Kurdish Studies
Feb 2024
Volume: 12, No: 2, pp.4060-4087
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: December 2023 Accepted: January 2024
DOI: https://doi.org/10.58262/ks.v12i2.300

The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law

Inas Fadel Salim*[1], Dr. Mohammed Redha Dhafri[2]

Abstract

One of the most important evidences of the seriousness of the criminal activity is that it occurred based on a prior criminal agreement that indicates an advanced level of criminal preparedness and social danger, as the agreement of two or more people to carry out criminal behavior clearly indicates a type of organization, disregard for the security of society, and a violation of all laws and social customs, and that It has elements agreed upon by all jurists, even if their expressions differ. We can confirm that agreement in its essence is a psychological state, consisting of two or more wills, but it has a physical appearance that is derived from the means of expressing the will. We have adopted for this study an inductive approach to the texts and an analytical approach to jurisprudential opinions. It has been proven to us that the criminal agreement is distinguished from the agreement as a method of participation in several aspects, and that there are two types of criminal agreement, the general agreement and the special agreement. The member of the criminal agreement is exempted from punishment in the event that he takes the initiative to inform the authorities of the existence of an agreement to commit a crime and the participants in it, before it occurs. The research has reached the conclusion: Several findings and recommendations, the purpose of which is to overcome the errors or shortcomings of the Iraqi criminal legislation, and the question of our message is summed up: What is the criminal agreement in cybercrimes in Iraqi, Emirati, and Qatari law, and what is meant by the criminal agreement, given that this crime is committed by more than one person and in the event of multiple For the people who commit the crime, in this case, the agreement is different depending on the role they play, and this is the case in all countries that are the subject of our research.In our message here, there is a special agreement between people who commit such crimes, given that the desired goal is to know the policy of Iraqi, Emirati, and Qatari legislators in confronting information crimes, considering them to be among the new crimes in terms of criminalization on the basis of their seriousness and consequences, and to contribute to the role of The legislator must rush to legislate a legal model or amend existing ones in order to confront cybercrimes in a way that is consistent with the extent of their seriousness, as the Emirati and Qatari law preceded the Iraqi one in legislating this law. As for the importance of this message, it will stem from the study of cybercrime and also a statement of the position of comparative legislation and Iraqi legislation on it. And arriving at a set of results and recommendations. The importance of our study lies in shedding light on the law on combating cybercrime in Iraqi, Emirati, and Qatari law, as well as the texts contained therein related to the crime of illegal entry, considering it a relatively modern law compared to the rest of the Arab legislation. Also, the importance of this study lies in stating its seriousness. The crime of illegal entry into the information system or the terrorist crime with regard to cybercrimes and the serious dangers that may lead to them. Also, this study aims to explain the pillars and elements of the terrorist cybercrime that the Iraqi, Emirati and Qatari legislators adopted in punishing this crime in order to combat it and reduce the serious risks resulting from it. As for the approach followed in our study, we relied in our study on the comparative analytical approach between

[1] Middle Technical University, Department of legal affairs, Iraq
[2] Qom University, College of Law, Iran
*Corresponding Author E-mail: Inas20062004@gmail.Com

Iraq, the Emirates, and Qatar. The subject of this research is the repercussions of the criminal agreement in cybercrime on international relations by examining the concept of the criminal agreement in cybercrime and the extent of its impact on international security and the international relations that A group of technological transformations contributed to its development, as anyone who personally commits an act of its physical implementation is considered a contributor to the crime. Any original actor is considered a contributor, whether his cooperation with the criminal or other criminals was through agreement or they were brought together by chance and assumed their intention towards one goal, as in the case of theft. Someone's house.

Keywords: *Criminal Participation, Cybersecurity, Cybercrime, Elements of Cybercrime, Penalties for Cybercrime.*

Introduction

First: Statement of the Issue

The world has witnessed a major revolution in the field of technology, automated calculations and electronic data processing, and this information revolution is the reason for what is currently called the information industry. Because of this development, new investment outlets have emerged that have taken the form of institutions, companies, and also individual projects. All of this is concerned with manufacturing accounts and some... The other has taken the aim of preparing programs to process information automatically. Because of this development and changes, it has affected all aspects of life and affected all segments of society. The topic of cybercrime is considered one of the emerging topics. In order to achieve legal protection for the cybernetic system and the topics arising from it, there should be legal rules here in order to criminalize this act. Which aims to attack these systems and must be used as a means to commit one of the traditional crimes, and this in turn may require the intervention of the judiciary in order to expand the scope of the criminal text in order to accommodate these crimes.

The Iraqi Parliament has not yet approved the new Iraqi draft law to combat cybercrime, which includes problematic articles restricting basic freedoms. This draft law was first presented in 2011, and the Parliamentary Committee for Culture and Media at that time requested its withdrawal in 2013, all because of... Facing pressure from individuals and civil society organizations who raised concerns about many of the restrictive provisions contained in this law, and because the Iraqi Parliament did not officially approve the decision to withdraw it, the text was resubmitted with amendments made to it in January 2019, after the Iraqi Parliament completed the first reading of the draft. In January 2019, the law was revised again and reintroduced in November 2020. The Iraqi authorities ordered the closure of more than 12 radio and television stations. Due to the revision of the draft law that was reintroduced in November 2020, it is slightly in line with international standards compared to previous versions, and all of this continues to criminalize other acts. Included in the draft law, as Article 5, paragraph (1), of the draft law stipulates that "anyone who eavesdrops on, picks up, or intercepts any messages via an information network, computer device, or the like, without permission from the competent authority or the owner, shall be sentenced to imprisonment." A period of not less than one year and not more than two years, in addition to fines."

The UAE legislation has addressed cybercrime in a detailed and broad manner, according to the UAE Anti-Cybercrime Law. It has begun to address the misuse of these means and cybercrime a relatively long time ago, and in more detail than other legislation, as the first UAE Federal Law No. 2 has been issued. of 2006 regarding combating information technology

crimes. On August 13, 2012, Federal Decree Law No. (5) of 2012 regarding combating information technology crimes was issued, which replaced Federal Law No. (2) of 2006 and also replaced Federal Law No. 12 of 2006. 2016 amending Federal Decree Law No. 5 of 2012 regarding combating information technology crimes, which was replaced by the text of Article Nine, comparing combating information technology crimes with a new text.

The Qatari law has addressed the subject of our message and the jurisprudence of the Anti-Cybercrime Law No. 14 of 2014, in addition to having referred to the crime of illegal entry contained in the Qatari Penal Code No. 11 of 2004.

As the cybercriminal uses hacking technology in order to carry out his crime, and this is through the fraud he performs on the information systems, the hacking is through the ability to reach a specific target through loopholes in the special protection system and is done through two programs. The first is the server, which is on the victim's device, meaning it carries out the assigned tasks. The second one is found in the hacker's device and is called the beneficiary program. Cybercrime is one of the new crimes that represent a great danger and threat to the individual, society, and also the state's security services, which we must be forced to study in order to combat these crimes by establishing deterrent penal systems, confronting criminal virus attacks, and prosecuting them before the judiciary.

Second: The Importance of Research

The necessity and importance of our message lies in studying cybercrime and also explaining the position of comparative legislation and Iraqi legislation on it and arriving at a set of results and recommendations. The importance of our study lies in shedding light on the law on combating cybercrime in Iraqi, Emirati and Qatari law, as well as the texts contained therein related to the crime of illegal entry into It is considered a relatively modern law compared to the rest of the Arab legislation. Also, the importance of this study lies in explaining the seriousness of the crime of illegal entry into the system, information regarding cybercrimes and the serious dangers that may lead to them. Also, this study aims to explain the pillars and elements of the crime, the criminal agreement for electronic crime adopted by the Iraqi legislator. The UAE and Qatar are seeking to punish this crime in order to combat it and reduce the serious risks resulting from it.

Third: Research questions

Main Question:
What is the criminal agreement in cybercrimes in Iraqi, Emirati, and Qatari law?

Sub-Questions

1- What are the special elements of the criminal agreement regarding cybercrimes in these countries?
2- What are the special penalties in the criminal agreement for cybercrimes in these countries?
Fourth: Research hypotheses

The Original Hypothesis

What are meant by the criminal agreement is whether there is a prior agreement between people in order to harm a person through the computer and the Internet and to infringe on his privacy and his personal space, which must be protected and whoever attacks it must be punished.

Sub-Hypotheses

1- Every crime has three elements in all countries, including the Emirates, Qatar, and Iraq, which are the material element, the moral element, and the causal relationship between them, which we will discuss in the body of our message.
2- Every crime in the world has a special punishment, and this punishment is different from one country to another, as the punishment for this crime is different from the State of Iraq to the State of the Emirates and the State of Qatar.

Fifth: The goal of the research

The primary goal of the subject of our thesis is to know the policy of Iraqi, Emirati, and Qatari legislators in confronting cybercrimes, considering them to be among the new crimes in terms of criminalization on the basis of their seriousness and consequences, and to contribute to the role of the legislator in rushing to legislate a legal model or modify existing ones in order to confront cybercrimes in a way that is consistent with the extent of their seriousness. The UAE and Qatari law preceded the Iraqi law by legislating this law.

Sixth: Research Methodology

In our research, we relied on the descriptive analytical comparative method: an investigative description of the research results in addition to the how of the issue, not its causes.
Explaining the reasons, not the descriptions, by making the basis of the research the analysis of theories and evidence, comparison between them, and inference for proof and denial.

Seventh: Research Structure

The structure through which our research was built using the three chapters, which contained topics, demands, and branches, in order to have a clear scientific research structure. We indicated in the first chapter the pillar of the research through which the research is built, in terms of referring to two sections. The first was titled Concepts and the second was Colleges. As for the second chapter, it was entitled The Legal Model of the Crime of the Cyber Criminal Agreement and the Elements of the Crime (A Comparative Study), and through it we touched on two sections, where in the first section we talked about the material element of the crime of the cyber criminal agreement.

The second section is the legal and moral pillar. As for the third section, the penalties prescribed for cybercrime. We have divided this chapter into three sections. The first section is the penalties prescribed according to Iraqi law. In the second section, we talked about the penalties prescribed according to Qatari law. As for the third section, we discussed the penalties prescribed according to Emirati law.

