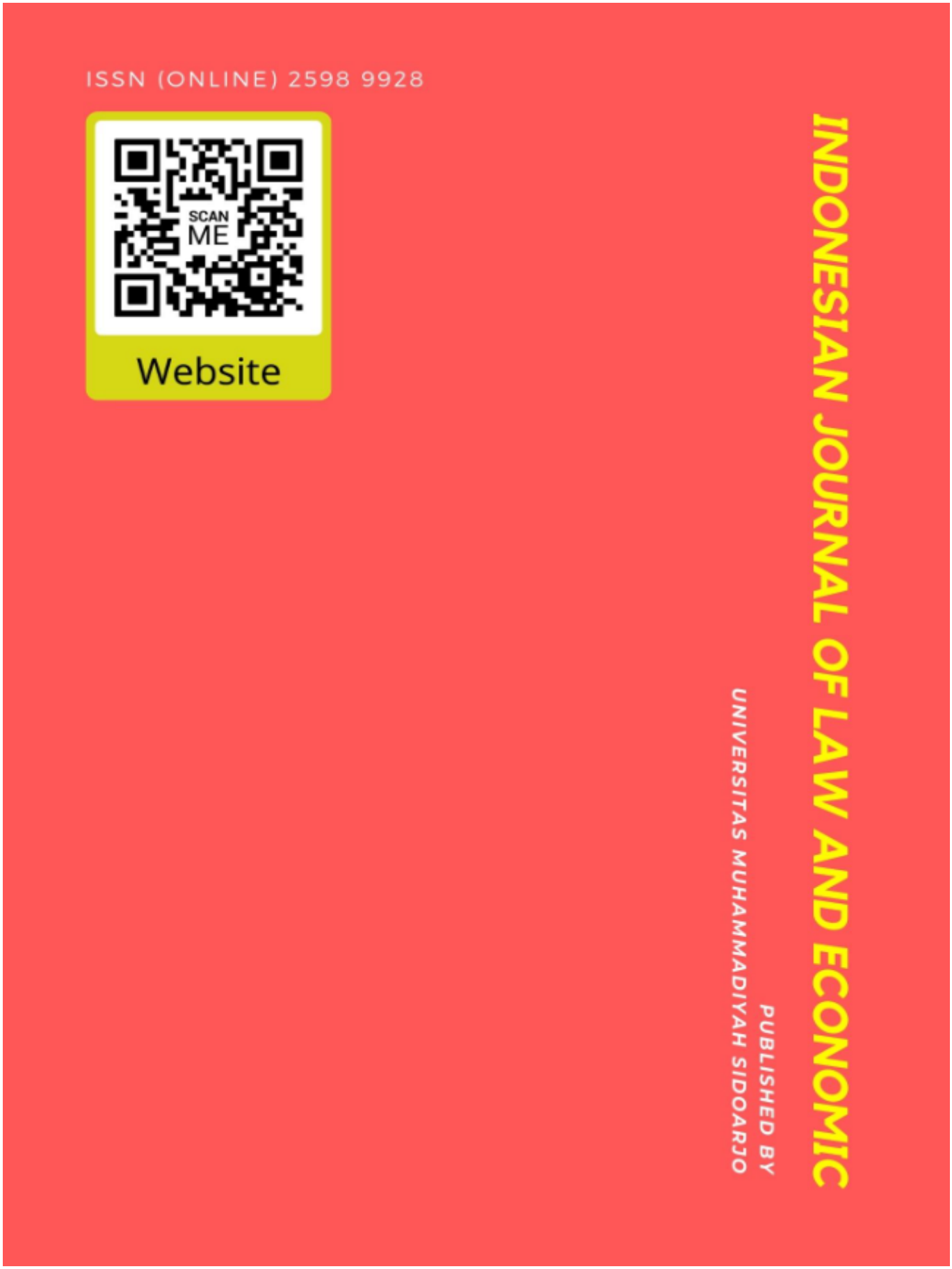
Indonesian Journal of Law and Economics Review

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647



ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Table Of Contents

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review
Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Indonesian Journal of Law and Economics Review
Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

