computer. Therefore, computer crimes differ according to the nature of the targets of the assault. The assault sometimes occurs on hard computer components, and other times occurs on programs and information inside the computer. In both cases, the computer and its contents are the targets of criminal behavior.

- Website-related crimes: It is every unlawful act that occurs on websites to disrupt, distort, or modify them. These crimes also include attempts to gain illegal access to unauthorized databases, use of false addresses to enter the information network, break into networks and transmit viruses, and send messages of all kinds via e-mail to compromise the dignity of the targeted persons or promote illegal materials or actions.
- Network-related crimes: It is every unlawful act that occurs on a document or text on the network, for example, the violation of intellectual, artistic, literary, and scientific property. Committing these crimes via the information network requires an internet connection and the use of computers to access and tamper with databases
- Computer-related crimes: These are crimes that the computer is a mean to commit such as fraud and forgery. This crime was classified as a computer crime, as the term computer crime was used to denote all forms of computer crime, whether the computer was an explicit target or a mean of a criminal act. However, after the expansion of computer crimes and the emergence of cybercrimes, the term computer-related crimes has come to refer to crimes that the computer is a mean to commit, meaning that it is every unlawful act that uses the computer as the main tool in the commission of the crime (Al-Oujali, 2016).

The targets of cybercrimes

The targets of cybercrime vary according to which side they are viewed. On the one hand, the computer or the information stored inside it may be the target of the crime, and on the other hand, the computer may be a tool for electronic crime and a means to carry out this crime. This calls for clarification as follows:

- The case in which the computer or the information stored in it is the target of electronic crime: In this case, there are two forms of assault. The first form is the assault on the physical components of the computer itself, such as devices and equipment, which is represented in the crimes of theft or destruction of the computer monitor or its private communications network or the printing machine (Hilali, 2007). On the other hand, the assault may be directed at non-physical computer components such as data and programs, such as crimes of assault on data stored in the computer's memory or data transferred over various communication networks, which is represented in the crimes of theft, destruction, imitation, erasure or disruption of this data. The second form of assault is directed at computer programs through forging electronic extracts and divulging their contents, this is called “cyber-capacity”.
- The case in which the computer is a tool for committing a crime: In this case, the perpetrator uses the computer to commit crimes of theft, swindling, breach of trust, or forgery of documents by manipulating the computer, as well as the information system in general. In this case, we are dealing with purely traditional crimes (Hassouneh, 1993).

Characteristics of cybercrime

Cybercrime differs from other crimes in several aspects:

- The perpetrator of cybercrime is most likely an extremely intelligent, sophisticated person with high technical skills. Moreover, the perpetrator of the electronic crime is an expert in computer systems, how to operate them, and how to store information and obtain it, while the perpetrator of the traditional crime is an illiterate person with a simple, average education.
- The perpetrator of cybercrime is often socially adapted and financially capable, whose motivation to commit his crime is the desire to conquer the system more than the desire to obtain a profit or material benefit (Al-Arian, 2004). On the other hand, the perpetrator of the traditional crime is often socially maladaptive, and his motivation for committing the crime is a quick financial benefit. Cybercrime targets the field of intangible electronic information. It is, therefore, less violent and more difficult to prove because the perpetrator who committed this crime does not leave behind any tangible external physical trace that can be examined. This makes the procedures for discovering the crime and identifying the perpetrator difficult, unlike the traditional crime in which the perpetrator usually leaves behind physical evidence, witness testimony, or other evidence. Also, the request for search and seizure may target persons other than the suspect.
- cybercrime has an international dimension, that is, it is a cross-border crime since it is carried out via the information network, which often raises technical, administrative, political, and legal challenges regarding its confrontation, especially concerning criminal prosecution procedures (Al-Mutradi, 2012).

The legal status of cybercrime

In this context, there is a discussion about the legal status of programs and data; to examine whether they have an intrinsic value or that their value comes from the fact that they are a modernized group of exceptionable values that can be attacked in many ways. Jurisprudence scholars are divided into two groups in this issue:

- The first party believes that according to the general rules that only material things follow the laws of possession, and that the target of theft must be physical, meaning that it has a tangible physical entity so that it can be transferred and possessed through embezzlement since one of the elements of proving the crime of theft is the material element. Since the information is intangible and cannot be considered as a value that is subject to possession and acquisition, except in the light of intellectual property rights, therefore information and mere ideas are excluded from the field of theft, unless it is recorded on a CD or tape. If the disc or tape is stolen, then there is no legal problem in describing the incident as theft of information of material nature. Rather, the problem arises when we are facing the theft of non-physical information money.
- The second party thinks that information is nothing but a new set of values that can be acquired independently of its material support, on the basis

that the information has an economic value that can be acquired illegally. The team also believes that the information is closely related to the owner, similar to the legal relationship that the owner has with the thing he owns. This means that information is money that can be owned or exploited based on its economic value and not based on its physical existence, and therefore it deserves legal protection and is treated as money (Al-Arian, 2004).

Forms of cybercrime

There are many forms of cybercrime, including, but not limited to, the following:

- Information sabotage and misuse of information, including databases, libraries, shredding of books, distortion of information, and distortion of official records. etc.
- Information theft, which includes selling, sabotaging, or destroying information such as research or important studies related to technical, industrial, or military development.
- Falsification of information, which includes illegal access to educational system databases and tampering with data, such as changing students' marks.
- Falsification of information, which includes replacing the information with false information, such as recording and issuing records of certificates not issued by the educational system.
- Violation of privacy, which includes publishing information of a private nature about individuals or entering individuals' electronic accounts and publishing information about them, or publishing information about individuals 'history.
- Wiretapping, which includes accessing databases and stealing conversations over the phone.
- Espionage, which includes intercepting information and trying to find out what individuals are doing.
- Defamation, which includes the use of private or information related to a deviation or crime and its dissemination in a manner that is intended to destroy individuals' personalities or offend them.
- Scientific theft of books and academic scientific research, especially of an experimental and applied nature.
- Theft of inventions, especially in the scientific fields, to be used or sold.
- Unlawful access to networks with the intention of misuse or obtaining benefits through sabotaging information, espionage, or information theft.
- Software piracy includes illegal copying, use, or further sale of the software
- Data and information piracy, which includes hacking and seizing data with the intent to benefit from it, especially credit card numbers, account numbers, login, and passwords.
- E-mail bombs, which include sending viruses to destroy data through e-mail
- Disclosure of secrets, which includes obtaining very private information and publishing it on the network.
- Card financial fraud, which is the result of the illegal use of shopping, money, or phone cards (Matar, 13, DC).

Evidence in cybercrime

Cybercrime is considered a new crime, and this has necessitated the enactment of special laws to prove this crime as this type of crime is full of great difficulties. The first of these difficulties involves monitoring and gathering evidence obtained from crime scenes, whether it is physical or virtual evidence. Another difficulty is that digital evidence is difficult to collect and easy to hide and erase, in addition to being easily accessed and manipulated. It has been necessary to define the evidence and indicate its methods, given that dealing with this type of crime raises many substantive problems related to criminalization, as well as procedural problems related to research, investigation, and providing evidence to institute a criminal case against the accused, which requires the presentation of evidence within the framework of the prosecution process (Rabiaa, 2016).

The concept of evidence

The definitions provided by the jurists in the law in defining Evidence have varied. Here we mention the definition of Dr. Al-Sadah, who has defined evidence as establishing evidence before the court in the manner specified by the law when there is a disputed right. Dr. Al-Senhawi has defined it by saying: It is the establishment of evidence before the courts in the manner specified by the law when there is a legal incident (Al-Zuhaili, 22. D.S.). We go with the definition of Dr. Al-Sanhuri in this context.

Means of evidence

There are many means of Evidence approved by the laws, and they are the same means of evidence in criminal matters in Islamic law so that the means of Evidence are limited to:

- Shahada: It is the highest and most important means of evidence. It has been approved by Islamic Sharia and adopted by man-made laws.
- Confession: which includes the explicit and implicit confession, and the confession by verbal, written, and sign. Sharia and positive laws have approved this mean of evidence.
- Oath and its many types, including the complementary oath, and the decisive oath. The Islamic Sharia has recognized other types of oath like the oath of? the oath of Compurgation, and the oath of condemnation.
- Written documents such as a confession letter written by the bequeathed or by the witness, the judge's letter to the other judge, court records, state bureaus, and so on. Sharia recognizes this mean of evidence so do the positive laws.
- Clues including tracking clues, clairvoyance, suspicion of the validity of the oath, status quo, customs, and habits. This mean of evidence is applicable in Sharia and man-made laws.
- Inspection and experiences including examination of the judge or his deputy of the criminal case, and the expertise of specialists in every science or branch of life. This includes the testimony of a doctor, a veterinarian, an examiner, a lawyer, a testimony of a midwife, moon sighting, and other things that need more experience and knowledge in one aspect of life in

such a way that the judge or the ordinary person cannot know if they simply relied on their general information. Sharia and man-made laws agree on this.

- The judge's knowledge and experience: This comes after he finishes diligence and examination of other means of evidence and after he reaches firm conviction. This is agreed upon in Sharia and man-made laws (Behansi, 2001). Here we point out that the means of evidence in Arab laws, including the UAE law, have comprehended all possible general means of evidence in the field of cybercrime

The position of the UAE legislator on cybercrime

The United Arab Emirates has shown a remarkable interest in combating cybercrime. It has also shown organizational and legal development in combating cybercrime and regulating the provisions for Evidence thereof. The UAE has always been a pioneer in the field of combating cybercrime as it has adopted the idea of combating cybercrimes according to the Arab Emirates Guidance Law to Combat Information Technology Crimes (2003), which was approved by the Council of Arab Justice Ministers in its nineteenth session by Resolution No. (495 - 19 - 8/10 / /). 2003) and the Council of Arab Interior Ministers in its twenty-first session by Resolution No. (417-21/2004). The UAE is considered the first Arab country to enact an independent law to combat cybercrime under Federal Law No. (2) of 2006. This law was followed by the issuance of the decree of Federal Law No. 3 of 2012 providing for the establishment of the National Electronic Security Authority, and then the issuance of Federal Law No. (5) of 2012 regarding combating cybercrime. Some articles of this decree have been amended according to Federal Law No. (12) of 2016 regarding combating cybercrime. Among the most important of these manifestations of the UAE's interest in combating cybercrimes is the establishment of the Federal Prosecution for Information Technology Crimes in the capital Abu Dhabi in 2017 to confront crimes resulting from the rapid technological development. The Information Technology Crimes Prosecution is responsible for investigating, acting, and initiating criminal proceedings in crimes of using the information network "the Internet"

Difficulties and challenges of evidence in cybercrime

Contrary to what many researchers and specialists in the field of combating information crime believe, the phenomenon of the proliferation of legislation and laws to eliminate cybercrime is increasing in many countries of the world, including the United Arab Emirates. When enacting laws against cybercrime, the legislators have neglected that information crime originates in one country so that its impact takes place in another country and that the perpetrator is a competent specialist with knowledge and experience. The most prominent challenges in evidence of cybercrime are summarized as follows:

- The international dimension: computer systems are accessed in one country, while data is manipulated in another country, and results are recorded in a third country. Needless to say, that evidence of cybercrime can be stored in a computer located in a country other than the one in

which the criminal committed his act, thus the cybercriminal can conceal his identity and transfer the material through channels located in different countries and on different continents before reaching the recipient, as a result of the ability to transfer information electronically from one network to another and to access databases on different continents. The crime takes place in several countries and is governed by several laws and rules that exist in each country thus rising a challenge to the judicial authorities in applying the law and increases the difficulty of investigating it (Morocco Conference, 2017).

- Electronic information and data are stored digitally making it invisible to see and track
- The Encryption of data stored electronically or transmitted over communication networks
- Ease of erasing evidence in a short time (Ibrahim, 40)

Conclusion

After a detailed presentation of cybercrime, its nature, characteristics, types, means of evidence, and the obstacles preventing the ability to prosecute the perpetrators, the study has concluded with a set of findings and recommendations, which we review as follows:

- In light of the diversity of transactions, the overlapping of relations, and the difference of human souls, the Emirati legislator has intended to keep pace with legislative development and enacted several important criminal legislation including a set of provisions that would enhance levels of protection of public and private interests.
- Cybercrime differs from its traditional counterpart in nature and means of collecting evidence. There are difficulties in proving electronic evidence and tampering with evidence does not leave a physical trace as is the case in other conventional crimes.
- UAE laws are devoid of evidentiary texts related to cybercrime. The weakness of the staff working in the field of prosecution and tracking of perpetrators of cybercrimes will cause the loss of evidence, in addition to poor awareness among the general public of the danger of dealing with unknown websites.

Recommendations

The study has culminated with several recommendations that may be important factors in promoting and advancing UAE legislation related to combating cybercrime, and these recommendations focus on the following:

- Granting more powers to the Judicial Enforcement Officer concerning the investigation of the suspects, as well as granting the enforcement offers more the permissions of the prosecution that is in cases of flagrant delicto, we do not need a prosecutor's permission.
- Imposing legislation that compels technology companies and social media platforms to demand customers and clients to provide personal documents

that prove their identities when registering on any platform on the Internet. These documents will serve as an electronic fingerprint.

- The need to create appropriate rules in the field of criminal procedures due to the inappropriateness of the current criminal procedures in the field of investigating information technology crimes.
- The necessity of expressly stipulating all laws regulating criminal and civil evidence thus allowing the judge to rely on evidence extracted from the computer and the Internet, as long as the seizure of this evidence is the result of legitimate procedures.
- Establishing special security departments concerned with combating cybercrimes and providing them with qualified employees who can collect information, conduct investigations, and communicate with similar entities in other countries.
- Qualifying those in charge of law enforcement agencies to develop their information in the field of information technology, by training and qualifying the administrators, experts, investigation authorities, and judges.
- Holding intensive courses for human cadres working in the field of investigation and investigation. Holding trials for crimes of infringing electronic information systems and computer applications, and the associated crimes.
- Activating the role of preventive control that precedes the occurrence of cybercrime, by activating the role of educational institutions (mosque, family, educational institutions, media), raising awareness of the danger of cybercrime on the family and society, and strengthening religious faith.

References

Abd al-Latif Rabiah, (2016) Electronic crimes (criminalization, prosecution, and evidence), research presented to the first conference of electronic crimes in Palestine. Held at An-Najah National University. Nablus.

Abeer Baqiqi (2018). Evidence in information crimes in Algerian law. Ph.D. thesis. Biskra University. Algeria

Ahmed Bahnasi (2000). Evidence theory in criminal jurisprudence, MA thesis. Naif Arab Academy for Security Sciences, Riyadh

Al-Tabib Al-Baraka. (2019): The Problem of Evidence in Cybercrime. Afaq Magazine, Volume 11. Number 1

Decree-by-Federal Law No. 3 of 2012 establishing the National Electronic Security Authority

Federal Law No. (12) of 2016 regarding combating information technology crimes

Federal Law No. (2) of 2006 regarding combating information crimes

Federal Law No. (5) of 2012 regarding combating cybercrime

Kamel Matar, Electronic Crime

Miftah Al-Matradi (2012). Electronic crime and overcoming its challenges. A working paper presented to the Third Conference of Presidents of Supreme Courts in the Arab Countries of the Republic of Sudan

Mohamed Hegazy: Computer and Internet Crimes (Information Crimes). The Egyptian Center for Intellectual Property

Mustafa Abdel Baqi (2018). Cybercrime investigation and Evidence. Journal of Sharia and Law Sciences. Volume 45 Issue 4.

Mustafa Al-Zuhaili Means of Evidence of Authentic Electronic Document, Al-Adl Magazine, Issue (32)

Rashid Ibrahim, Criminal Investigation of Information Technology Crimes, an applied study on the city of Abu Dhabi. Crisis Center for Studies and Research, Issue 131.