Chapter One: Concepts and Universals

The First Section: General Concepts

The First Requirement: The Concept of The Criminal Agreement

In this requirement, we will present two branches. In the first section, we will present the linguistic concept, and in the second section, we will present the terminological concept:

The First Section: The Concept of The Criminal Agreement in Language

These are applications of linguistic knowledge, methods, and insights into the judicial text of law, language, criminal investigation, trial, and judicial procedures. It is a branch of applied

linguistics. There are three basic applied fields for linguists specializing in judicial texts: understanding the written language of law, understanding the use of language in judicial and legal processes, and providing linguistic evidence. The field of forensic linguistics is considered homogeneous, but it includes many experts and researchers in different areas of this branch (1).

The Second Section: The Concept of the Criminal Agreement in the Criminal Law of Other Countries

The Iraqi legislator defined the crime of criminal agreement in Article 55 Penalties: "A criminal agreement is considered an agreement between two or more persons to commit a felony or misdemeanor of theft, fraud, and forgery, whether specific or not, or to commit acts prepared or facilitated, provided that the agreement is organized, even in the principle of its formation. continues, even for a short period." The agreement is considered criminal, whether its ultimate purpose is to commit crimes or use it as a means to achieve an illegal purpose. Article 56 of the Penal Code stipulates that "every member of a criminal agreement, even if he does not attempt to commit the agreed-upon crime, shall be punished with imprisonment for a period." Not more than seven years if the crime agreed to be committed was a felony, and with imprisonment for a period not exceeding two years or a fine... if the crime was a misdemeanor, unless the law stipulates a special penalty for the agreement...)), and from this text It is clear that the Iraqi legislator considered the criminal agreement to be a crime in itself, independent of the agreement as a means of participation, and this matter is achieved by one of the shareholders expressing it, whether verbally, in writing, by indicating, or by suggesting, so that the expression reaches the other shareholders and is accepted by them. All shareholders must be accepted in such a way that it can be said that there is an agreement.

The crime of criminal agreement is not conceivable to be attempted, because agreement is a psychological state that takes place through the meeting of wills and does not have a beginning or an end. This is a crime that either occurs or does not occur. The crime of criminal agreement is concluded by simply agreeing to commit a felony or misdemeanor, and therefore abstaining after this does not exempt from punishment because the material element of this crime has been completed and there is no contradiction between the crime of criminal conspiracy and the agreement as a form of previous participation due to the difference in the field of application of each of them. The participants in the agreement are not considered accomplices unless the crime subject to the agreement occurs, whether it occurred completely or as an attempt, unlike the criminal agreement which It is available once it is held, whether the crime has occurred or not. Based on the above, it is conceivable that there would be a material difference between the crime of criminal conspiracy and the crime subject to the agreement, whether it occurred in its entirety or in the form of its attempt. The legislator's goal in this is to eliminate the agreement while it is at the beginning of its formation, and he does not want to wait until the stage of preparation for the crime. As for the ignorance of the members of the criminal agreement that they do not know that the law criminalizes the criminal agreement, this does not count because ignorance of the law is not an excuse, and this is what Article 37/1 of the Penal Code stipulates. The member of the criminal agreement is exempted from punishment in the case of information about the existence of a criminal agreement before the crime occurs. However, if the information occurred after the authorities conducted research and investigation, the informant is not exempted from punishment unless the information facilitated the arrest of the perpetrators.[2].

[1] https://ar.wikipedia.org/wik
[2] https://www.sjc.iq/view.4488/

The Second Requirement: The Concept of Cybercrime

Before giving a definition of cybercrime, we must give a clear idea of what is meant by cybercrime and the images and terminology due to which this crime has been called the information bank currently because of its distinguished position in our current time based on considerations that represent the focus of every discussion related to informatics as a processing science. Available information.[1]

Electronic devices have now become a part of human daily life, computers of all kinds, and communications devices of all kinds, as many consider them the pillars of the civilization in which we live and the development we are witnessing, as well as satellite broadcasting and receiving devices, cameras, audio recording devices, and others.[2]

Certainly, these devices complement each other in function, in addition to complete coordination in the industry, which has widely integrated camera machines with computers and mobile phones.[3]

Certainly, this development is accompanied by the emergence of some computer and Internet crimes, including the term electronic crime, high-tech crimes, or cybercrime.[4]

The First Section: The Legal Concept of Cybercrime

The legal concept of cybercrime, and according to the draft Iraqi cybercrime law, cybercrime, that is, information crime, has been defined as "data, texts, images, shapes, sounds, symbols, databases, computer programs, and the like that are created, stored, processed, or sent by electronic means."[5]

The Emirati legislator did not define cybercrime, that is, electronic crime, in the old repealed laws No. 2 of 2006 and Federal Decree Law No. 5 of 2012, nor in the new legislation decreed by Federal Law No. 34 of 2021. The Emirati legislator left the task of this matter to the jurists in defining this crime, as Each trend deals with the definition from a specific angle, including a technical angle or a legal angle.[6]

The legal definition, according to what the Qatari legislator called, for cybercrime is "any act that involves the use of an information technology means, an information system, or an information network in an illegal manner in violation of the provisions of the law."[7]

Section Two: The Jurisprudential Concept of Cybercrime

There have been many jurisprudential opinions regarding the definition of cybercrime in Iraq, as each person has adopted an understanding of this jurisprudential definition by looking at the angles from which he saw it, as one side of jurisprudence defined it from a technical and other legal angles, and another side of jurisprudence defined it by looking at the means of committing it, its subject, or Depending on the availability of knowledge of the technique of the person who committed it, or based on other criteria according to those who said it.[8]

---

[1]Al-Shawi Munther, Philosophy of Law, Publications of the Iraqi Scientific Academy, Baghdad, 1994, p. 7.
[2], Muhammad Eid, The Internet and its Role in the Spread of Drugs, first edition, Al-Khereiji Publishing House, Riyadh, 2003, p. 23.
[3]Al-Roumi Ahmed, Computer and Internet Crimes, third edition, University Press, Alexandria, 2003, p. 123.
[4], Al-Saghir Jamil Abdel-Baqi, The Internet and Criminal Law (Objective Provisions for Internet-related Crimes), Dar Al-Nahda Al-Arabiyya for Publishing and Distribution, Cairo, 2012, p. 30.
[5]Article (1/twelfth) of the Iraqi cybercrimes draft law.
[6], Iraqi Khaled Ali, rumor crimes and electronic crimes in the United Arab Emirates, research published in the Journal of Jurisprudential and Legal Research, Issue Thirty-Eight, Zagazig University, Egypt, 2022, p. 169.
[7]Article (1) of the Qatari Anti-Cybercrime Law No. (14) of 2014.
[8], Al-Maamouri Raafat Hamid Rais, The impact of information crime and its impact on society, research published in Al-Mufakir Journal for Legal and Political Studies, Iraq, Volume Four, Issue Four, 2022, p. 134.

It has also been defined as the crime of legal attacks that can be committed by means of information technology, by entering forged data into systems and misusing the outputs, in addition to other acts that constitute more complex crimes from a technical standpoint, such as modifying websites.[1]

No matter how many definitions there are, the difference and multiplicity of these labels should not change the content of the cybercrime, that is, an information crime. Therefore, we will focus on some definitions that are considered a definition to be taken jointly in order to come up with a definition that is unified for the elements that make up the cybercrime, as some jurists have argued in Their definition of cybercrime is every illegal behavior related to the automated processing of data or the transfer of this data, and also according to the opinion of some jurists, it is every illegal activity directed at copying, deleting, or accessing information stored inside the computer or transferred through them.[2]

The Second Topic: Colleges

The First Requirement: The Historical Development of the Criminal Agreement in Cybercrimes

The scope of the criminal agreement in cybercrimes is not limited to merely that the crime occurs on the computer itself or that it occurs by means of the computer, such that this computer is considered a tool in the hands of the offender who uses it in order to achieve his criminal purposes within the state. Rather, it has become outside the scope of the state and has taken on a global dimension due to the development of networks. Electronic communications, which have taken on a scope and surrounded the entire world, where the world has become a small village in which geographical and political borders are not recognized, and to determine the scope of crimes, we must clarify the concept of information crime and the position of comparative laws. The duty that we must clarify in defining the concept of information crime is to stand on the concept Crime in national laws and the concept of crime in international laws In order to determine the scope of information crimes, the definition of the crime in the National Penal Code has led to the point that most modern criminal legislation does not provide a definition of the crime, as the task of this matter is left to jurisprudence, and no matter how much jurists differ in defining the crime, In all cases, it does not deviate from positive illegal behavior resulting from a criminal will for which the law imposes a criminal penalty.[3]

The First Section: The Historical Development of the Criminal Agreement in Cybercrimes in Iraqi Law

After it became clear that the nature of information crime related to the automated information processing system is considered global crimes and not international crimes, the position of Iraqi law on the concept of information crime is considered global crimes. What is meant by the principle of universality of criminal law is what is called the term comprehensive jurisdiction, meaning the law is applied. The State Criminal Court has jurisdiction over every crime whose perpetrators are arrested in the State's territory, regardless of the territory in which it was committed and whatever the nationality of the person who committed this crime.[4]

---

[1]Al-Azzawi Samir Ibrahim, Criminal Liability Arising from Misuse of the Internet, Master's thesis submitted to the College of Law, University of Baghdad, 2005, p. 24.
[2]Al-Shukri Adel Youssef Abdel Nabi, information crime and the crisis of criminal legitimacy, research published in Al-Kufa Magazine, Kufa Studies Center, Iraq, seventh issue, 2008, p. 113.
[3], Al-Khalaf Ali Hussein and Al-Shawi Sultan Abdul Qadir, previous source, p. 134.
[4], Al-Hadithi Fakhri Abdul Razzaq, Explanation of the Penal Code, General Section, Al-Zaman Press, Baghdad, 1992, p. 96.