EDITORIAL TEAM

Editor in Chief

Managing Editor

Editors

Complete list of editorial team (link)

Complete list of indexing services for this journal (link)

How to submit to this journal (link)

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

Indonesian Journal of Law and Economics Review
Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Cybercrimes in the General Criminal Law

Asraa Hamid Majeed , israahm13@uomustansiriyah.edu.iq (*)
Faculty of Tourism Sciences - Mustansiriyah University , Iraq

(*) Corresponding author

Abstract

As digital transformation accelerates globally, reliance on information networks has given rise to sophisticated criminal activities that challenge traditional legal enforcement. The rapid evolution of internet-mediated offenses has exposed critical vulnerabilities within existing general criminal law statutes. However, statutory frameworks often lack tailored procedural mechanisms to effectively prosecute transnational digital offenses. **General Background** This study examines cybercrime within the framework of general criminal law, focusing on legal nature, offender typologies, and enforcement protocols. **Specific Background** Using a descriptive-analytical legal methodology, the research evaluates legislative texts and juristic doctrines governing digital offenses. **Knowledge Gap** Existing legal literature frequently fails to address procedural gaps in cross-border jurisdiction and electronic evidence handling. **Aims** The primary objective is to evaluate statutory adequacy and propose robust legislative mechanisms. **Results** Findings reveal significant procedural hurdles in perpetrator identification and international judicial cooperation. **Novelty** The research establishes a specialized synthesis of multi-tiered penalty structures and administrative oversight. **Implications** These insights inform policy reformations to fortify statutory resilience against digital threats.

Keywords: Cybercrime, General Criminal Law, Legal Nature, Penalty Structure, Digital Evidence

Key Findings Highlights

Cybercrimes possess distinct transnational characteristics that complicate conventional territorial jurisdiction and offender identification.

Traditional penal provisions frequently lack specialized procedural provisions required for effective digital evidence collection.

Comprehensive legislative reform requires combining primary financial sanctions, operational closures, and enhanced international police collaboration.

Published date: 2026-08-19

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Introduction:

After a huge revolution in the information sector, life has relied heavily on computers and the Internet, which has become a reality imposed on government agencies and public and private companies, and even in some personal transactions, they are keen to use them, what we can say by this is that we often use social media sites, applications and other electronic programs that have made the world like a small village, it is clear that this tremendous scientific and technological progress is accompanied by the emergence of different types of criminal activity for that, sometimes it seems. The law is insufficient to counter this new type of crime, and the crime of information fraud may be a form of this behavior.

In order to determine the legal framework for these crimes, a distinction should be made between two types of crimes, the first is when information technology and remote communications have been used as a means to commit crimes, meaning that we are facing criminal acts committed with the help of computers, while the second type of cybercrime is when information technology is remote and is the target and purpose of the crimes, and we are facing new criminal acts related to exposure to the security and safety of information systems and the confidentiality of the data and information it contains, and this type is called cybercrimes. In the Internet, the computer has become a fundamental pillar of the goals of development in all areas of life, including various activities, whether economic, scientific or social, and the steady use of information technology, whether in the form of information money or new methods, has led to the emergence of what is known as information crimes, as this is the inevitable result of every new scientific and technological advancement, and this type of crime is based on two axes, one against money and the other against people, as it derives its activity from the enormous capabilities of the computer.

It is known that Iraqi legislators regulate the crime of fraud by the traditional means of Article 456 [1] represented in the use of fraudulent methods, i.e., lying and deception, but the above text is often used at the moment, especially when it comes to fraud in the field of electronic transfer systems and magnetic credit cards (main cards), so the law is a phenomenon of society. Because it reflects the birth of his need, it was necessary to pass laws dedicated to these crimes.

Research Problem:

The problem of the research lies in the fact that cybercrime is the result of technological development, i.e. it is committed through modern technology (computers and the Internet), and here is what made there a real problem in the difficulty of revealing the identity of the perpetrators of this crime, and in which country it was committed, it is a transnational crime, in addition to representing a very great danger to Internet users and smart devices who are not protected from this category, and therefore the main question of our research is raised, which is what is the problem of cybercrime on society?

