Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

The Criminal Prosecution for the Crime of Electronic Threat According to Jordanian Legislation

mahmoud Aref aleshoush[1]

Abstract

This study addresses an important and emerging topic, which is electronic threat crimes and their criminal consequences according to the new Jordanian Cybercrime Law of 2023. The study is divided into two sections. The first section discusses the legal nature of electronic threat crimes, divided into two parts: the nature of electronic threat crimes and the elements of electronic threat crimes. The second section discusses the mechanism of combating electronic threat crimes, also divided into two parts: how to prove electronic threat crimes and the penalty for threat crimes using electronic means. The study concludes with important findings that highlight the need for specialized teams to investigate electronic threat crimes and adapt to modern developments in dealing with intelligent criminals who possess different characteristics from traditional criminals. The conclusion also includes recommendations to establish units within security institutions to handle electronic threat crimes, receive threat reports, and develop high-level skills to track such intelligent criminals.

Keywords: *Technological Advancement, Cyber Threat Crime.*

Introduction

We live today in a new era of scientific, technical, and technological progress that results in a human development revolution at all local and global levels. The process of exchanging information and knowledge has become easy and smooth. The rapid spread of information through various technological communication means has facilitated the flow of information, news, knowledge, and conversations smoothly and freely.

On the other hand, this technological advancement has brought about numerous risks and damages, especially due to weak regulation, resulting in the emergence of a new type of sophisticated crime that differ from their predecessors in terms of methods, styles of perpetration, and the characteristics of criminals. They are known as cybercrimes, and they have become a direct and clear threat to local and global security and stability, hindering the completion of the process of economic and security development.

And because of that, many countries have sought to develop legislative systems to introduce texts and penal and procedural legislation that are in line with the phenomenon of modern cybercrime. Some of these legislations were successful, while others suffered from some defects and shortcomings. With the spread of social networking sites, which provide users with the ease of communication with others through chat rooms and social networks, individuals, both young and old, often expose their personal information, photos, videos, and private moments or those of their families on the Internet, especially young people who are the most frequent users of the Internet.

In recent years, advanced technology has emerged to serve and assist humans in accomplishing their tasks. However, some morally weak individuals have decided to make money through illegal methods, misusing this technology and causing harm to others by threatening them electronically.

[1] Assistant Professor of Criminal Law, Faculty of Law, Al-Zarqa University, Email: maleshoush@zu.edu.jo.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

The Problem of the Study

The problem of this study lies in determining the adequacy of the provisions of the new Electronic Crimes Law for the year 2023 in combating the crime of electronic threats. This main problem raises several questions as follows:

- What is the crime of electronic threat?
- What are the types of electronic threats?
- How should electronic threats be dealt with?
- What are the forms of electronic threats?
- What are the procedural mechanisms for combating electronic threats?

Study Importance

The importance of this study lies in shedding light on the mechanisms for combating cyber threats, which concern an important and vulnerable segment of society. The significance of the study is demonstrated by outlining the criminal protection provided for individuals threatened through electronic means.

Study Objectives

- Statement of the legal nature of the crime of cyber threat.
- Statement of the forms of cyber threat.

Study Methodology

In this study, we relied on the following approaches: the descriptive approach by selecting the relevant legal texts related to the study topic under the new Electronic Crimes Law of 2023, and the analytical approach based on analyzing the regulated legal texts of the study topic.

The Legal Nature of the Crime of Electronic Threats

Cybercrimes are considered modern crimes. These crimes only emerged after the spread of the Internet, computers, electronic media, and various modern means of communication, especially those used by advanced smartphones. Without these devices, cybercrime would not exist. It requires sufficient knowledge, control, and familiarity with information technology, especially for the Internet. It cannot be conceived without its involvement in an element of the crime, such as the misuse of obtained information and the threat posed by it. If electronic threats resemble traditional crimes, the use of illegal means by criminals distinguishes them, as they are committed by highly intelligent and skilled individuals with good knowledge of modern technologies and their misuse. It constitutes a violation of privacy and a threat to the owner (Ahmed, 2014).