The position of the Emirati law on the criminal agreement in cybercrimes has given the Emirati legislator's interest in personal and intellectual rights and freedoms, which are related and related to the human being and the idea of considerations, are fundamental rights for the human being, whether in terms of the human personality and the other freedoms required for it, or in terms of what is related to the human being's idea of opinion, privacy, and other things. The rights attached to it.[1]

Every human being has the right to privacy in his private affairs and correspondence. Under privacy are the inviolability of the home, the privacy of correspondence, and the right to dignity and security. With regard to the violation of the inviolability of the home, contemporary constitutions have been keen to approve this field. It is worth mentioning that the inviolability of the home is connected to the inviolability of private life, which prevents eavesdropping. It is permissible to photograph inside the home and on the public road by taking pictures without their consent. It is also not permissible to look into their private lives and affairs without their consent.[2]

Qatari jurisprudence has been divided into two parts in order to define cybercrime. Part of the jurisprudence has stated that, according to general rules, only material things are subject to possession and acquisition, and that the thing that is the subject of the theft must be physical so that it can be transferred and possessed through theft that constitutes the material element. In the crime of theft, since the information has an intangible nature, it cannot be considered as a value capable of possession or possession except in light of intellectual property rights. Thus, the information is excluded from the scope of theft unless it is recorded on cylinders or tape. If the theft occurred from one of these two things, it can be considered and qualified. The reality is that it is an information theft of a material nature, and the problem that arises here when faced with the theft of informational property is non-material.[3]

The Second Requirement: The Nature of the Criminal Consequence in Information Crimes and the Criminal Agreement Therein

What is meant by the criminal consequence resulting from cybercrime is the natural effect that results from behavior whenever it becomes, from a legislative standpoint, an aggression against a right or interest protected by the law.[4]

There has been a dispute over the criminal result, the criminal agreement, and its determination, and it has gone in two directions in order to determine the meaning of the result. The first direction takes the material or natural nature and is based on the idea that the criminal result is the change that behavior brings about in the outside world, and in other words, it is visible or tangible, and the second direction, which The idea of a legal or legitimate nature may be adopted, as the criminal result was originally considered to be an assault on a right or interest, for which the criminal legislator has established protection in order not to harm it or threaten it with danger, and this is what the Iraqi legislator went for.[5]

On the same subject, the opinion of the Emirati and Qatari legislators was similar in that criminal jurisprudence has divided crimes in terms of the criminal result into crimes of danger

[1]Al-Qaisi returned Ali Al-Hamoud, Principles of Constitutional Law and Systems of Governance, a comparative analytical study of the Constitution of the United Arab Emirates, first edition, University Library, Sharjah, 2013, p. 257.
[2], Abdel Azim Abdel Salam and Salem Jarwan Al Naqbi, Constitutional and Criminal Guarantees for Human Rights and Public Liberties in the United Arab Emirates, Academy of Police Sciences, Sharjah, 2009, p. 31.
[3]Al-Mutadi Muftah Boubakar, Electronic Crime, a working paper presented to the Third Conference of Presidents of Supreme Courts in the Arab Countries, Sudan, 2012, p. 17.
[4]Suleiman Abdel Moneim, The General Theory of the Penal Code, A Comparative Study, Al-Halabi Legal Publications, Beirut, 2003, p. 475.
[5], Ramadan Omar Al-Saeed, The Idea of Consequence in the Penal Code, research published in the Journal of Law and Economics, first issue, 1961, p. 105.

and crimes of harm, and that criminal jurisprudence has called crimes of means to crimes of danger and crimes of consequences to crimes of harm, and the basis on which they rely on these The nomenclature is the idea of distinguishing between obligation to a means and obligation to a result within the framework of civil law.[1]

Whereas crimes of harm are intended as crimes whose material component is the criminal behavior that leads to an actual or future assault on the right or interest subject to criminal protection.[2]

The First Section: Dangerous Information Crimes

The dangerous information crimes are in which the criminal agreement, and according to what is found in Iraqi law, is that the material result is considered a necessary element in all crimes, as there are crimes in which the criminal legislator does not need to achieve a criminal result in order to complete it, as the material result is present as soon as the stipulated criminal behavior is present. On criminalizing it, and after that, the crime is realized, as it is called the term formal crimes, which are crimes that the legislator does not require that any result result from them, but it is enough just to commit the criminal behavior, as it is considered a complete crime, which is considered one of the crimes with basic behavior, and as for the crimes that are called dangerous crimes. This applies to forms of cybercrime that are achieved once the criminal behavior is committed, even if a specific material result is not achieved, but the legal result, represented by the danger, is sufficient.[3]

Section Two: Information Crimes That Cause Harm

The material result that occurs as a result of a damaging information crime is a necessary element in most crimes, as the Iraqi legislator requires for this crime to occur that there be a result, as the crime cannot be completed except when there is a result of the occurrence of this crime, which are called material crimes and damage crimes, as Most jurists mean it as a crime in which the law stipulates actual damages and a definite violation of the interest subject to criminal protection.[4]

Third Requirement: Pictures Of Cybercrimes

Section One: Computer Crimes

A crime committed via a computer is one of the types of crimes known in society, whether Iraqi, Emirati, or Qatari. In addition, it is very difficult for the criminal to stop at a certain point in his crime when he discovers that there is a way out of The system also considers computer crime to be the use of the computer as a means of commercial crime, through the practice of fraud, theft, extortion, and other types of crimes, and this is done through misuse of the computer.[5]

It can also be said, according to what is stated in the legislation of the Gulf countries, that cybercrime is an electronic activity that leads to harming others in a material or moral way through the use of the computer as the main tool, and at the same time the victim's computer is considered the subject of the crime.[6]

---

[1]Atiq Al-Sayyid, Explanation of the Penal Code, General Section, Part One, The Crime, Third Edition, Dar Al-Nahda Al-Arabiyya, Cairo, 2009, p. 52.

[2]Harm is defined as "disrupting, diminishing, or wasting the rights or interests protected by laws." It looks at:
Odeh Youssef Suleiman, The Crime of Targeting the Civil War Through the Media, first edition, Arab Center for Publishing, Cairo, 2018, p. 120.

[3], Taha Ahmed Hossam, Exposing others to danger in criminal law, a comparative study, Dar Al-Nahda Al-Arabiya, Cairo, 2004, p. 39.

[4]Hilali Abdullah Ahmed, Explanation of the Penal Code, General Section, first edition, Dar Al-Nahda Al-Arabiya, Cairo, 1998, 1987, p. 68.

[5]Al-Shaddi Tariq, Towards the Security Construction of Information Systems, Dar Al-Watan for Printing, Publishing and Information, Riyadh, 2000, p. 19.

[6]Al-Shehri Abdullah, Administrative Obstacles in Security Dealing with Computer Crimes, Master's thesis submitted to the College of Administrative Sciences, King Saud University, 2000, p. 30.

Section Two: Internet Crimes

Internet crimes, especially in the Emirates and Qatar, are many and varied, unlike Iraq, but Iraq is not as serious and severe as it is found in the rest of the countries of the world because these crimes are difficult to limit, but they are generally considered to include crimes committed against persons, crimes against money, and electronic commerce, and crimes committed by The Internet is closely linked to terrestrial sites, as happened in the incident of the British police, in cooperation with America and European countries, attacking terrestrial sites of institutions working in Internet prostitution.[1]

Section Three: Crimes Committed against Individuals

What is meant here by assault is insult, slander, defamation, and broadcasting ideas and news that would cause moral or moral harm to the person or entity in question. This is the variety of methods of assault, starting with entering the personal website of the defamed person and changing its contents. Thus, it falls under crimes that will be against the computer, networks, or the work of another website. Incorrect information, which falls under crimes, is published using computers and networks, which is often done through one of the free web page hosting sites, which have now numbered in the thousands in all countries connected to the Internet. One of the most famous sites is what happened on the Central Bank of Egypt's website on the Internet about approximately Three years ago, the attacker illegally accessed the server from which the site was broadcast, exploited one of its weak points, and changed the home page of the site, which caused confusion among those dealing with the bank, fearing that it had spread to other banking information and images. The other type of attack, which represents the attack on the intellectual property of names, is the attacks that occur on the names of Internet sites, as the global rule in registering domain names is that registration is based on precedence, not entitlement.[2]

Section Four: Crimes of Assault on Funds and Electronic Commerce

Due to an increase in the degree of dependence of banking and financial institutions on information and communications technology and the gradual transfer in all parts of the world to the term banks, banks and financial institutions, this development has witnessed the emergence of many electronic crimes, as at the level of banks and financial institutions the management and accounting systems and linking of the various branches have been reduced. These institutions interact with each other through the information network in order to ensure the ease and convenience of managing financial operations inside and outside them, as these institutions work with clients remotely and this matter is done through a direct communication method through private information networks that is not available to Internet users.[3]

Chapter Two: Elements of the Criminal Agreement in Cybercrimes

The First Section: The Legal Basis of the Criminal Agreement in Cybercrimes in Law

The First Requirement: in Iraqi Law

Cyberspace is defined as the metaphorical field of computer systems and electronic networks where information is stored electronically and direct communications take place via the

[1], Younis Omar Muhammad Abu Bakr, crimes arising from the use of the Internet, doctoral thesis submitted to Ain Al-Shams University, 2004, p. 231.
[2], Al-Jubouri Samer Salman Abd, previous source, p. 108
[3], Ibrahim Hosni Abdel Samie, previous source, p. 202.

international communications network known for short as the Internet, the use of which with electronic means has become inevitable at all levels and in all public and private circles or at the level of ordinary individuals. Because of the ease and speed it achieves in performing work and dealing with information, as is the case with applications for e-government, e-health, distance education, inquiries, e-commerce, and many others.[1]

The Second Requirement: in Qatari Law

The Qatari legislator issued a special system for combating cybercrimes, and among these crimes addressed by the Saudi system for combating cybercrimes was cybercrime. This system stipulates that: He shall be punished by imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand riyals, or by one of these two penalties. Every person who commits any of the following cyber crimes[2].

1, Unlawful entry to threaten or blackmail a person; To force him to do or abstain from doing an act, even if doing or abstaining from that act is lawful.
Private life by misusing camera-equipped mobile phones, or
2, Infringing on private life by misusing mobile phones equipped with a camera, or something similar.
3, defaming others, and harming them through various means of information technology."

The Third Requirement: in UAE Law

The United Arab Emirates has tended to issue special legislation and laws to combat cybercrime. It has issued the Anti-Information Technology Crimes Law, which sets the criminal and punitive framework for cybercrimes in its various forms. The crime of electronic extortion was one of those crimes that the legislator addressed with criminalization and punishment through this law, as it stipulated Article Sixteen of it stipulates that "Anyone who blackmails or threatens another person to force him to do or abstain from doing an act by using an information network shall be punished by imprisonment for a period not exceeding two years and a fine not less than two hundred and fifty thousand dirhams and not exceeding five hundred thousand dirhams, or by one of these two penalties." Or an information technology means, and the penalty shall be imprisonment for a period not exceeding ten years if the threat is to commit a felony or attribute matters dishonorable or disgraceful, as the previous texts represent the legal pillar of cybercrime in UAE law, through which the judge can punish the perpetrators in all forms of these crimes. Through these texts that set the framework for criminalization and punishment for that crime [3].