Importance of the research:

- **Scientific Importance:**

The scientific importance of the research lies in identifying information technology crimes, as it is one of the modern crimes that fraudsters resort to for their ease of use, and the importance of our research lies in explaining the legal nature of this type of crimes, identifying the perpetrators of these crimes, and clarifying ways to address them.

- **Practical Importance:**

The scientific importance of this research lies in benefiting society as much as possible, and benefiting researchers and scholars, such as referring to it as one of the references in information technology crimes, in addition to developing recommendations and proposals through which it is possible to include the contemporary changes that are attracted by the Iraqi state as well as those witnessed by the world, as this file occupies a large aspect of the attention of countries, and therefore the importance of this study lies in practice.

Research Objectives:

The research aims to:

- Identify the nature of cybercrime and identify the persons of cybercrime.
- Explaining the legal nature of cybercrime.
- Identifying the position of the Iraqi legislator on cybercrime.
- Identify the most important precautionary measures to combat cybercrime.
- Identify the punishment prescribed for the perpetrators of cybercrime.

Research Questions:

The research raises several sub-questions, which are:

- What is Cybercrime?
- Has the Iraqi legislator addressed cybercrime?
- What are the most important precautionary measures that countries should take?
- What is the penalty prescribed to deter the perpetrator of a cybercrime?

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Reasons for choosing the topic:

The researcher's attention came from subjective and objective considerations as follows:

1. **Subjective causes:**

- The desire to know the extent of cooperation at the international level in combating information technology crimes.
- The desire to study the field of combating information technology crime, and to identify the most important legal texts related to combating cybercrime.

1. **Objective reasons:**

- The desire to point out the shortcomings and try to find appropriate solutions in order to combat cybercrime.
- To increase the number of cybercrimes in light of the enormous technological revolution in light of the inadequacy of national legislation to combat cybercrime.

Research Methodology:

The researcher was keen to choose the method that is appropriate to the legal nature of the research, which obliges us to follow the descriptive-analytical method in order to be familiar with all its aspects:

- **Descriptive Method:** The researcher relied on the descriptive approach by addressing the definition of information technology crimes.
- **Analytical Method: The** analytical method was used in the analysis of the legal texts stipulated by the legislator and their analysis in a precise analysis of perception and clear understanding.

Previous Studies:

1. **Hatem Ahmed Mohamed Battikh conducted a study entitled (The Evolution of Legislative Policy in the Field of Combating Information Technology Crimes) in (2021). [2]**

The study relied on the comparative analytical method, as it is the most consistent approach with the nature and objectives of the study by extrapolating and analyzing the provisions mentioned in the Egyptian Anti-Information Technology Crimes Law and some comparative countries.

The study aimed to: Study the subject of the study is a comparative analytical study between the legal texts to combat information technology crimes and the executive regulations from the objective and procedural aspects, and it also aims to identify the most important advantages included in the law, and to reach the shortcomings that resembled its comparative texts.

The study concluded: the way in which the countries of the world have confronted this technological threat, and showed the way in which they have addressed it by clarifying the necessary legislative solutions to combat information technology crimes.

2. **Nisreen Mohsen Nehme conducted a study entitled (Information Fraud Crime) in (2018). [3, p. 36]**

The study relied on the descriptive-analytical approach to address the concepts of the study and the analysis of the legal texts that stipulate combating information technology crimes in Article (456) of the Iraqi Penal Code.

The study aimed to : identify the legal value of information, indicate the forms of informational criminal behavior, indicate the most important means used, and the extent and suitability of the information as a crime object.

The study concluded: The crime of information fraud differs from the crime of fraud in its traditional forms in terms of the methods and methods used in committing the crime, that one of the most prominent features of the crime is the difficulty resulting from the use of keys, codes and electronic instructions to commit it, and the Iraqi legislator has specified the fraudulent methods exclusively in application of the text of Article (456) of the Iraqi Penal Code.