The private lives of individuals, which require significant protection in the present time due to violations that infringe upon privacy caused by the interference of other individuals or public authorities, have as their goals the respect for individual and collective rights and freedoms. They serve as a true measure of the progress and development of nations. Therefore, comparative criminal jurisprudence largely considers the existence of a contradiction between freedom and the law (Sheri, 2015). This is because preserving individual freedom will inevitably be balanced with the preservation of public security and order in society, thus ensuring the privacy of individuals, which is part of their rights and freedoms. Any assault on human life and intrusion upon it will create a fearful individual who is not fit for a society of free individuals, as

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

discussed in the second paragraph of the preamble to the Universal Declaration of Human Rights, which is considered a model society for safeguarding human rights.

Nature of the Crime of Electronic Threats

Feeling safe and secure in one's life, possessions, and dignity is one of the most important aspects of fundamental purposes that modern societies seek to achieve, and this can only come through the provision of legal foundations that guarantee the realization of this matter (Al-Hayt, 2015)

Internet crimes are new types of crimes that carry real threats across all sectors, making their identification and classification difficult, unlike traditional crimes that can be easily classified. They lack established criteria and their misuse poses security threats to nations and individuals.

The Concept of The Crime of Electronic Threats

The danger of electronic threats lies in their impact on the affected individuals and countries. Threats aim to instill fear and disrupt the psychological well-being of individuals, thereby exerting pressure on their will and causing harm to them and their surroundings.

The term "threat" refers to "intimidation and fear" (Al-Rashidi, 2016) and it is commonly understood as the act of instilling fear and implying potential harm or punishment.

It is a process of identifying and analyzing electronic threats. The term "threat intelligence" can refer to the data collected about a potential threat or the process of collecting, processing, and analyzing that data to gain a better understanding of the threats. Threat intelligence involves examining data in context to identify issues and disseminate solutions to the problem found (Abd Al-Rahman, 2015).

Thanks to digital technology, the world is more interconnected today than ever before. However, this increasing interconnectivity has also led to an increase in the risks of cyber-attacks, such as security breaches, data theft, and malware. Threat intelligence represents a key aspect of cybersecurity (Abdel-Qawi, 2012)

Conditions for Committing the Crime of Electronic Threats

The Threat Subject

The threat subject must involve the commission of a crime against the person or property of the threatened individual, such as the threat of murder, assault, or property damage, or against others who are closely related to the threatened person, such as their children or family members. It can also be through tarnishing their honor or reputation, by threatening to defame them or attribute things to them that would harm their dignity or reputation among people, or by threatening to disclose personal secrets that, if exposed, would harm their dignity and reputation. The essential element in the threat subject is that the victim believes the threat to be serious, even if the perpetrator does not intend to actually carry out the threat. The crime occurs as soon as the perpetrator has the ability, whether through spoken or written words, to instill fear in the heart of the victim (Hanash, 2020)

The Means of Threat

It must be either written or verbal. Verbal threats require the involvement of a third party. Therefore, direct verbal threats without the involvement of a third party are not considered a threat crime. They often occur in the heat of anger or during a heated argument between the parties. Threatening words do not necessarily have to be expressed in specific phrases or be explicit. It is sufficient that they convey the meaning of a threat, either directly or based on the circumstances (Al-Hasnawi, 2009)

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

Means of Committing the Crime of Electronic Threats

- The computer and its accessories and programs are considered to be a device that is "an electronic, and optical device for preparing high-speed information and performs logical, arithmetic, or numerical functions." It also includes any facilitation of information storage or communication, whether direct or indirect.

- The Internet: The Internet is known as the international network of communication that has connected computers worldwide and is one of the most significant advancements in human history.

- Mobile phones and their accessories and software: The mobile phone is used by the cybercriminal as a tool to commit crimes when using the internet in communication programs, such as spying on others. It is known as "any behavior arising from the unauthorized use of telecommunications technology and information related to the mobile phone that can harm the interests of others or expose them to danger." As for the phone accessories, they include a camera, Bluetooth, and recording devices. Regarding software, there are also various programs designed for the mobile phone.

According to the Electronic Crimes Law, it appears that the definition of a mobile phone is missing, despite it being one of the most important tools used in electronic crime. This is because it has become accessible to everyone, which allows it to be misused by minors due to their lack of knowledge of the regulations. However, we note that the law compensates for this omission by mentioning the prescribed punishment for the perpetrator when misusing the phone.