The Second Section: The Material Element of the Crime of Cybercriminal Agreement

The UAE ranked eighth globally and first regionally on the list of countries most exposed to electronic attacks. The country also ranked 41st globally in terms of electronic security threats, up from 49th in 2014, according to the 21st edition of security threats by Symantec, the global company specializing in information security solutions, and building... According to this report, the ranking of the UAE with regard to its exposure to electronic security threats during the year 2015 changed rapidly, as the country ranked 41st after it was ranked 49th during the year

[1] Al-Jubouri Samer Salman Abd, previous source, p. 108
[2]Ahmed Kilan Abdullah, Muhammad Jabbar Anwa al-Nasrawi, Criminal Justice in Explanation of Criminalization and Punishment, Kufa Journal of Legal and Political Sciences, Volume (12), Issue (41), 2019, p. 10.

[3]https://almerja.com/reading.php?idm=187850

2014, and this shift indicates a global high percentage of security threats based on sources, including This includes malware, unwanted e-mail messages, phishing attacks, attacks on websites and networks, and independent software in the country. Perhaps the most prominent reasons for this are that the UAE is a pivotal gateway to the Middle East region, and enjoys a world-class infrastructure for information and communication technology and an attractive work environment for investments. Which makes it a commercial center for a large number of international companies.[1]

The First Requirement: Elements of the Material Pillar

The material element in the crime consists of three elements: It is criminal behavior, its result, and the causal link between them. Criminal behavior consists of two parts: The first is a voluntary activity, and the second is the location on which this activity is focused. As for criminal behavior, it is a specific act required by law that is subject to punishment for this crime provided that a harmful result of this criminal behavior is achieved as a condition in itself that must be punished for the crime, in addition to the connection between the criminal activity or behavior and its result. The crime does not exist except through a legislative text that criminalizes the criminal act and imposes a penalty on it. The result of this is that the Penal Code specifies in advance the actions that it considers to be known crimes and the penalties imposed on their perpetrators. An information crime is no different from Ordinary crimes, where the presence of criminal behavior is required to be criminalized by law. Criminal behavior in information crime can be defined as every act or abstention from action that leads to damage to information stored on a computer, which leads to wasting or reducing the value of the information and causing harm to others. Ordinary criminal behavior in this Crimes must be committed through computers or the Internet.[2]

The First Section: The Criminal Behavior of the Crime of Cybercriminal Agreement

The constitutional legislator guaranteed the human right to freedom of correspondence and conversations. Article (39) of the Constitution stipulates that "the freedom of postal, telegraphic, and telephone correspondence is safeguarded, and its confidentiality is guaranteed. It is not permissible to monitor messages or divulge their confidentiality except in the circumstances specified in the law and in the procedures stipulated therein." The UAE constitutional legislator also did the same, as Article (31) of the Federal Constitution of the United Arab Emirates stipulated that "the freedom and confidentiality of postal and telegraphic correspondence and other means of communication are guaranteed in accordance with the law." Hence, it was necessary for the ordinary legislator to keep this constitutional protection in mind, so he decided, in addition to the substantive criminal protection that we presented above, procedural criminal protection, including the provisions of the Code of Criminal Procedure in both countries. This protection was embodied in more than one form, including: the inadmissibility of monitoring conversations. And phone calls except after obtaining permission from the investigating authority, and also excluding evidence derived from audio recordings of conversations or phone calls that took place without the permission of the investigating authority. We present these two images, each in a separate request, then we conclude the study with a special request in which we address the balance between violating the right to privacy of calls. Telephony and the protection of society, whether this protection

[1]Ismail Abdel Rahman, The UAE is the first regionally in terms of exposure to electronic attacks, published in Al-Ittihad newspaper on 04/18/2016.

[2]Abdullah Kariri, The Moral Corner, in Information Crimes in the Saudi Regime - A Original Study (Master's Thesis, Riyadh: Naif Arab University for Security Sciences, 2013, pp. 40,41).

is embodied in ensuring the interest of investigating a crime committed, or in protecting national security in the face of some internal or external dangers.[1]

The Second Section: The Result and the Causal Relationship

Article 25 of Law No. 175 of 2018 regarding combating information technology crimes. What is the point? The reference is to know the truth of the information and news and the extent to which it relates to the private life of the victim and its violation of his privacy without his consent. Objective. How much is that? Investigate the truth of the news and the extent to which it relates to the private life of the victim. Legal adaptation subject to the supervision of the Court of Cassation. Why is that? The post attributed to the appellant, which he wrote and posted on Facebook, did not include anything that would affect the private life of the victim or violate his privacy without his consent and his encounter with an incident regarding which a report was written. Its effect: Not being punished under Article 25 of Law 175 of 2018 regarding combating information technology crimes. The ruling contradicts this view. Misapplying the law. It must be overturned and acquitted.[2]

The Second Requirement: Issues Related to the Material Aspect

Section One: Criminal Contribution to Cybercriminal Agreement Crimes

The Iraqi legislator dealt with the crime of threat within the framework of Articles (430, 433). As for the crime of extortion, he did not single out a specific text for it or address it explicitly, but rather implicitly stipulated the threat associated with a request in Article (430).[3]From the Penal Code No. 111 of 1969, as amended; It is noted from extrapolating the aforementioned text that the Iraqi legislator intended to use broad phrases regarding the means of committing the crime of threat, whether the threat is abstract or accompanied by a request. We note that the first paragraph of Article (430) did not specify a specific means, but rather used the phrase (everyone who threatens another... .), and thus it is valid in this case for the threat to be made accompanied by a request by any means; Therefore, it is equal to commit the crime of a threat associated with a request through a traditional means or an electronic means (such as e-mail, chat rooms, ...), based on the generality and absoluteness that was stated in the wording of the previous paragraph. The absolute text applies to its absoluteness unless there is a text to the contrary, and we see that This punishment is insufficient to confront the crime of blackmail, especially if it is committed electronically, and especially given the ease with which it is committed, its spread, and the difficulty of proving it. One of the most important effects that results from the causal link between a crimewiseElectronic blackmail and the punishment prescribed for it (considering that the second is the social reaction to the crime and its perpetrator) there is a necessity for there to be proportionality between the amount of the punishment on the one hand, and the gravity of the crime and the effects it generated on the other hand, and this necessity is a logical consequence of a main purpose of the punishment, which is (to achieve Justice), which requires that the punishment be satisfactory to the feeling of justice, and it is not so unless it is proportionate to the gravity of the crime, considering that

[1]Ghanam Al-Quwari, General Principles in the Federal Criminal Procedure Code of the United Arab Emirates, 2nd edition, Al-Emirates, Bright Horizons, pp. 163,168

[2]The updated principles issued by the criminal chambers of the Court of Cassation, Technical Office, Criminal Group, 2020/2021.

[3]See Article 430 of the Iraqi Penal Code No. 111 of 1969, which states:

1 - Anyone who threatens another person to commit a felony against himself or his property, or against the life or property of another, or to attribute or disclose matters that are dishonorable, and this is accompanied by a request or commission to do something, or refraining from an act, or intending to do so, shall be punished by imprisonment for a period not exceeding seven years or by imprisonment. .

2 - The threat shall be punished with the same penalty if the threat is in a letter devoid of the sender's name or if its issuance is attributed to an existing or alleged secret group.

this punishment is the just punishment for this crime, such that it is neither exaggerated in its severity nor lenient in it.[1]

Section Two: Attempting Cybercrime

The Iraqi judiciary did not stand idly by in the face of a crime when there was no legislative text punishing this despicable act. It also missed the opportunity due to the legislative vacuum, or to adhere to the rule (no crime and no punishment except by a text), as our judiciary had a decisive role in addressing this defect and passing judgment on me. Blackmailer perpetrators according to the legal provisions mentioned above. By following the judicial authority's website, we were able to find a set of judicial decisions related to many electronic blackmail crimes, according to the following:

1, The Al-Karkh Investigation Court, which specializes in terrorism cases, under the chairmanship of the Baghdad Al-Karkh Federal Court of Appeal, ratified the confessions of members of a network specialized in hacking social media sites, by taking pictures and copies of electronic conversations, bargaining with their owners, and threatening to publish them on the sites when payment is not made, with the intention of defamation and blackmail, and legal measures have been taken. against the accused and refer them to the competent court in accordance with the provisions of Article (430) of the Penal Code."

2, sentencing two defendants accused of blackmailing a girl. They were both those who carried out the luring operation under the pretext of marriage and those who photographed them red-handed by ambushing them when the gold jewelry was handed over by the victim. They confessed to the crime committed in detail, and the competent court sentenced them to temporary imprisonment for seven years. According to the provisions of Article 430 of the Penal Code, this is a crime of threatening to disclose matters that offend the honor of the victim, accompanied by a request for sums of money and gold jewelry.

3, The Al-Karkh Investigation Court, under the presidency of the Baghdad Al-Karkh Federal Court of Appeal, ratified the confessions of an accused who claimed to be a "electronic blackmail warrior," but he blackmailed girls through social networking sites and threatened them, while the court ratified the confessions of another accused who blackmailed a minor girl in exchange for sums of money, where the competent court decided All legal procedures will be taken against them in accordance with the provisions of Article (456) of the Penal Code."

4, recording the confessions of an experienced hacker who blackmailed many subscribers to the social networking program (Telegram) by hacking their accounts, accessing personal data, withdrawing photos, and then requesting sums of money and credit cards of a large value for a fair trial in the court of law, after he shook several families through a method It was cheap to threaten to publish their privacy on social media sites, and the Basra Investigation Court stated that other victims had filed several complaints showing similar methods of blackmailing them, with the same mechanism and requesting cash amounts in the form of a card, and that the perpetrator would be punished by law, the type of crime committed and the legal matter.