Commenting on previous studies:

Similarities:

The current study is similar to the previous studies in that both of them address the importance of information technology crimes, which are considered one of the modern methods resulting from the technological development witnessed in the modern era, and the current study has been adopted with the previous studies in using the descriptive-analytical approach that is in line with the legal nature of our subject under study, and the current study is similar to the second study in both of them in dealing with information technology crime within the framework of the Iraqi state.

D ifferences:

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

The current study differs from the previous studies in several respects, including the adoption of the study in its application within the framework of the Iraqi state, while the first study was adopted in its application within the framework of the Arab Republic of Egypt, and the current study differs from the previous studies in dealing with the international methods that have been resorted to in order to combat information technology crimes at the international level, not only at the local level.

Research Plan:

The first topic: What is cybercrime?

Criminal jurisprudence has not agreed on a unified designation for cybercrime, as some call it cybercrime, others call it crimes of misuse of information and communication technology, and others call it computer and internet crimes.

The first requirement: the definition of information crime.

Cybercrime is defined as: any crime committed against money related to the use of automated information processing, and cybercrime is also defined as legal assaults committed by means of information for the purpose of making a profit.

It is also defined as: a set of acts related to information that can be punishable, and the unlawful activity of altering, copying, deleting, or accessing information stored inside or transmitted through a computer. [4, p. 21]

It is also defined as any criminal act or activity committed using a computer or the global information network or through any means of communication and information technology.

[5, p. 4] Most of the cybercrimes are committed within the scope of electronic processing of data or texts, and therefore they are predominantly evidence of the digital nature and not of the physical nature, and there are many types and forms of cybercrimes used, the most prominent of which are the following: (computer crimes, information crimes, cybercrimes, telecommunications crimes, cybercrimes).

Second Section: Forms of Cybercrime.

There are multiple forms of cybercrime, and this is due to the multiple roles of information technology on the one hand, and the multiplicity of forms of traditional crime on the other hand, and we will limit here to legal problems in the framework of attacks on persons, money, and forgery.

First: Crimes of assault on the private life of individuals.

The crimes of assaulting the private life of persons are meant to be exposed to this type of crime that is difficult to confront with the traditional legal texts, as the assault on them is carried out using a technique, which has led to the absence of the necessity of the materiality of the behavior and the discussion of cases that raise a problem with regard to the application of the traditional texts and reveal the extent of the need for a legislative response to this type of crime, which makes it difficult to limit the elements of the right to private life, and that it is one of the elements that are not agreed upon among the jurists, that is, it has been It includes the inviolability of the human body, images, conversations, and professional life [6, p. 609].

Second: Crimes of Assault on Funds.

The transformation of the paper monetary and banking system into an information system in the management of operations, those related to the field, for which banknotes are the main axis, is an example in opening the way for the emergence of new images related to the crimes of intentional abuse of funds on the computer and communication and information technology.

1. **Use of software designed to carry out embezzlement.**

The most famous of these methods is the design of a specific program aimed at automatic transfer from one bank account to another of the same bank, provided that this is done at a certain time, determined by the designers of this program [7, p. 81].

2. **Direct transfer of balances.**

This is done by hacking the computer system and passcode[8, p. 71].

3. **Manipulation of financial cards.**

This type of fraud first emerged by capturing the secret numbers of credit cards and various point cards from ATMs with cash, until ATMs and cash appeared.

4. **Crimes of assault on ATMs.**

This problem occurs if the device is used to spend more than the actual balance if it is done by the customer holding the card, the problem here is no longer aggression, but the problem of debts between the financial institution and the customer, which cannot be adapted as theft according to Article (444) of the Iraqi Penal Code as long as the latter knows that the

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

device is not tied to the upper limit of the customer's account, so as not to exceed it, because the seizure of the amount was not done without the approval of the financial institution [9, p. 232].

5. **Crimes of seizing electronic money.**

E-money can be defined as monetary value that is stored in a prepaid electronic medium that is not tied to a bank account and accepted by anyone other than the person who issued it and used as a means of payment [9, p. 235].

Third: Electronic forgery.