Elements of the Crime of Electronic Threats

Since ancient times, the act of threatening the victim has been criminalized, due to its infringement on their freedom. The act of threat was previously criminalized according to the provisions of the minimum criminal law, but due to its evolution and consideration, it is now regulated by the traditional provisions of the technological criminal law, which encompasses all aspects of life along with the development of the means of threat. These means are embodied in the material component of the crime, which is the criminal behavior that results in the crime (Sadiq, 2015) Punishment for the crime of threat through electronic means, in its technological form, is now governed by the new Electronic Crimes Law of 2023.

The Material Element

Committing a crime online requires logical and technical involvement, including positive material conduct, making online crimes uniformly characterized. It involves a material action as one of the elements of the material component, and the use of a computer and the internet falls under the scope of legality. This means that the use of a computer and the internet becomes part of the material conduct in crimes arising from internet usage (Al-Feel, 2011).

From the foregoing, we can see that material activity is built on the technical relationship between the perpetrator of an internet crime and the machine. In determining the occurrence of criminal behavior using the internet, the American legislator has found that internet use does not have a purpose in itself; it is not used for the sake of using it but rather to achieve significant benefits. However, it can also be a means to commit a crime. The material component in crimes committed online poses various challenges imposed by the nature of the environment in which the crime takes place, involving the use of computer devices or the World Wide Web. The digital environment and internet connectivity require an understanding of the initiation, engagement, and consequences of this activity. This criminal activity can take various forms, such as breaching the secrecy and privacy of personal data, causing harm to its owner, or intercepting correspondence (Sakr, p. 54).

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

The Legal Element

In the legal context, "the legal element" means the presence of a law that criminalizes an act, specifies the punishment for it, and clarifies the consequences of committing the criminal act. However, the task of the judiciary and law enforcement agencies has become extremely challenging in the face of significant challenges posed by crimes committed on the internet. Countries that have not yet enacted specific laws to criminalize various offenses arising from the unlawful use of the Internet are left with no choice but to apply traditional criminal laws to these cases. This is done out of concern for security breaches and to prevent criminals from continuing their unlawful activities and evading the reach of justice.

However, this should not hinder the effort to interpret traditional legal texts concerning various forms of attacks and threats on individuals' private lives or public property and apply them to newly emerging crimes brought about by the communications revolution. Taking an expansive interpretation of traditional texts and applying them to crimes committed on the internet allows judicial authorities the flexibility to interpret these texts in light of the discretionary power vested in judges. The principle of criminal legality prohibits criminal prosecution in the absence of a legal text; there is no crime or punishment without a legal provision.

The Moral Element

Understanding the moral element of internet crimes is an important aspect in determining the nature of the perpetrator's behavior and how to apply punitive texts. Without the moral element, there would only be one crime, which is unlawful access or unauthorized entry. Therefore, the direction taken by comparative jurisprudence in terms of the age of criminal responsibility for unlawful entry might be a relevant topic here. Distinguishing between the crime of unauthorized access to a data processing system and the crime of exceeding one's authority in accessing such a system represents a precise differentiation (Lalhouni, 2004).

The moral element, specifically, refers to the mental and psychological state of the perpetrator as the focal point of criminal law. Within this element, all elements of criminal responsibility are met, including intent and causation, along with the recognition of the state's right to punishment based on these elements (Al-Huqbani, 2013). This element can be defined as the relationship that links the material aspects of the crime to the personality of the perpetrator, and it is the locus of culpability in the sense of deserving punishment. As a result, the law assigns blame and punishment to it. Through this element, the scope of holding the perpetrator accountable can be determined by defining the criminal intent they possess, without which a person cannot be punished for their actions.

Criminal intent, both in its general and specific forms, converges in crimes committed on the internet with its counterparts in traditional crimes, including knowledge and will. The offender must be aware that the action they are committing is unlawful, based on the embodiment of the sinful will within the perpetrator, and the direction of this will towards performing an unlawful act, which is a legal offense (Adbad, p. 29).

Since the era in which responsibility was determined only by the mere occurrence of the physical act of the crime, and the role of intent in the crime was taken into consideration, the discussion about the moral element of the crime began. It is no longer sufficient for the physical aspect of the crime to be fulfilled alone. The compositional act of the crime must also have been committed consciously and willingly. Criminal liability or wrongdoing, in its broad sense, is the essence of the material aspect, and this wrongdoing is represented by a malevolent intent that deviates intentionally towards violating the law. Wrongdoing can take two forms: intent (criminal intent) or mistake (non-deliberate mistake).