5, In implementation of this, the Najaf Criminal Court stated in one of its decisions that "he is the accused (B.M.A.) in accordance with the provisions of Article (1/430) Penalties, for the crime of threatening the female complainants (A.K) and (H.A.Y)." By publishing video clips of them accompanied by a request for sums of money from them,and versityHe was sentenced to 7 years in prison, including the period of his honor, and the court did not award civil compensation to the complainants because they dropped the complaint...)[2]

[1]Sami Abdul Karim Mahmoud, Criminal Penalty, 1st edition, Al-Halabi Publications, Beirut 2010, p. 31.
[2]Resolution No. 8/C/2018 dated 12/12/2018. Unpublished

6, In other cases, some courts apply the provisions of Article (452) of the Penal Code to some incidents of extortion, which stipulates that (a penalty of imprisonment for a period not exceeding seven years or imprisonment shall be imposed on whoever forces another person, by threat, to hand over money or other items other than those mentioned in Article One of the judicial applications of this is what the Central Criminal Court (Second Circuit) ruled in its decision (The Central Criminal Court decided to convict the accused (A.A.F.) in accordance with the provisions of Article (452) of the Penal Code, due to the sufficiency of the evidence obtained against him. On 3/3/2018, in conjunction with defendants whose cases were separate, he threatened the complainant (H.R.H) and blackmailed her into paying sums of money in exchange for not publishing her photos on social media sites, and sentenced him to severe imprisonment for a period of three years, counting the period of his detention, and giving the complainant the right to demand with compensation...) It is noteworthy that the Federal Court of Cassation ratified the aforementioned decision."[1]

The Third Requirement: The Material Element of the Law

The First Section: The Material Element of Cybercrime in Iraqi Law

According to the Iraqi legislator, the crime of threatening (which the Iraqi judiciary considered electronic blackmail) is considered a dangerous crime, for which it is sufficient for the perpetrator to merely commit criminal behavior represented by the act of threatening. This appears from the fact that the legislator made the crime of threatening a crime that affects human freedom and sanctity. These are the crimes dealt with by the legislator in Chapter Two of the Iraqi Penal Code. Therefore, criminal responsibility is achieved once the behavior criminalized by the text of the law is committed without searching for the verification of the result. Therefore, there is no need to look for proof of the causal relationship between the behavior and the result, and this appears through the text of Article (430).) of the Iraqi Penal Code, which stipulates that: "Anyone who threatens another to commit a felony against himself or his property, or against the life or property of another, or to attribute or disclose matters that are offensive to honor, or disclose them, and this is accompanied by a request or commission shall be punished with imprisonment for a period not exceeding seven years or imprisonment." "By ordering or abstaining from an act or intending to do so."

Section Two: The Material Element of Cybercrime in Qatari Law

We note that the Qatari legislator has expanded the scope of persons who have the right to take action, as Article (87) granted it to the investigator, and by referring to the Qatari Code of Criminal Procedure, we find it distinguishes between felonies and misdemeanors in determining the person of the investigator or who has the authority to investigate. The first paragraph of Article (9) was assigned to (Qatari Criminal Procedures) The task of investigating felonies is for the Public Prosecution, while the second paragraph of the same article assigns it in misdemeanors to persons appointed for this purpose from the Department of Police and Public Security. The same article also grants the status of investigator to police officers who are appointed by the internal regulations stipulated in Article (38). ([2])From the same law, the last paragraph of Article (9) also gives the Public Prosecution the right to entrust the investigation of the crime to officers from the police department. Accordingly, the Qatari legislator has expanded the scope of persons who conduct investigations into crimes, making it the responsibility of the Public Prosecution in felonies, and of police officers and others in

[1]Resolution No. 20212 / Criminal Authority / 2018 dated 1/16/2019 unpublished
(2) Article 38 of the Qatari Code of Criminal Procedure

misdemeanors, and even in felonies as well if the Public Prosecution entrusts them with that, while we find that the Emirati legislator limited the direct investigation and accusation to the Public Prosecution. In all crimes without discrimination. He delegates one of the judges of the court of first instance upon the request of the Public Prosecution. He also did not grant the Public Prosecution the authority to monitor or register except after obtaining in advance a reasoned order from the district judge after reviewing the papers. Accordingly, the procedure is invalid if it is carried out based on her direct permission.

Section Three: The Material Element of Cybercrime in UAE Law

As for the UAE Penal Code, it did not fully specify the elements of the material element, but rather was limited to mentioning one of its elements, which is the act. Article No. 31 of it stipulates that "The material element of the crime consists of procedural activity by committing an act or abstaining from an act when this commission or Abstaining is legally binding, and according to this text, the material element is the realization of a criminal activity."[1]
As for the crime that we are dealing with, it is the crime stipulated in the law as stated in Article No. 10 of Federal Decree Law No. 5 of 2012 AD regarding combating information technology crimes, and the criminal behavior that occurs here is e-mail, which means written or transmitted documentary correspondence. Behind him or Otherwise, it is sent and received through an electronic postal communication system, and film materials or electronic documents can be added to be attached to the message, and the importance of e-mail appears in its advantages; The most prominent of which is: high speed. This is the most important feature of e-mail, which is the ability to send messages to anyone in the world at high speed, in addition to the fact that it can be opened anywhere in the world. When an e-mail was created, its owner can access the mail anywhere in the year where there is a network. Internet.[2]

The Third Topic: The Moral Element in Cybercrimes

The concept of cyber attacks still faces significant differences, which has led to a dilemma and a greater challenge facing specialists in international law. This is embodied in the adaptation of cyber attacks, as well as research into the source and basis of the adaptation. Do we find it in the principles of general international law or the principles and rules applied in international humanitarian law?? The dilemma will be great if it is recognized that there is a legal vacuum, the absence of specific legal rules that regulate cyber attacks, which raises the following question: What are the applicable rules? Especially since the scope of their use increases day by day and their dangers loom on the horizon, threatening international peace and security, and by reviewing the opinions of specialists related to the subject of the study, this challenge is indicated, as some of them believe that the principles and rules established by international humanitarian law apply to these attacks.[3]

The First Requirement: The Moral Element of the Crime of Cybercriminal Agreement

The legal conditioning of cyber warfare consists of clarifying the extent to which the nature of war is recognized or denied, and the conditioning of cyber warfare revolves around two hypotheses: The first is denying the nature of war in cyber warfare as a result of the inability to prove the physical evidence resulting from the use of cyber attacks, which is the greatest obstacle facing specialists, unlike... Methods and means of conventional warfare, known by

[1]Muhammad Shalal Al-Ani, Provisions of Oaths in the UAE Federal Penal Code - The General Theory of Crime (Sharjah: Bright Horizons, 2010), 1st edition, p. 196
[2]Abdel Hamid Bassiouni, Computer License - Information and Communications (Cairo, Dar Al-Kutub Al-Ilmiyyah, 2009), 1st edition, pp. 58,59.
[3]Noura Shaloush, Electronic Piracy in Cyberspace, p. 190

their methods, which leave a tangible, direct or indirect material effect after the attack, such as the partial or total destruction or disabling of military or civilian objects, or the killing or wounding of fighters or civilians. As for the second hypothesis, it is the opposite if it is proven that cyber attacks It may lead to tangible material effects on all economic, security and military levels, so it is considered a war.[1]

The Second Requirement: The Moral Element of Cybercrime in the Law

The First Section: In Iraqi Law

In Iraqi law, it means the perpetrator's awareness at the time of committing the physical act constituting the crime that saying or writing it would cause discomfort to the victim. It was translated as a threat accompanied by a request or assignment to do something. It is not required that the blackmailer's goal be to achieve the thing threatened, because the mere threat is a crime in itself and is punishable by law because it causes discomfort to the victim and affects his psyche. The moral element is a mental and psychological course for the offender, as it provides the elements for establishing immediate responsibility, taking into account The state has the right to punish that is based primarily on the pleasure, these elements. The threat must be serious enough to make the person intended believe that it will come true, such that this threat would have an impact on the soul of the victim. It is also noted that the moral element of the crime of extortion must be directed towards it. The offender's will to commit the act that constitutes the material element of the crime, while knowing that he is committing a crime punishable by law. For the offender's will to be considered, this means that it must be free and distinct. In other words, the moral element of the crime is achieved in the criminal intent of the blackmailer, that is, his will and knowledge were directed to threatening the victim with the information or images he possesses and blackmailing her, or exploiting them, which represents an assault on the sanctity of her private life.[2]

Section Two: In Qatari law

It is intended with the moral pillar of the crime of intentional or error according to Article No. 38 of the laws of the conjugation penalties, so the mayor is the direction of the perpetrator's intention to commit the act or abstinence that we were lawful criminals, due to the direct result or result of the last criminal that the perpetrator expects, as well as the reason for the cause between the behavior and the result, With the existence of this relationship, the material element of this crime is complete. In this crime, there must be a causal relationship between sending spam messages and the consequences resulting from this behavior, which are specified by the text of the decree to stop or disable e-mail, or destroy, erase, delete, destroy, or change data or information.[3]

Section Three: in UAE Law

We believe that the crime under study is an intentional crime for which the law requires the presence of criminal intent in the elements of knowledge and will, meaning that the offender knows the nature of his act, whether it takes the form of copying, disclosing, or distributing. He also knows the location of the crime and that it is a phone call or message belonging to another person, and finally he knows that his act It represents an assault on the right of others to privacy, meaning that there is no legal basis or justification that gives him the right to copy,

[1]Hamdoun Tarwiyeh, The International Response to Cyber Warfare, p. 44
[2]Dr. Ali Jabbar, Internet and Computer Crimes, Al-Yazouri Scientific Publishing House, Amman, Jordan, p. 31
[3]Abdul Latif, Explanation of the Information Technology Crimes Law, p. 111

disclose, or distribute the communication. Therefore, the crime does not occur if the perpetrator believes in the existence of that document, as if he believed that permission had been issued to him by the investigation authority, or the authority. General purpose of the telecommunications sector. Criminal intent also requires that the offender direct his will to commit the act and achieve the result by reaching the content of the call or telephone message to others. But the matter becomes more nuanced and becomes more complicated because of what was raised about the text of Article (43) of federal penalties, which makes the offender responsible for his crime, whether he committed it intentionally or accidentally, unless the intentional law stipulates its frankness, which is what the Emirati legislator did not do in Article (72) of the Decree-Law. This What raises controversy is the extent to which the crime under study occurred unintentionally, that is, by mistake, as stipulated in the Penal Code (Article 38 Penalties).[1]

Chapter Three: The Criminal Effects of the Agreement on Cybercrimes

The First Section: Penalties Imposed According to Iraqi Law

In this study, we will present two requirements. In the first, we will present the penalties for cybercrimes, and in the second, we will present the aggravating circumstances for cybercrimes:

The First Requirement: Penalties for Cybercrimes

Given that cybercrime is one of the new crimes in the Iraqi criminal law, for which the legislator has not allocated its own legal texts, therefore, the legal texts that currently address issues related to this crime are the punitive texts for the crime of threatening within the amended Iraqi Penal Code No. 111 of 1961 (2).