The essence of the crime of forgery is the violation of the public trust, which the legislator wanted to protect in this document, because of its legal effect as a means of evidence for this, since the strength of the document in proof is the essence of its criminal protection, all materials suitable for proof are subject to forgery, regardless of its form or area and the material used in writing is equally important Made of wood or leather [10, p. 47].

The second requirement: Persons of information crime.

Cybercrimes, like other crimes that require two parties, the perpetrator and the victim, and there is no doubt that the natural person is the one who provides the opportunity to exploit the information medium, and accordingly, the persons of cybercrime can be identified as follows:

First Section: The Information Criminal.

In cybercrime, we are not dealing with an ordinary criminal, but with a criminal with technical skills and who is aware of the technique used in the system of automatic calculations, because the personality of the information criminal and the mechanism of committing the crime make him a person characterized by different smiles, in addition to the other qualities that must be present in the ordinary criminal[11, p. 32].

No punishment can be imposed in this cybercrime without the knowledge of this criminal so that he can be socially rehabilitated in order to reintegrate with society, considering that the reform of the criminal is the fulcrum of the penal system, as cybercrime is considered as smart crimes when compared to traditional crimes, which tend to violence, despite the perception of violent crime directed against information systems embodied in the destruction of computers.

There are many who resort to committing such a crime for the purpose of amusement, or in order to show their superiority over the machine, or on specialized programs for the security of information systems, without obtaining financial benefit, but they are content with boasting and showing themselves to the victims of the weakness of their systems, which shows that there is no social risk of cybercrime, and it is not the reason There is no evil intention, but unconscious behavior that can cause a lot of serious damage even if there is no hostility to society[8, p. 37].

2. The victim in the information crime: Just as a crime can be committed by a natural or legal person, the victim may also be, although the vast majority of these crimes are committed by a legal person represented by financial institutions and sectors, but abstract information is considered at this time one of the most important interests after money, especially if this information is of great importance and the goal of the information criminal is to obtain compensation through illegal bartering or Sell it to its rightful owners, whether this information is stored in the computer's ready memory or entered into the information banks when it has been distorted and shown to be untrue.[12, p. 90]

In this type of crime, the role of the victim is largely negative, as many victims prefer to keep their abuse secret, and the reason for this lies in their desire to preserve their social status or commercial reputation in order to protect their financial position, and the trust of customers in them, as they still want to disclose the differences that occur on their computers so that their protection measures are not seen as weak It is not effective, which causes a weak trust in the organization, which results in customer reluctance to do so.

This, in addition to the inability of the victims to materially prove the crime, and their fear of the possibility of legal issues in real time, is that they have a duty to supervise any of the information targeted and to have the necessary authority to assess and take important action when damage arises arising from the disclosure of sensitive and dangerous information[13, p. 109].

The second topic: The legal nature of the cybercrime and its characteristics.

The nature of cybercrimes is related to the automated information processing system in that it is considered one of the global crimes and not international crimes, and accordingly we will identify the legal nature of cybercrime, clarify the position of the Iraqi legislator on it, and identify its characteristics.

The first requirement: the legal nature of the cybercrime

The position of Iraqi law on the concept of information crime was that it was a global crime, and that the principle of universality of criminal law, known as universal jurisdiction, was intended to apply the criminal law of the State to every crime in which the perpetrator was arrested in the territory of the State, regardless of the territory in which it was committed, and regardless of the nationality of the perpetrators.

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

Section One: The Nature of Cybercrime.

The basis for the application of the principle of universality of criminal law depends on a main condition that the crime to be punished by the criminal is such as crimes of a universal character, which applies to information crimes. Anyone who commits a crime abroad as an original perpetrator or accomplice to any of the following crimes (sabotage, disruption of the work of intelligence means, international transportation, and trafficking in women or drugs) may extend the comprehensive jurisdiction of the Iraqi Penal Code to include cybercrimes, provided that a new paragraph is added to Article (13) of the Penal Code, according to which cybercrimes committed inside or outside the State of Iraq are subject to the authorities of the Penal Code and the jurisdiction of the courts The Iraqi Penal Code because of the dangers of this crime worldwide[14, p. 123].

Second Section: Elements of Cybercrime.