Mechanism of Combating Electronic Threat Crimes

There is no doubt that new technology brings along new threats, and these threats have had a significant and direct impact on people's lives, threatening their stability. The phenomenon of cybercrime has significantly and rapidly spread in recent times due to the widespread use of personal computers and smartphones connected to the internet. It is undeniable that this type of crime has become a disturbing reality, endangering the reputation and lives of individuals. Therefore, it is essential to be alert to avoid

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

becoming victims of it. Electronic threat crime is a crime that affects all groups, including institutions and individuals who use personal computers or smartphones. It is undoubtedly an unethical behavior, unauthorized, prohibited by the law, condemned by ethics, and rejected by society.

Proof in the Crime of Electronic Threat

Proof is the establishment of an argument, evidence, and indication. It is the prevailing belief but does not reach the level of certainty that leaves no room for doubt. Evidence serves various purposes, including being a means used to prove a fact, as well as a means of defense when the evidence favors the accused. It is also used to reveal the truth of an act committed, claimed by the plaintiff and denied by the accused. Moreover, evidence is vital for criminal cases, where it is the focal point around which the process of searching for the perpetrator of the crime revolves, and it is the goal of law enforcement agencies.

Criminal proof is defined as the establishment of evidence of the commission of a crime and then attributing it to the accused as the perpetrator of the crime. The process of gathering evidence in traditional crimes differs from the process in electronic crimes. The uniqueness of digital evidence is what sets electronic crimes apart, which poses obstacles and challenges for the competent authorities in the realm of proof. We will address this issue in two sections, as follows:

Digital Criminal Evidence

The aim of justice systems is to diligently pursue all available evidence in both traditional and electronic crimes. To understand the importance of digital evidence in electronic crimes, specifically in the case of electronic threats, it's crucial to define and outline the characteristics of digital criminal evidence. This type of evidence plays a significant role in identifying and prosecuting individuals involved in electronic crimes (Hassan, 2012). Therefore, we will explore the definition and attributes of digital criminal evidence as follows:

Definition of Digital Evidence

Digital evidence, also known as electronic evidence, is defined as evidence derived from computer systems and is typically in the form of magnetic fields or electrical pulses that can be collected and analyzed using specialized software and technology. It is a collection of data or information that can prove that a crime has occurred or establish a connection between the crime, the perpetrator, or the victim. The term "digital" in digital evidence refers to the fact that the data within the virtual crime environment, whether they are images, recordings, or other forms, are represented as numbers within computer systems. These numbers are encoded in a way that allows them to be transformed into images, audio recordings, or videos when displayed.

Some definitions of electronic evidence also refer to it as electronic data, encompassing all digital data that can prove the occurrence of a crime or establish a connection between the crime and the victim or the evidence collected. Digital data includes various types of information such as written text, graphics, maps, sound, and images, all represented in numerical form within electronic systems (Younis, 2004).

Based on the information provided, the most suitable definition for electronic evidence is that it is evidence derived from computer systems, software, computer hardware, or communication networks through legal and technical procedures. This evidence is presented in legal proceedings after being scientifically analyzed or interpreted in the form of written texts, graphics, images, sounds, or other forms to prove the occurrence of a crime or to determine guilt or innocence.

Digital Evidence Characteristics

The digital evidence is indeed non-tangible and cannot be perceived through the natural human senses, as it consists of electrical pulses that cannot be physically touched. It is considered non-material or intangible

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

evidence. Translating digital evidence into a tangible form does not change its digital nature, as it remains based on the electronic representation of information.

Some may argue that digital evidence is less tangible than physical evidence (Al-Halabi, 2014) but this is not accurate. Digital evidence's tangibility is based on its representation, which is not fixed in form, location, or size. Various challenges are faced by authorities when it comes to proving cases using digital evidence, and these challenges arise due to several reasons, including:

- Ease of erasing evidence is indeed a significant challenge when dealing with digital evidence. Cybercriminals, especially in cases of cyberbullying or online threats, may actively try to cover their tracks by deleting or altering evidence after committing the crime. This makes it difficult, and at times impossible, to access and preserve the digital evidence that can prove their guilt.

- Detecting the identity of the perpetrator through digital evidence can indeed be challenging. In cases of cyberbullying or online threats, distinguishing the digital identities of offenders in the virtual world can be far more complex than traditional crimes. Unlike conventional crimes that leave physical traces like fingerprints or bloodstains, cybercrimes often occur in a virtual environment where the offenders hide behind digital avatars or pseudonyms (Al-Husseini, 2015).

- Hindering access to evidence: Sometimes, the perpetrator places technical obstacles to prevent the discovery of their crime and its evidence. This is done through encryption systems with the intention of concealing information from public scrutiny and blocking access to the transmission source.

- Lack of experience among some investigators: One of the challenges in obtaining digital evidence in electronic extortion crimes is the lack of expertise among some law enforcement officers and members of investigative bodies. This lack of expertise relates to computer hardware and its accessories, computer language, and skills required for interrogating an intelligent criminal, such as an electronic blackmailer in electronic extortion crimes.

- Reluctance to report by the victim: This is often due to the victim's fear that reporting the crime will lead to the exposure of their secrets. In essence, this crime is committed primarily because the victim is afraid of their secrets being revealed. Consequently, this reluctance helps conceal the digital evidence that points to the perpetrator. This makes it a significant obstacle in the path of proving the case through digital evidence.

- 6. Lack of a unified legislative mechanism: Variations in legislation criminalizing electronic extortion in different countries create obstacles and difficulties in pursuing the perpetrators. What one country considers legal, another may consider criminal. There is a pressing need for uniform international criminal legislation that is more adaptable to keep up with the rapidly evolving landscape of cybercrime.

The Penalty for the Crime of Electronic Threats

The recent Electronic Crimes Law that was amended in 2023 (The Jordanian Electronic Crimes Law, 2023), has imposed stricter penalties on several crimes, including threats, extortion, data manipulation without authorization, identity theft, defamation, rumor spreading, and personal attacks, among others. The Jordanian Penal Code considers these acts as crimes. This law was introduced to address issues in the digital and virtual world, recognizing the similarity of the acts while differentiating the means used. The increased penalties, however, have sparked concerns that they may discourage citizens from freely expressing their opinions.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

The Electronic Crimes Law amends Article 18 as follows

Anyone who extorts or threatens another person to make them commit an act, refrain from an act, or gain any benefit through the use of information systems, information networks, websites, electronic platforms, or any other information technology means shall be punished with imprisonment for no less than one year and a fine of not less than 3,000 Jordanian dinars and not more than 6,000 Jordanian dinars.

The penalty shall be temporary hard labor and a fine of not less than 5,000 Jordanian dinars and not more than 10,000 Jordanian dinars if the threat is related to the commission of a crime or involves making explicit or implicit requests for dishonorable or offensive matters and is accompanied by a request, whether explicit or implicit, to commit an act or refrain from it.

Conclusion

Electronic threat crimes are considered one of the modern crimes, often referred to as soft crimes in the field of criminology, as they lack physical violence. These crimes are a form of cybercrime. Electronic threat crimes represent the other side of traditional threat crimes that occur in the physical world, where the perpetrator leaves physical evidence such as fingerprints or traces of blood. In contrast, electronic threats occur in the virtual world, filled with symbols and codes, which pose significant challenges for investigative agencies when dealing with digital evidence.

The rise of electronic threat crimes has become a concerning phenomenon among users of modern technology, particularly after the information and technology revolution that took place in the 20th century. In response to this revolution, countries initially tried to adapt their legislation to address these emerging crimes. However, they soon realized the need for specialized legal provisions to deal with these cybercrimes, including electronic threat crimes.

In our study, we have reached several conclusions, which can be summarized as follows:

Results

Electronic threat crimes are modern crimes committed using information networks, modern devices, and their applications.

Electronic threat crimes are challenging to prove as their traces can be easily erased.

Electronic threat crimes require specialized investigative teams with experts who are qualified and trained to adapt to modern developments in investigating intelligent criminals with distinct characteristics from traditional criminals.

Recommendations

It is essential to raise community awareness about the dangers of electronic threat crimes. Encourage individuals who are targeted by electronic threats to report the crimes while ensuring the confidentiality of the victims to prevent them from refraining from reporting. Train and equip personnel in investigative and judicial authorities with modern investigative techniques and digital evidence handling to avoid allowing crimes to escape due to a lack of expertise in dealing with digital evidence.

Establish units within law enforcement agencies to handle electronic threat crimes, receive threat reports, and track those making threats. Provide high-level training and expertise in tracking intelligent criminals.