The Requirement the Second Aggravating Circumstances for Cyber Crimes

Cybercrime has cases where the punishment may be severed, if certain conditions are met, which the legislator sees and has previously included in the system. There are also cases in which the perpetrator is exempted from punishment due to the availability of circumstances in which the system decided that there is a higher interest in deciding to exempt the perpetrator, and that by exempting him, it is achieved. A greater interest, according to the criminal policy that each legislator sees, and we will discuss these points in two sections as follows:

There are cases in which the penalty is aggravated if the crime of electronic blackmail is committed. What is meant by aggravation here is for the judge to rule the maximum limit of the prescribed penalty or to issue both penalties, i.e. imprisonment and a fine together.

The legislator stipulated the tightening of the penalty for the crime of electronic blackmail, and specified the cases in which the judge must, if presented to him, tighten the penalty. It was stated in Article Eight: "The penalty of imprisonment or a fine shall not be less than half of its maximum limit if the crime is accompanied by any of the following cases."

The perpetrator committed the crime through an organized gang.[3].

The perpetrator held a public job and the crime was connected to this job or he committed the crime by exploiting his authority and influence.

---

[1]Abdel Khaleq, The General Theory of the Crime of Disclosing Secrets, in Comparative Criminal Legislation, Egypt, Doctoral Thesis, Ain Shams University, pp. 650, 670

(2) Jamil Abdel Baqi Al-Safir, book on procedural aspects related to the Internet, Dar Al-Nahda Al-Arabiyya, 2002 edition, p. 72.

(3) Muhammad Salem, Crimes against reputation through electronic information technology, King Saud University Libraries, Riyadh, 2014, p. 68.

Deception and exploitation of minors and those under their authority

Issuance of previous local or foreign judgments convicting the perpetrator of similar crimes.

Where the judge has the right, through the text of the law, to increase the punishment against the offender in the previous cases above, or to punish him by half the period stipulated in the text of the law, and it becomes clear to us that the legislator is keen in the aforementioned cases to tighten the punishment by combining imprisonment and a fine, or for the punishment not to be less than half, since committing The perpetrator is punished through a criminal organization, as the legislator perceives a danger to society that this crime will spread, as a result of its practice by an organized structure such as organized criminal gangs. The punishment should also be increased if it is committed by a public employee, since he is supposed to be a carefully selected person and in whom the state's trust is placed, so the state's trust must be placed. He must be far from any suspicion, so if he commits a crime like this, he is entitled to aggravated punishment. It is also necessary for the aggravated punishment to be related to blackmail and deceit of minors, and for the crime to occur against a group entitled to criminal protection to a greater extent than other groups. The issuance of previous local or foreign sentences is also considered a reason for aggravation. against the blackmailer in similar crimes, and it seems that the reason for this aggravation is due to the same idea of aggravation in the event of recidivism or criminal seriousness [1].

The Second Section: Penalties Imposed According to UAE Law

In this topic, we will present two requirements. In the first requirement, we will present the penalties for crimes of assault on the state and public order. In the second requirement, we will present the penalties for crimes of assault on individuals. In the third requirement: the judicial rulings related to the criminal agreement for cybercrime:

The First Requirement: Penalties for Crimes of Assault Against the State and Public Order

It is known that the legislator, while in the process of criminalizing behavior that puts into its considerations, society, is trying to protect it in the language of punishment, and information crime is a type of behavior that the offender commits and attacks interests that the legislator deems worthy of criminal protection, and there are a number of reasons behind criminalizing the actions that lead to them. The most important of these crimes is the failure of technical means to provide protection for the interests that are achieved using information technology. No matter how much effort a person makes to protect his technical products and information and tries to make them secret, the matter is not difficult if one of the IT specialists wants to pass through these walls (fortification).) And he gets what he wants from the programs and information.

Then, the capital required to create programs and other information technology is very large amounts of money. If these programs are undermined, this will cause a waste of wealth and the efforts of workers, in addition to the fact that the matter will be a reason for the fear of capital owners, which will force them to withdraw from these giant projects or Choosing other outlets to exploit this money. On the third hand, cybercrimes are dangerous beyond measure in size or number because they attack a huge amount of information of economic value. Cybercrimes, as some see, are[2].

---

[1] Same source, p. 80.

[2] Ahmed, Abdul Rahman Tawfiq, Explanation of the Penal Code, General Section, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2011, p. 34.

The Second Requirement: Penalties for Crimes of Assault on Individuals

After looking at the legal texts that address social media information crimes contained in Federal Decree Law No. (5) of 2012 regarding combating information technology crimes and the amendments that were made to some of its articles, it is worth reviewing the most prominent articles related to crimes of assault on individuals. (1):

First: Article (20) of Federal Decree Law No. (5) of 2012 regarding combating information technology crimes stipulates that: Without prejudice to the provisions of the crime of defamation stipulated in Islamic law. Anyone who insults another or attributes a fact to him that would make him subject to punishment or contempt by others shall be punished by imprisonment and a fine not less than two hundred and fifty thousand dirhams and not exceeding five hundred thousand dirhams, or by one of these two penalties, by using an information network or an information technology means. If this occurs Insulting or slandering a public employee or someone charged with a public service on an occasion. Because of his performance of his work, this is considered an aggravating circumstance for the crime."

Defamation in Islamic law means accusing others of obscenity, and it is one of the hudud crimes in Islamic law. The evidence that is proven by it is acknowledgment or testimony, and confession is one of the strongest arguments. If the defendant admits to defamation, his admission is challenged and the legal punishment for defamation is applied to him. As for testimony, it is required to have two practical witnesses, so it is not accepted. The testimony of women is a precaution for honor, because it is a hudud crime, and because this crime is something that men know about, it is proven by their testimony.

Accordingly, if the conditions for the legitimate crime of defamation are met, then this article does not apply. Rather, the punishment of defamation is applied to the perpetrator of the legitimate crime of defamation. However, other than normal insult through social media, other information networks, or an information technology means such as a smart phone, for example, the penalty for a misdemeanor is applied to its perpetrator, which is either Imprisonment and a fine of not less than two hundred and fifty thousand dirhams and not exceeding five hundred thousand dirhams, or one of these two penalties, with a note that insulting or defaming a public employee or person charged with a public service on the occasion of or because of the performance of his work through an information social media means or other information networks or technical means. Information such as computers, for example, is still an aggravating circumstance for the crime.2).

The Third Requirement: Judicial Rulings Related to the Criminal Agreement for Cybercrime

First: The crime subject to the sentence: an assault on the victim's bodily integrity and then incapacitating her for a period of more than twenty days, an assault on the victim's privacy. She was victimized with words that insulted her honor

Second: The facts[3]

The incident is that the accused filmed the complainant (who is his wife) via WhatsApp and sent the clip to the complainant's father with the intention of proving her daughter's behavior

(1) Samir Ibrahim Jamil Al-Azzawi - Criminal liability arising from misuse of the Internet - Master's thesis submitted to the University of Baghdad - 2005, p. 96.
(2) Ibrahim Al-Majid - The most important means and methods of fraud, fraud and deception via the Internet - published in Al-Jazeera newspaper - Issue - 58 of 2004 - p. 1.
(3) Al-Qahtani, Abdullah bin Hussein Al Hajraf, Developing criminal investigation skills in confronting electronic crime, College of Police Sciences, Naif Arab University for Minimal Sciences, Riyadh, 2014, pp. 61, 60, 59.

and not with the intention of showing it to others, and he did not show it to anyone other than her mother.

The Third Section: Penalties Imposed According to Qatari Law

In this section, we will present several demands, including: In the first requirement: the precautionary nature of cybercrimes, in the second requirement: aggravating circumstances for cybercrime, in the third requirement: subsidiary penalties, while in the fourth requirement: exemption from punishment:

The First Requirement: The Precautionary Nature of Cybercrimes

In legislation, no special legislation has been singled out to deal with this type of crime, while there are legislations and in other countries that are satisfied with the traditional texts in their laws to deal with this type of crime, as they have adapted their traditional texts to punish the perpetrators of this type of crime 140, and the first type is called the method Special legislation, while the other type is called the listing method, and among the foreign countries that followed the listing method are the French legislator, in Article No. (1/323) to 7 of the Penal Code, as well as the German legislator, which dealt with electronic crimes in Chapter 2002/A, C of the Penal Code 14, and among the Arab legislations that some have suggested is the method of inclusion in the Penal Code, the Algerian legislator, in Chapter Three, specifically Section Seven, bis, under the title of violating automated data processing systems, in Article (394) bis to Article (394) bis 1407. Among the foreign countries that have adopted special legislation to confront this type of crime are the English Computer Misuse Act of 1990 and the United States Computer Fraud and Misuse Act. Among the Arab countries that have issued special legislation to confront this type of crime are the Omani Information Technology Crimes Law of 2011, as well as The Kuwaiti Information Technology Crimes Law of 2015, and the Jordanian Cybercrimes Law of 1452015. Referring to the Qatari legislator, we find that it had previously followed the inclusion method, as it included in Chapter Five of the Penal Code a chapter entitled "Computer Crimes." It dealt with electronic crimes in the direction of the Qatari legislator. To the method of special legislation, where legislation has been singled out to punish this type of crime, which is the Anti-Cybercrime Law 14, due to the inability to cover all forms of cybercrimes and for fear of the rule that special legislation has priority in application over general legislation. Most of the legislations that have singled out special texts to confront them Cybercrimes have taken on a precautionary nature in cybercrime legislation, such that if there is a more severe penalty prescribed in other legislation, then it is the one that can be tolerated. Accordingly, cybercrime legislation becomes general in this scenario, so as not to tolerate a lighter spontaneity mentioned in a special text 14. The legislation that stipulates the precautionary nature of penalties is the Al-Ghammani Law on Combating Information Technology Crimes, where Article No. (35) of it stipulates that the penalties stipulated in this law shall not prejudice any more severe punishment stipulated in another law, as well as the Qatari legislator in combating electronic crimes, as Article No. No. (44) of it stating that, without prejudice to any penalty stipulated in the Penal Code or any other law, the perpetrators of crimes punishable under the provisions of this law shall be punished with the penalties stipulated therein? 140, and accordingly the goal comes. The purpose of the precautionary nature of punishments in cybercrime legislation is to prevent perpetrators from getting rid of the lesser punishment and to ensure that they are punished for the crime with the harshest punishment possible. This is also consistent with the rule of moral plurality of crimes, according to which a person commits an act of indecency in the Penal Code or in any other

penal law. This act applies. This text applies to the Anti-Cybercrime Law unless there is a more severe penalty in another law [1].

The Second Requirement: Aggravating Circumstances for Cybercrime

Since comparative legislation stipulates that for the crime of illegal entry entry, a simple penalty is imposed if the crime stops at the point of entry, and the penalty is aggravated if the entry results in a specific result or the entry is for the purpose of achieving a specific goal, whether this goal is achieved or not, some legislation tightens the penalty for the crime if committed by employees responsible for those systems.

The court, in accordance with the rules of moral pluralism, will apply the most severe punishment to him. However, the Qatari legislator, in fact, after stipulating the provisional status in Article No. (44) of the Anti-Cybercrime Law, we find that it has stipulated in Article Four of the articles of the issuance of the same law. However, it repeals every provision that contravenes the provisions of this attached law. Accordingly, the important question that must be answered is whether the computer crimes stipulated in the Penal Code are repealed in accordance with the provisions of this last article? Or is it still valid, and the judge must apply it if it imposes a more severe punishment? It carries a more severe penalty and does not violate the provisions of the articles contained in the Anti-Cybercrime Law, except that the crime of illegal entry mentioned in the Anti-Cybercrime Law is considered the same as the provisions contained in the Penal Code, and with regard to electronic crimes it is considered a subject of application [2].

The Third Requirement: Subsidiary Penalties

The legislation that punishes cybercrimes stipulates, in addition to the original penalties, secondary penalties. Secondary penalties are of two types, either accessory or supplementary. Accessory penalties are those penalties that follow the ruling with an original penalty and by the force of the law and do not require that they be pronounced in the ruling. As for the supplementary penalties. They are those penalties that the court pronounces in addition to another original penalty. 170 Complementary penalties may be complementary and existential or may be complementary permissible. The Qatari legislator has specified a definition for each of them, saying that the penalty is accessory if the law excludes it as an effect of the ruling with the original penalty, and it is the penalty is complementary, if its imposition depends on the judge's ruling, whether the law obliges him to do so or permits it.

Section One: Deportation

Deportation means the residence of the foreigner in the State of Qatar and his deportation to the country to which he belongs, by virtue of its goal of reducing the criminal danger resulting from the presence of the offender within the territory of the country by removing him from the country and deporting him. In addition to that, deportation is only for foreigners, and therefore the citizen may not be deported from his country or prevent him from returning to her.

Given the nature of cybercrimes, some legislators were required to stipulate the penalty of deportation, especially countries that attract the foreign issue, such as the Arab Gulf countries,

[1] Salma Ihab, Specialists: The violations of the electronic press and "social media" require a law, Bahraini newspaper Al-Watan, March 23, 2013, available at the link: http://www.alwatannews.ne
[2] Muhammad Amin Al-Rumi, previous source, p. 89.

where the foreigner poses a threat to the electronic system, especially since the foreigner who commits a cybercrime is subject to the law of the country, so he deserves such a penalty, and deportation may be a complementary, permissible penalty. It may be an obligatory complementary punishment.[1].

Section Two: Penalty of Confiscation and Closure

Some legislation has imposed the penalty of confiscating items used in committing the crime and closing the place where the crime was committed on cybercrime perpetrators, including the crime of illegal entry as a supplementary permissible or obligatory reinforcement, as we will see. Confiscation means that property is expropriated in order to prove its connection to the crime and is added to state property without Opposite 17, general and private confiscation and general confiscation. On all of a person's money, which is limited by the text of the Constitution, while private confiscation is that which applies to specific money and is only by a judicial ruling and in the cases specified in Law 17, and the penalty of closure means that it is prohibited to carry out a specific activity in a place that takes the status of a public place.[2].

Fourth Requirement: Exemption From Punishment

Some legislation stipulates the possibility of exemption from punishment upon reporting the commission of a cybercrime, including the crime of illegal entry. This legislative policy undoubtedly helps in combating this type of crime and leads to encouraging perpetrators to report it and giving them an opportunity to escape punishment, even after committing the crime. However, although some legislations have stipulated the possibility of exemption from punishment in the event of reporting, they have differed in the limits of those controls, according to which the perpetrator can escape punishment, while there are legislations that have not stipulated the possibility of exemption from punishment in the event of reporting in legislation. Concerning cybercrimes, such as Jordanian and Bahraini legislation. Among the Arab legislations that stipulate the possibility of exemption from punishment upon reporting them is the Kuwaiti Law on Combating Information Technology Crimes, as it stipulates in Article No. (12) of it that the court may exempt from punishment any of the perpetrators who takes the initiative to inform the authorities. The person responsible for the crime before she knew about it and before the crime was carried out. If the reporting was after learning about the crime and before the investigation. In order to be exempt from the penalty, the report must be able to arrest the rest of the perpetrators in the event that they are multiple. It should be noted that the Kuwaiti legislator stipulates that in order to be exempt from the penalty, the crime must be reported before the authorities become aware of it and before the crime begins to be carried out, and in the event that the crime is reported after the competent authorities become aware of it. Thus, in order to be exempt from the penalty, reporting must be made before investigating the crime, and this reporting must lead to the disciplinary action of the remaining perpetrators in the event that they are multiple. It is noted that the Kuwaiti legislator notes that if these controls are met, then this remains subject to the discretion of the court, as the wording of the text states that the court may be exempted from the penalty. Therefore, if these controls specified in the aforementioned article are met, this will not be obligatory for the court, but rather it will remain subject to the court's discretion. Among the Arab legislations, you also said that it stipulates the possibility of exemption from punishment upon

(1) Fahd bin Mubarak, Incitement to Crime in Jurisprudence and the Saudi System, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, 2006, p. 34.
(2) Muhammad Salem, Crimes against reputation through electronic information technology, King Saud University Libraries, Riyadh, 2014, p. 68.

reporting it. The Omani legislator in the law on combating information technology crimes, as it stipulated in Article No. (33) of it that it exempts from punishment any of the perpetrators or their companies who took the initiative to inform the authorities. The person concerned with information about a crime committed in violation of the provisions of this law before its disclosure. If that information is provided after its disclosure, the court may exempt him from punishment, provided that providing it results in the arrest of the rest of the perpetrators. It is noted that the Omani legislator has stipulated that he must be exempted from punishment in the event that it is reported. About the crime before it was revealed, and the court was given permissible authority to exempt from punishment if information was provided about the crime after it was revealed, and that statement led to the arrest of the remaining perpetrators.

Returning to the Qatari legislator, we find that it has also stipulated the possibility of exemption from punishment in the event of reporting electronic crimes, including, of course, the crime of illegal entry, as it stipulated in Article No. (54) of the Anti-Cybercrime Law that it is exempt from the penalties stipulated in This law applies to any perpetrator who took the initiative to inform the competent authorities of any information about the crime or the persons involved in it, and that the authorities knew about it before the incident occurred, and led to the arrest of the rest of the year 1986. It is noted that the Qatari legislator has made it obligatory to exempt from punishment in the event that notification is made. Authorities provide any information about the crime and the persons harmed, and the court may order a stay of execution[1]The penalty, if the notification occurs after the authorities know about the participants, before they become aware of it and before the damage occurs, and it is permissible for the court to rule that the implementation of the penalty be suspended if the notification is made after the authorities become aware, provided that this leads to the arrest of the remaining perpetrators.[2].

Conclusion

Through our research, we have reached a set of results and recommendations as follows:

First: The Results

1. Cybercrime (i.e., electronic) is an advanced form of transnational crime. The increasing involvement of organized crime groups exacerbates the complex nature of this crime, which occurs in the borderless field of cyberspace. Perpetrators of cybercrimes and their victims can be located in different regions, and the effects of crime can extend across societies around the world, highlighting the need for an urgent, dynamic and international response.
2. Email and Internet fraud. Identity fraud (where personal information is stolen and used). Theft of financial or card payment data. Stealing company data and selling it.
3. Cybercrime is also related to people's privacy. The way a person behaves on the Internet can also reveal private data and facilitate his exposure to various dangers in cyberspace. Besides, privacy relates to the actions of individuals, in particular to how people can harm each other (for example, by circulating personal images without the consent of the person concerned). As digital technologies penetrate every aspect of our lives, the importance of security and protection of online communication also increases.
4. The law defines the crime of criminal agreement in Article 55 Penalties: "An agreement is considered a criminal agreement by two or more persons to commit a felony or

(2) Youssef Dilshad Abdel Rahman, previous source, p. 60.

misdemeanor of theft, fraud and forgery, whether specific or not, or to commit acts prepared or facilitated for their commission, as long as the agreement is organized, even in the principle of its formation." "continues, even if only for a short period."

5. The agreement is considered criminal whether its ultimate purpose is to commit crimes or use it as a means to achieve an illegal purpose.
6. The legislator considered that the criminal agreement is an existing crime in itself, independent of the agreement as a means of participation, and this matter is achieved by one of the shareholders expressing it, whether verbally, in writing, by indicating, or by suggesting, so that the expression reaches the other shareholders and is accepted by them. All shareholders must be accepted in such a way that it can be said that there is an agreement.
7. Cybercrime is distinguished from the rest of the known traditional crimes, so to speak. This matter is, of course, due to the characteristics that this crime has, and these characteristics are that the computer and technical systems are an element in its implementation. Therefore, detecting, investigating and proving cybercrime is It is a difficult matter to a certain extent, and what makes this more difficult is that it is a phenomenon that has widened geographical barriers and overcome all the rules that govern the spatial concept of crime. Therefore, it is a crime that does not recognize borders. We may find every element of the crime realized in a place or region.
8. The person who commits these crimes is somewhat distinct from the criminals of traditional crimes. We are not facing a thief, a fraudster, or an ordinary passer-by, but rather we are facing what is called the information criminal, who in addition to the characteristics of the ordinary criminal, we find that he possesses a kind of intelligence and knowledge of the latest developments in digital technology that It is the environment to carry out his criminal activity, not to mention that he has the skill required to carry out the criminal activity, which stems from his possession of a degree of knowledge and skill that he may acquire as a result of his studies or practical experience in this field.
9. The reality of these crimes has produced new innovative crimes that were not known before, or traditional crimes committed in a new manner. In this context, great efforts have been made to classify information crimes, whether at the level of the individual efforts of jurists or at the level of international or regional organizations, and since the crimes Information technology has proven to be crimes that cannot be enumerated in parentheses. As a result of the previously mentioned characteristics, it is classified into four categories: crimes against persons, crimes against trust and the public interest, crimes against funds, and crimes against the security of the state, organizations, and institutions. Of course, under each category there are many names that represent criminal activities. It violates the correct structure of society and threatens its existence. This division stems from the principle of interest that the legislator sought to protect. Therefore, we have tried to develop a classification capable of absorbing any developments in this context and understanding the situation of these crimes, especially since they are related to computers and information technology, which have different roles in carrying out the crime.
10. Qatari law punishes the criminal agreement. The criminal agreement is punishable by imprisonment for a period not exceeding five years. If the penalty for the crime that is the subject of the agreement is death. And life imprisonment.
11. The UAE law described the criminal agreement as being considered shirk in causing the crime: First: Whoever instigated its commission, it occurred based on this Incitement. Secondly: Whoever agrees with others to commit it, then the crime is committed based on this agreement.

12. In Article 59 1 of the Iraqi Penal Code, every member of a criminal agreement, even if he does not attempt to commit the agreed-upon crime, shall be punished with imprisonment for a period not exceeding seven years if the crime agreed to be committed is a felony. Imprisonment for a period not exceeding two years or a fine not exceeding one hundred and fifty dinars if the crime is a misdemeanor. This is unless the law stipulates a special penalty for the agreement.

Second: Recommendations

1- We hope that the Iraqi legislator will develop a clear and specific definition of the concept of cybercrime, without leaving this matter to legal jurisprudence and their definitions, since the latter's definitions do not distinguish between information crime, electronic blackmail crime, and cybercrime.
2- We hope that the Iraqi legislator will create a special text to attack the functioning of the automated data processing system.
3- We recommend that the Iraqi legislator create a special text for information fraud, as well as expand the concept of editor to include any other support.
4- We call on the Iraqi legislator to protect programs and information processed independently by punishing their seizure without compromising their integrity or authenticity or copying copies of them when the device is running.
5 - It is noted that our legislator has recently realized the noticeable legal vacuum in the field of information crime and has relied in this on the necessity of double protection for the computer through copyright texts on the one hand, and through special texts that he has incorporated into the Penal Code on the other hand.

Sources and References

The Holy Quran

First: Books

1. Ahmed, Abdul Rahman Tawfiq, Explanation of the Penal Code, General Section, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2011, p. 34.
2. Jamil Abdel Baqi Al-Safir, Book of Procedural Aspects Related to the Internet, Dar Al-Nahda Al-Arabiyya, 2002 edition, p. 72.
3. Al-Hadithi Fakhri Abdul Razzaq, Explanation of the Penal Code, General Section, Al-Zaman Press, Baghdad, 1992, p. 96.
4. Al-Roumi Ahmed, Computer and Internet Crimes, third edition, University Press, Alexandria, 2003, p. 123.
5. Sami Abdul Karim Mahmoud, Criminal Penalty, 1st edition, Al-Halabi Publications, Beirut 2010, p. 31.
6. Suleiman Abdel Moneim, The General Theory of the Penal Code, a Comparative Study, Al-Halabi Legal Publications, Beirut, 2003, p. 475.
7. Al-Shawi Munther, Philosophy of Law, Publications of the Iraqi Scientific Academy, Baghdad, 1994, p. 7.
8. Al-Shadi Tariq, Towards the Security Construction of Information Systems, Dar Al-Watan for Printing, Publishing and Information, Riyadh, 2000, p. 19.
9. Al-Saghir Jamil Abdel-Baqi, The Internet and Criminal Law (Objective Provisions for Internet-related Crimes), Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Cairo, 2012, p. 30.

10. Taha Ahmed Hossam, Exposing others to danger in criminal law, a comparative study, Dar Al-Nahda Al-Arabiya, Cairo, 2004, p. 39.
11. Abdel Hamid Bassiouni, Computer License - Information and Communications (Cairo, Dar Al-Kutub Al-Ilmiyyah, 2009), 1st edition, pp. 58,59.
12. Abdel Azim Abdel Salam and Salem Jarwan Al Naqbi, Constitutional and Criminal Guarantees for Human Rights and Public Liberties in the United Arab Emirates, Academy of Police Sciences, Sharjah, 2009, p. 31.
13. Atiq Al-Sayyid, Explanation of the Penal Code, General Section, Part One, The Crime, Third Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2009, p. 52.
14. Ali Jabbar, Internet and Computer Crimes, Al-Yazouri Scientific Publishing House, Amman, Jordan, p. 31
15. Odeh Youssef Suleiman, The Crime of Targeting the Civil War Through the Media, first edition, Arab Center for Publishing, Cairo, 2018, p. 120.
16. Ghanam Al-Quwari, General Principles in the Federal Criminal Procedure Code of the United Arab Emirates, 2nd edition, Al-Emirates, Bright Horizons, pp. 163,168
17. Al-Qaisi returned to Al-Hamoud, Principles of Constitutional Law and Systems of Governance, a comparative analytical study of the Constitution of the United Arab Emirates, first edition, University Library, Sharjah, 2013, p. 257.
18. Muhammad Salem, Crimes against reputation through electronic information technology, King Saud University Libraries, Riyadh, 2014, p. 68.
19. Muhammad Salem, Crimes against reputation through electronic information technology, King Saud University Libraries, Riyadh, 2014, p. 68.
20. Muhammad Shalal Al-Ani, Provisions of Oaths in the UAE Federal Penal Code - The General Theory of Crime (Sharjah: Bright Horizons, 2010), 1st edition, p. 196
21. Muhammad Eid, The Internet and its Role in the Spread of Drugs, first edition, Al-Khereiji Publishing House, Riyadh, 2003, p. 23.
22. Hilali Abdullah Ahmed, Explanation of the Penal Code, General Section, first edition, Dar Al-Nahda Al-Arabiya, Cairo, 1998, 1987, p. 68.

Second: Theses and Dissertations

1. Samir Ibrahim Jamil Al-Azzawi - Criminal liability arising from misuse of the Internet - Master's thesis submitted to the University of Baghdad - 2005, p. 96.
2. Al-Shehri Abdullah, Administrative Obstacles in Security Dealing with Computer Crimes, Master's thesis submitted to the College of Administrative Sciences, King Saud University, 2000, p. 30.
3. Abdel Khaleq, The General Theory of the Crime of Disclosing Secrets, in Comparative Criminal Legislation, Egypt, Doctoral Thesis, Ain Shams University, pp. 650, 670
4. Abdullah Kariri, The Moral Corner, in Information Crimes in the Saudi Regime - A Original Study (Master's Thesis, Riyadh: Naif Arab University for Security Sciences, 2013, pp. 40,41).
5. Al-Azzawi Samir Ibrahim, Criminal Liability Arising from Misuse of the Internet, Master's thesis submitted to the College of Law, University of Baghdad, 2005, p. 24.
6. Fahd bin Mubarak, Incitement to Crime in Jurisprudence and the Saudi System, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, 2006, p. 34.
7. Younis Omar Muhammad Abu Bakr, crimes arising from the use of the Internet, doctoral thesis submitted to Ain Al-Shams University, 2004, p. 231.

Third: Research and magazines

1. Ibrahim Al-Majid - The most important means and methods of fraud, fraud and deception via the Internet - published in Al-Jazeera newspaper - Issue - 58 of 2004 - p. 1.
2. Ahmed Kilan Abdullah, Muhammad Jabbar Anwa al-Nasrawi, Criminal Justice in Explanation of Criminalization and Punishment, Kufa Journal of Legal and Political Sciences, Volume (12), Issue (41), 2019, p. 10.
3. Ismail Abdel Rahman, The UAE is the first regionally in terms of exposure to electronic attacks, published in Al-Ittihad newspaper on 04/18/2016.
4. Ramadan Omar Al-Saeed, The Idea of Consequence in the Penal Code, research published in the Journal of Law and Economics, first issue, 1961, p. 105.
5. Al-Shukri Adel Youssef Abdel Nabi, information crime and the crisis of criminal legitimacy, research published in Al-Kufa Magazine, Kufa Studies Center, Iraq, seventh issue, 2008, p. 113.
6. Iraqi Khaled Ali, rumor crimes and electronic crimes in the United Arab Emirates, research published in the Journal of Jurisprudential and Legal Research, Issue Thirty-Eight, Zagazig University, Egypt, 2022, p. 169.
7. Al-Qahtani, Abdullah bin Hussein Al Hajraf, Developing criminal investigation skills in confronting electronic crime, College of Police Sciences, Naif Arab University for Minimal Sciences, Riyadh, 2014, pp. 61, 60, 59.
8. Al-Muttaridi Muftah Boubakar, Electronic Crime, a working paper presented to the Third Conference of Presidents of Supreme Courts in the Arab Countries Sudan, 2012, p. 17.
9. Al-Mamouri Raafat Hamid Rais, The impact of cybercrime and its impact on society, research published in Al-Mufakir Journal for Legal and Political Studies, Iraq, Volume Four, Issue Four, 2022, p. 134.

Fourth: Electronic sources

https://ar.wikipedia.org/wik
https://www.sjc.iq/view.4488/
https://almerja.com/reading.php?idm=187850
Salma Ihab, Specialists: The violations of the electronic press and "social media" require a law, Bahraini newspaper Al-Watan, March 23, 2013, available at the link:http://www.alwatannews.ne

Fifth: Laws

1. Qatari Criminal Procedure Code
2. Iraqi Penal Code No. 111 of 1969
3. Qatari Anti-Cybercrime Law No. (14) of 2014.
4. Iraqi cybercrimes draft law.