First: The Material Element:

The nature of the physical element of cybercrime may be related to the problems that can arise, and it means the illegal misuse of electronic systems, the intrusion of tangible physical traces that help in the destruction of information, the theft of credit cards, or the forgery and manipulation of data that is linked to computers.

Second: The Moral Pillar:

The moral element is considered one of the pillars of information crime in the Saudi system, which means the psychological and mood state of the person who commits the information crime, with the importance of focusing on the relationships that are related between the materiality of the crime and the personality of the offender.

Third: The Shari'a Pillar:

This element refers to the legitimate qualities of the act, where there is a rule of criminalization and penalties imposed on information crimes that are related to information systems, and criminal behavior is also related to information stored or entered into the computer, and criminal behavior is also represented in the destruction of the information system or forgery by infiltrating the balances of accounts available in banks.

The second requirement: the characteristics of information crime.

Cybercrime is related to the computer and modern information systems, to which several characteristics have been added that distinguish it from traditional crimes, the most important of which are:

1. **Cybercrime is transnational.**

The world has become a small village in light of the information technology revolution that does not recognize geographical boundaries, after the emergence of information networks, there is no longer what is known as the visual borders that stand in the way of the transfer of information across different countries, this was a result of technological development in the world of computer technology, which led to the ease of the movement of information through modern technology systems, which made it possible to commit this type of crime through a computer in a specific country, while the act took place This is the nature of information crime as a transnational crime, which has created many problems with regard to the determination of the competent State of this crime[15, p. 92].

2. **Difficulty in detecting cybercrime.**

Cybercrime is difficult to detect, and even if it is discovered, it is often accidental, and it is possible to explain the reasons behind the difficulty of detecting cybercrime for several reasons [16, p. 17].

3. **The difficulty of proving a cybercrime.**

It is not easy to detect an information crime, but even if such a crime is discovered and reported, its proof is surrounded by many difficulties, the most prominent of which are the following: [17, p. 59]

- Cybercrime takes place in a virtual world, which makes it more complicated for the competent security authorities.
- The lack of technical and technical expertise of the police, prosecutors and the judiciary is a major obstacle to proving cybercrime.

4. **The method of committing the information crime.**

Cybercrime is more clearly manifested in the way it is committed, as it is a quiet crime by nature that does not need violence, but all it needs is experience and the ability to deal with information technology.

5. **Cybercrime is often committed by more than one individual.**

Cybercrime is carried out by an omelette of individuals specialized in information technology, as it carries out the technical

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

aspect of the criminal project, and another person from the periphery, or from outside the victimized organization, in order to cover the fraud and transfer profits to it [18, p. 32].

6. **Privacy of the perpetrators of cybercrimes.**

The perpetrator of the cybercrime is called the cybercriminal, as he is specialized in specific characteristics that are distinguished from the criminal in the traditional crime, due to the fact that the technology crime requires knowledge and high ability in the field of information technology.

Third Topic: Procedural Measures to Combat Cybercrimes and the Prescribed Penalty for Cybercrimes.

There are a number of precautionary measures at the international level in order to combat information technology crimes, and we will also present the prescribed punishment for this crime.

The first demand: Combating cybercrimes.

The most important procedural measures that States must take, with the aim of overcoming the problems of international cooperation on combating cybercrimes, are as follows:

1. To the extent that this issue is useful for the investigation of a crime and its interests are required, it is necessary to allow the inspection of computer systems and networks or their parts, and the examination of the data stored therein and in various other storage media, regardless of whether such parts under inspection are located in the country or abroad. Adoption of procedural legislative measures[19, p. 253].
2. States shall take the necessary legislative measures to give the competent authorities the power to arrest and bring to justice, whether in their territory or elsewhere, a person so that that person can provide the data stored in computer systems or in one of the media used in data storage operations in the manner requested by those authorities for investigation.
3. Adding a judicial seizure to non-police information workers monitors the progress of work movements through service providers and the degree of law and order compliance by Internet workers, and if a crime is detected, those who handle this discovery in this way grant judicial administrative status to information workers who are not policemen, such as Internet access and service providers [20, p. 809].
4. Police agencies in each country patrol computer production agencies to prevent all forms of computer and internet-related crime, such as illegal copying of computer programs or mismanagement of computer components.
5. It is necessary to strengthen cooperation between national police agencies in accordance with international conventions, and this cooperation is important, in order for the country's national police to be able to access the Internet through websites located abroad, it reports this crime to the police authorities of the country in which the broadcast took place, each country must also appoint a security department to combat this type of criminal activity, which is entrusted with receiving communications that are the focus of information crime, and has the ability to take appropriate legal action in accordance with National law should implement security measures to protect against the aggravation of this danger adjacent to modern technology, which is destructive to the proper use of information.
6. Every country has the right to allow designated authorities access to computer systems for the benefit of investigation, especially if such data is found to be vulnerable to damage, loss, alteration, or erasure.
7. Each State shall adopt such legislative measures as are necessary for the duration of its jurisdiction over any cybercrime once it occurs:

- wholly or partially on its territory, or it is on board a ship, aircraft, or satellite bearing its flag or registered with it.
- If the offence is an offence punishable in accordance with the provisions of the Criminal Code in force in the place where the offence was committed, or if the offence is committed outside the territorial jurisdiction of another State[21, p. 452].

The second requirement: the punishment for cybercrimes.

Section One: Sections of Punishment in Regard to the Existing Association:

1. **Original Penalty:**

This is achieved when the judge sentences imprisonment without a fine or a fine without imprisonment, and the organizer has authorized this in his statement or by one of the two penalties, as it is stated in the text of the third article, which specified the first amount of the penalty, that any person who commits any of the crimes 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 the two penalties. Informatics. [22, p. 106]

2. **Supplementary Penalty:**

It is represented in the penalty of imprisonment or a fine if the judge adds one to the other, the penalties of confiscation and closure if the judge pronounces them, and the confiscation is a financial penalty, which is a penalty in kind, i.e., it is a refund of money, and it is a supplementary penalty that crosses the penalty of one of the two cases and obligations in the second case, and it has a third when it is compensation, where the judge may, in the case of a felony or misdemeanor sentence, order the confiscation of the seized items obtained from the cybercrime, as well as weapons and machines. Closure is also a

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

supplementary financial penalty as it needs to be stipulated by the judge.

Section Two: Sections of Punishment in Respect of Their Placement:

1. Corporal punishment: It is the punishment that falls on the human body, such as death and imprisonment.
2. Psychological punishment: It is the punishment that falls on the human soul.
3. Financial Penalty: It is the one that is imposed on a person's money, such as a fine.

Section Three: Sections of Punishment Considering the Judge's Authority to Rule on Them:

The punishment is divided into two parts: [22, p. 108]

1. Punishments in which the judge's authority is restricted, such as the death penalty.
2. The penalties of the judge's authority are broad, which are penalties below the death penalty, where the penal laws stipulate in the punishments of deprivation of liberty that the maximum and the judge has the broad authority to rule on the amount of the appropriate punishment for the crime according to the circumstances of each crime.

Conclusion:

In this modern research, we discussed the nature of cybercrimes, as they are among the crimes of the modern era, as well as the pillars of the commission of cybercrime, other than ordinary crimes, as well as the types of penalties prescribed for this crime, as the system took into account the diversity of punishment in quantity and quality, and how much the system set the minimum for each crime.

First: Results:

1. Information crime is one of the crimes that has not been dealt with in criminal jurisprudence in recent times.
2. The cybercriminal is characterized by advanced practical and technical skills and is knowledgeable about the technique used in the system.
3. The seriousness of cybercrimes increases with the development that has taken place in the field of information, as the development here depends on the success of the legal rules for crisis protection.

Second: Recommendations:

1. Issuing rules and instructions to improve social behavior in the field of combating cybercrime in line with the tremendous development and speed that keeps pace with the misuse of users targeting individuals, property, communities, countries and organizations.
2. Organizing seminars and specialized courses for judges, prosecutors and police investigators in the field of computer information technology and the Internet to develop capacities and everything related to cybercrime and its risks.
3. Signing international and regional treaties and conventions, including combating and preventing cybercrime.
4. The Cabinet should adopt an integrated strategic plan to combat cybercrime, engage in international and regional tensions, and identify ways to combat this crime.