Enhance international cooperation by developing an international mechanism for standardizing laws that criminalize electronic extortion, preventing criminals from escaping punishment due to varying legal

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 4966 – 4974
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4605

systems. Reevaluate Arab legislation and recognize electronic crimes as a reality that must be addressed with appropriate criminalization and penalties.

References

Ahmed, Tarek Afifi, electronic crimes, mobile phone crimes, a comparative study between Egyptian, Emirati, and Saudi Arabian laws. National Center for Legal Publications, Egypt, 2014, p. 77.

Sheri, Muhammad Al-Amin., Investigating Emerging Crimes, Saudi Arabia: Center for Studies and Research, Naif Arab University for Security Sciences, Riyadh, 2015, p. 34.

Al-Hayt, Adel Azzam, Crimes of Defamation, Insult, and Disparagement Committed through Electronic Media, the Internet, Mobile Networks, and Traditional, Mechanical, and Printed Media: A Comparative Legal Study. Amman: Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2015.

Al-Rashidi, Taha Al-Sayed, The Special Nature of Information Technology Crimes and Their Impact on Investigation Procedures in the Egyptian and Saudi Criminal Justice Systems, Dar Al-Kotob and Arab Studies, Egypt, 2016, p.29.

Abd Al-Rahman, Muhammad Jalal, Cybercrime in Islamic Jurisprudence and Laws: Comparative Study, Law and Economics Library, Cairo, 2015, p. 54.

Egyptian, Abdel-Sabour Abdel-Qawi, The Digital Court and Information Crime, Library of Economics and Law, Kingdom of Saudi Arabia, 2012, p. 34.

Sarah Muhammad Hanash, Criminal Liability for Threats Via Electronic Means, a comparative study, a thesis submitted in fulfillment of the requirements for obtaining a master's degree in public law, Department of Public Law, Middle East University, Faculty of Law, Amman, January 2020, p. 43.

Ali Jabbar Al-Hasnawi: Computer and Internet Crimes, first edition, Al-Yazouri Publishing and Distribution House, Jordan, Amman, 2009, p. 33.

Sadiq, Nahida Omar, 2015, The Crime of Threat in the Iraqi Penal Code, Kurdistan Regional Government of Iraq, Ministry of Justice, Dohuk, p. 12.

Al-Feel, Ali Adnan, 2011, Cybercrime, 1st edition, Beirut: Zain Legal Publications, p. 43.

Sakr, Ahmed Kilani Abdullah, crimes arising from computer misuse, Master's thesis, College of Law, Baghdad University, p. 54.

Lalhouni, Hussam al-Din, 2004, "Legal Protection of Private Life in the Face of the Computer," Journal of Legal Sciences, P. 43.

Al-Huqbani, Rayez Salem. "Research and Investigation Skills in Cybercrime: An Analytical Study of Research and Investigation Skills in Cybercrime Among Police Officers in the City of Riyadh. PhD thesis. Department of Police Sciences, Graduate Studies College, Naif Arab University for Security Sciences. Saudi Arabia, 2013, p. 98."

Ghalib Rami Adbad, Journal of Electronic Blackmail and the Mechanism to Combat It in the Republic of Iraq, Iraq, Baghdad, Dar Al-Kutub and Documents, 1st edition, p. 29.

Hassan, Amal Abdul Rahman Youssef, Modern Evidence and its Role in Criminal Proof, Master's Thesis, Faculty of Law, Middle East University, Jordan, 2012.

Omar Muhammad Abu Bakr Younis - Crimes arising from the use of the Internet, substantive rulings and procedural aspects, PhD thesis, Ain Shams University, Dar Al-Nahda Al-Arabiya, Cairo, 2004, p. 46

Al-Halabi, Khalid Abbad Al-Halabi, 2014, Investigative Procedures and Evidence Collection in Computer and Internet Crimes, 1st ed. Amman: Dar Al-Thaqafa for Publishing and Distribution, p. 54.

Al-Husseini, Ammar Abbas, 2015, Criminal Investigation and Modern Methods in Crime Detection, 1st ed., Beirut: Al-Halabi Legal Publications, p. 32.

The Jordanian Electronic Crimes Law of 2023 will be effective 30 days after its publication in the Official Gazette, on August 13, 2023, in Official Gazette No. 5874.