References

1. Republic of Iraq, "Iraqi Penal Code No. 111 of 1969," 1969.
2. H. A. M. Battikh, "The Evolution of Legislative Policy in the Field of Combating Information Technology Crimes: A Comparative Analytical Study," Ph.D. dissertation, Faculty of Law, Ain Shams University, Cairo, Egypt, 2021.
3. N. M. Nehme, "The Crime of Information Fraud: A Comparative Study," Journal of Faculty of Law, University of Kufa, vol. 11, no. 36, pp. 1–40, 2018.
4. Research and Studies Complex, Cybercrime in the Gulf Society and How to Confront It, Riyadh, Saudi Arabia: Cooperation Council for the Arab States of the Gulf, General Secretariat, 2016.
5. M. N. Ghayeb, "Cybercrime," Al-Takni Magazine, vol. 24, no. 9, pp. 1–15, 2011.
6. B. Hijazi, The Conflict Between the Computer and the Internet in Model Arab Law, Cairo, Egypt: Dar Al-Kutub Al-Qanoon, 2007.
7. F. Rustom, Penal Law and Information Technology Risks, Assiut, Egypt: Modern Machines Library, 1992.
8. M. S. Al-Shawa, The Information Revolution and Its Reflection on the Penal Code, Cairo, Egypt: Dar Al-Nahda Al-Arabiya, 1994.
9. S. H. Nassef, "International Cooperation Mechanisms Need to Be Updated in the Fight Against Cybercrime," Journal of Tekrit University for Law, vol. 5, no. 2, pp. 200–245, 2020.
10. M. Al-Janbihi, Electronic Banking, Alexandria, Egypt: Dar Al-Fikr Al-Jamia, 2006.
11. H. Hamed, Criminal Protection of Online Electronic Commerce, Cairo, Egypt: Dar Al-Nahda Al-Arabiya, 2000.
12. A. Salem, "Cybercrime," Journal of the University of Babylon, vol. 2, no. 14, pp. 80–110, 2007.
13. H. Lotfy, Information Contracts and Services: A Comparative Study, Cairo, Egypt: Dar Al-Nahda Al-Arabiya, 1994.
14. Y. A. N. Al-Shukri, "Information Crime and the Crisis of Penal Legitimacy," Journal of the Faculty of Law, University of Kufa, vol. 7, pp. 110–135, 2008.
15. A. Salem, "Cybercrime," Journal of the University of Babylon (Humanities), vol. 14, no. 2, pp. 85–105, 2007.

Vol. 21 No. 3 (2026): Agustus
DOI: 10.21070/ijler.v21i3.1647

16. S. J. Abdel Baqi, Criminal Law and Modern Technology, 1st ed., Cairo, Egypt: Dar Al-Nahda Al-Arabiya, 1992.
17. F. B. Hegazy, Forensic Evidence and Forgery in Computer and Internet Crimes, 1st ed., Cairo, Egypt: Dar Al-Kutub Al-Qanoon, 2002.
18. K. Afifi, Computer Crimes, Copyright and Artistic Works, 1st ed., Cairo, Egypt: Dar Al-Kutub Al-Qanuniyya, 2002.
19. I. Kharashi, The Problem of International Cooperation in Combating Cybercrime and Ways to Overcome It, Egypt: New University Publishing House, 2014.
20. O. M. A. Bin Younis, Crimes Arising From the Use of the Internet, Cairo, Egypt: Dar Al-Nahda Al-Arabiya, 2004.
21. Abdel Hafeez, Technical and Security Trends to Confront Cybercrimes, Egypt: Arabic Books Library, 2005.
22. M. A. A. Azzam, "Punishment in the Anti-Cybercrime System in the Kingdom of Saudi Arabia," Journal of Faculty of Arts and Humanities, Taibah University, Medina, Saudi Arabia, 2019.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo