Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Integrating Science, Arts, Commerce and Technology for Future Innovations 7(12s)

CYBERCRIMES IN LIBYAN LAW

Maatouk Salah Eddine [1], Alfakhreeyah Hussein Abubakr [2]

[1] Professor, Department of Private Law, University of Sidi Mohamed Ben Abdellah, Fez, Morocco
[2] Vice Dean for Scientific Affairs, Faculty of Law, Omar Al-Mukhtar University, Libya and PhD Student, University of Sidi Mohamed Ben Abdellah, Fez, Morocco

Received 15 March 2026
Accepted 14 May 2026
Published 26 May 2026

Corresponding Author
Alfakhreeyah Hussein Abubakr,
issebbo@gmail.com

DOI
10.29121/shodhkosh.v7.i12s.2026.8363

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

This study examines the Libyan legislator's policy in confronting cybercrimes, focusing on Law No. 6 of 2022. It analyzes the challenges faced by traditional legal frameworks in addressing the evolving nature of digital offenses and the efforts undertaken at regional and international levels to combat them. The research adopts an analytical-inductive approach to evaluate the Libyan legislation's effectiveness, identifying its strengths and weaknesses in balancing crime deterrence with human rights protection. Key findings reveal legislative shortcomings, inconsistencies in penalties, and a lack of alignment with international agreements, leading to recommendations for redrafting laws, enhancing judicial and security capabilities, and fostering international cooperation to create a robust framework against cybercrime.

Keywords: Cybercrime, Libyan Law, Law No. 6 of 2022, Money Laundering, Digital Forensics, International Cooperation, Legislative Policy, Human Rights, Scopus

1. INTRODUCTION

With the evolution of cybercrime forms and their threat to individual rights, it has become imperative to confront this development with a robust criminal policy to halt the threat posed to the digital legal system due to the misuse of technological means. Traditional legal systems are no longer capable of confronting modern technological crimes and their methods. Therefore, it was natural to search for a modern criminal policy to address them, resulting in recommendations for specific criminal laws and texts to combat cybercrimes on both international and domestic levels. This includes Law No. 6 of 2022 concerning Libyan Cybercrimes, which was enacted to bridge the legislative gap that hindered the application of digital criminal justice due to the inadequacy of traditional texts in confronting emerging cybercrimes.

1.1. IMPORTANCE OF THE STUDY

The Libyan legislator introduced a new law to combat cybercrimes, namely Law No. 6 of 2022. It was important to address this topic, which is scarce in Libyan libraries due to its novelty. I could not find a comprehensive scientific study dedicated to the Cybercrime Law in Libyan law. Therefore, this study aims to provide a resource for researchers and interested individuals to benefit from.

1.2. PROBLEM STATEMENT OF THE STUDY

Perhaps one of the most prominent issues that encouraged me to choose this research topic revolves around the demands from various entities to amend the provisions of the Cybercrime Law immediately after its issuance. Thus, the research questions are: What approach has the Libyan legislator taken to combat cybercrimes? What are the forms of crimes criminalized by the Libyan legislator through this policy? Has the Libyan legislator achieved a balance between combating cybercrimes and human rights values? Were the phrases contained in this law clear in their meaning? Did the legislator benefit from regional and international recommendations in legislating this law?

2. RESEARCH METHODOLOGY

I have chosen to adopt an analytical-inductive approach by analyzing the texts of Libyan legislation related to cybercrimes, then evaluating them, along with an inductive study of international efforts to combat them.

2.1. SCOPE OF THE STUDY

The scope of our study will cover cybercrimes in Law No. 6 of 2022 concerning cybercrimes. It also aims to identify, as much as possible, regional and international efforts in this regard.

2.2. STUDY PLAN

First Section: The Nature of Cybercrimes and Efforts to Combat Them Second Section: The Position of Libyan Legislation on Cybercrimes

2.3. FIRST SECTION: THE NATURE OF CYBERCRIMES AND EFFORTS TO COMBAT THEM

Cybercrime has raised numerous challenges, starting from the difficulty of defining it to the difficulty of confronting it. Through the first requirement of this section, we will clarify the nature of cybercrime, while the second requirement will shed light on the efforts aimed at confronting it.

First Requirement: The Nature of Cybercrime

Understanding the nature of crime requires presenting the meaning of the term and clarifying the reasons for cybercrime.

First Branch: Definition of Cybercrime

Firstly: Terminological Definition of Cybercrime:

Legal scholars have differed in defining this crime, adopting the following approaches:

First Approach: Based on the criterion of the crime's objective, defining it as any aggression targeting information and data stored in a computer device or transmitted via the internet [1]. The criticism against this approach is that it limits the crime to acts targeting stored or transmitted information via the internet. However, information may not be the target of the crime but rather a means for its perpetration.

Second Approach: Based on the criterion of the means, defining it as any criminal activity in which a computer is used [2]. It is noted that this approach did not cover the aspects of technological development in the field of information technology devices and limited the use of computers in its perpetration, despite the possibility of its occurrence through other electronic means.

Third Approach: Defined it based on the knowledge of technology as those crimes that require special knowledge of computer technology and information systems for their perpetration [3]. A criticism of this view is that the perpetrator may commit their crime without needing this degree of expertise, knowledge, and familiarity.

Some believe that it is preferable not to provide a legislative definition for this crime, which was called for by the G8 conference in 1998, as an attempt to expand the scope of cybercrimes [4].

2.4. SECONDLY: THE POSITION OF THE LIBYAN LEGISLATOR ON THE DEFINITION OF CYBERCRIME

With the issuance of Law No. 5 of 2022 concerning combating cybercrimes, the Libyan legislator defined cybercrime in Article 1 as:

"Cybercrime is every act committed through the use of computer systems, the international information network, or other means of information technology, in violation of the provisions of this law."

2.5. THROUGH THE ANALYSIS OF THE TERMS IN THIS DEFINITION, THE FOLLOWING IS NOTED

Every act: A broad term that includes positive acts such as publishing, unauthorized access, and negative acts such as remaining after the expiration of the permitted period, or breaking the blocking. This emphasizes the principle of legality, as there is no cybercrime without a text.

The means through which the criminal act is committed: "the use of computer systems, the international information network, or other means of information technology." Here, the role of the technical means as the place of execution of the crime is highlighted. This excludes purely traditional means and includes all modern technical means within the scope of criminalization through a flexible wording.

In violation of the provisions of this law: This confirms the principle of legality, as there is no cybercrime except by text.

2.6. THIRDLY: LEGAL CLASSIFICATION OF CYBERCRIME IN LIBYAN LEGISLATION

The material elements of cybercrime in Libyan law can be extracted as follows:

Conduct: It is every unlawful positive or negative behavior that occurs in the digital space, executed through an electronic means, which is a fundamental and prerequisite element for the occurrence of this criminal pattern.

Result: The result may be material damage (e.g., hacking, fraud, encryption) or moral damage (e.g., blackmail, banking manipulation, eavesdropping on state secrets), or a potential threat to the state's security and stability.

Causal Link: There must be a causal link between the criminal conduct and the criminal result, such that the conduct is what led to the occurrence of the criminal result.

2.7. SECOND BRANCH: CAUSES OF CYBERCRIME

Cybercrime has become a threat not only to individuals but also to the state's stability and trust in its digital systems. It is a product of the technological environment, complex moral and material motives, legislative fragility in some countries, and a decline in the awareness system for individuals. Its causes can be summarized as follows:

Ease of access to hacking and piracy tools: The internet has become full of thousands of sites that provide hacking tools that can be used without any in-depth technical knowledge [5].

Security vulnerabilities in digital systems: The cybercriminal exploits security vulnerabilities in operating systems and governmental infrastructure [6].

Spread of smartphones and social media applications: The spread of smartphones and social media applications has led to an increase in the number of children using the internet, which in turn has led to an increase in the phenomenon of cybercrime.

Achieving quick financial gain: Crimes such as credit card hacking are committed to achieve quick profits. Cybercrime usually requires economic criminals specialized in the field of information technology.

Achieving political gains: This includes spying on state data, distorting the image of a political party, or spreading sedition for the benefit of external parties, or contacting the enemy to achieve objectives harmful to the state [7].

Lack of informational awareness among users: There must be a focus on educating users on how to protect technology, as much as developing it. The security of information must be placed among the priorities of national security [8].

Revenge motives: Some crimes involve the use of viruses to damage data, committed out of revenge.

Isolation and the desire for self-affirmation:Isolation and the breakdown of family ties contribute to the spread of this crime among teenagers who find hacking a means to affirm themselves by challenging digital systems. This is often committed by teenagers, often referred to as "geniuses" or "amateurs" [9].

Weakness of legislation in some countries: Some countries still rely on outdated laws that do not cover digital crimes, making them a safe haven for cybercriminals.

Lack of international cooperation: Despite the existence of agreements to combat cybercrime, the non-accession of some countries weakens their effectiveness in judicial prosecution across borders.

2.8. SECOND REQUIREMENT: DIFFICULTIES IN COMBATING CYBERCRIME AND EFFORTS TO COMBAT IT

First Branch: Difficulties in Combating Cybercrime

Combating cybercrime faces numerous technical, legal, and judicial difficulties, including:

The technical nature of cybercrime: Cybercrime is constantly evolving with the development of systems and software. Cybersecurity rarely develops a defensive tool until a new attack method emerges that surpasses it [10].

Weak technical qualification of security and judicial cadres: The lack of technical expertise is considered the most important obstacle to the success of investigations. This is because public prosecutions in some countries do not care about training security personnel on modern devices, which leads to the absence of the skills required to uncover digital evidence, and they may deliberately avoid it due to lack of knowledge of technology [11]. The cybercriminal always develops themselves in the field of information technology, which necessitates the continuous development of security agencies in this field.

Reluctance of victims to report cybercrime: Many institutions, especially financial ones, are reluctant to report crimes for fear of losing the trust of their clients, which increases their financial losses. Companies also fear the seizure of their computer devices, the disruption of their information network, and the seizure of evidence for inspection purposes [12].

Difficulties related to the principle of spatial criminal jurisdiction of computers: Information networks have become interconnected in all countries, which has led to the association of cybercrime with judicial issues related to legal jurisdiction and judicial procedures for prosecution and specialized judiciary.

Lack of awareness among most users regarding the security aspects of personal data: Most users are not aware of the security aspects of personal data, which facilitates the hacking of electronic sites and emails. Also, most users are content with free protection programs available on the web, which do not provide the strong protection conditions for sites from hacking or piracy [13].

Difficulties related to proving cybercrime, including the volatility of evidence: It is easy to destroy and erase evidence in a few seconds, as digital evidence is characterized by its susceptibility to disappearance. Electronic records and data may be tampered with or disappear easily, making their security difficult [14].

High costs of obtaining digital evidence compared to traditional evidence: Digital evidence requires continuous reliance on experts to access and understand its content [15].

Slowness of inspection procedures: The issuance of an inspection warrant may take hours, while digital evidence may disappear within seconds. Therefore, an inspection order is not issued until the traces of digital evidence have disappeared [16].

Legislative shortcomings in criminalizing emerging acts such as manipulating artificial intelligence models: Many laws still lack texts criminalizing the manipulation of artificial intelligence models. The rapid technological development necessitates that legislators develop legislation to confront this crime with its constantly evolving methods [17].

In conclusion, the difficulties generated by the nature of cybercrime lie in a criminal who develops their capabilities, benefits from the slowness of legislation, the complexity of procedures, and the ignorance of the user.

2.9. SECOND BRANCH: EFFORTS TO COMBAT CYBERCRIME

Regional and international efforts to combat cybercrime have varied, including holding international and regional conferences and concluding agreements, in addition to some countries adopting these recommendations and efforts in their national legislation. In this branch, we will clarify these legislative positions and efforts as follows:

Firstly: Regional and International Efforts in Combating Cybercrime

International efforts have been embodied in the movement of international organizations, realizing that the digital space is indivisible. This has been done through holding numerous conferences and agreements. Recognizing by countries that regional integration remains the first line of defense, regional efforts have emerged that seek to confront it. These efforts are embodied in the following:

The Council of Europe: It initiated numerous recommendations, including the recommendation related to the protection of personal data from misuse. An agreement was signed in January 1981 concerning the protection of individuals from electronic processing of personal data [18]. This was one of the initiatives of the Council to develop a comprehensive international treaty to combat cybercrime, which was adopted in 2001 in Budapest and entered into force in 2004 [19]. This agreement focuses on strengthening international cooperation and unifying legislative measures to prevent this crime. It also emphasized the importance of both substantive and procedural aspects, and the need to achieve a balance between human rights and freedoms and the search for and prosecution of the crime and its perpetrators.

United Nations Efforts: The United Nations has made great efforts in combating cybercrime, including:

1) **The Fifteenth Conference of the International Society for Penal Law, Brazil 1984:** The conference emphasized a set of principles, including the need to define the authorities that carry out seizure and inspection in the digital environment, and to allow them to object to communications, while taking into account the sanctity of private life and economic opportunities. It also emphasized the importance of reconsidering the rules of electronic evidence [20].
2) **Organization for Economic Cooperation and Development (OECD):** It developed a set of guidelines related to information technology and issued a report in 1983 titled "Computer-Related Crimes," which included a minimum set of acts that countries should criminalize, such as manipulating data processing, information espionage, unauthorized use of data, and unauthorized access to or transfer of data [21].

Interpol (International Criminal Police Organization): Established in 1923 with its headquarters in France, this organization has branches in every member state and consists of 177 member states. Given the special nature of cybercrime, it was imperative to have international cooperation at the criminal procedural level, where there is communication between police agencies in different countries to combat crime and apprehend criminals [22]. This cooperation is evident in the centralized reference point system, meaning that each member state in Interpol has a national central bureau that serves as a point of contact with countries where investigations are conducted outside its borders. It includes a network of investigators in all concerned countries, which facilitates the exchange of expertise and the speed of field communication between countries in combating crime [23].

International Labour Organization (ILO): It made efforts in the field of protecting personal information related to work. This was done by codifying a set of recommendations adopted by the International Labour Office, through the conference of experts related to the protection of private life for work. These recommendations were the nucleus for building and paying attention to internal laws for member states to protect individual data recorded on computer devices [24].

League of Arab States: The League initiated the drafting of the Information Technology Crimes Combat Agreement in 2010, which was signed by most Arab countries. The agreement aims to strengthen Arab cooperation in combating

cybercrime. Libya ratified the agreement but did not refer to it in its legislation. Among the most prominent provisions in the agreement are the criminalization of unauthorized access or remaining, data destruction, and misuse of information technology means, as well as emphasizing the need for security and judicial cooperation and the exchange of information and evidence and the development of a common information security infrastructure [25].

Riyadh Document for the Unified System for Combating Information Technology Crimes: This document, issued by the Cooperation Council for the Arab States of the Gulf in 2013, criminalizes anyone who establishes a website or publishes information on an information network or any means of information technology to facilitate communication for a terrorist group, promote its ideas, finance it, or its members or leaders, or publish how to manufacture any devices or explosives used in terrorist acts [26].

Secondly: The Position of Criminal Legislation on Cybercrime

Countries have differed in combating cybercrime. While most legislations have dedicated specific laws for it, some countries have sufficed by adding texts to their existing laws. This will be clarified as follows:

Firstly: Countries that established specific laws for cybercrime

In response to international calls, some countries issued their own laws for cybercrime, including:

Western countries that issued specific laws for cybercrime:

1) The United States of America: It issued several legislations, starting with the Computer Systems Protection Law in 1976, followed by the Fraud and Abuse Law in 1984. In 1986, Law No. 1213, the Computer Fraud and Abuse Act, was issued, which has been amended several times to expand the scope of covered crimes [27].
2) Sweden: Sweden is considered the first country to enact specific legislation for cybercrimes. It issued the Swedish Data Law in 1973, which addresses cases of fraud through computers, in addition to criminalizing unauthorized access to or alteration or forgery or transfer of computer data, or unauthorized acquisition thereof [28].

Arab countries that issued specific laws for cybercrime:

Many Arab countries have issued specific laws to combat cybercrime, including:

1) Libyan Legislator: Law No. 5 of 2022 concerning cybercrimes was issued [29].
2) Jordan: It issued the Cybercrime Law No. 27 of 2015 and its amendments [30].
3) Saudi Arabia: It issued the Cybercrime Combat System in 2007 [31].
4) Egypt: It issued the Information Technology Crimes Combat Law No. 175 of 2018 [32].

Secondly: Countries that added texts for cybercrime within their existing laws

Some countries chose to integrate these crimes within the existing legislative structure. We mention among them:

Western countries that added texts to their existing laws:

1) France: The French legislator was interested in developing criminal laws to keep pace with the developments of cybercrime. In 1988, Law No. 88-19 was issued, by virtue of which cybercrimes and their prescribed penalties were added to the Penal Code. This was later amended by Law No. 2004/575, which dealt with a set of crimes against data processing systems [33].
2) Britain: The Computer Misuse Act of 1990 was not drafted as a specific law for cybercrimes, but rather as an addition to the General Penal Code. It contained 18 articles divided into three chapters. The law was amended in 1998, 2006, and 2015 [34].

Arab countries that added texts to their existing laws:

1) Kingdom of Morocco: Law No. 07-02 of 2003 concerning disruption of automated data processing was published in Morocco. This law forms Chapter Ten of the first part of the third book of the Moroccan Penal Code under the title "Crimes Affecting Automated Data Processing." This law contains nine articles from 607-3 to 607-11, through which the Moroccan legislator criminalized acts that constitute an attack on information systems [35].
2) Lebanon: It did not amend its traditional laws to apply to cybercrimes [36].
3) Yemen: Paragraphs were included within the Press and Publications Law and the Penal Code [37].

3. SECOND SECTION: THE POSITION OF LIBYAN LEGISLATION ON CYBERCRIME

The Libyan legislator issued Law No. 5 of 2022 concerning cybercrime, aiming to protect digital rights. Has the legislator succeeded in drawing a criminal policy to combat cybercrime? To answer this question, we have divided cybercrimes in this law into two requirements: the first requirement for cybercrimes that constitute an attack on the electronic device itself, and the second requirement for traditional crimes that use the electronic device in their perpetration.

First Requirement: Crimes of Attacking the Electronic Device

Cybercrime may occur by attacking the electronic device itself, where information technology becomes the subject of the attack. Through this requirement, we will divide these crimes into two branches: the first branch for crimes of unauthorized access, encryption, and information technology, and the second branch for crimes of attacking private accounts and electronic mail.

First Branch: Crimes of Unauthorized Access, Encryption, and Information Technology

Among the forms of unauthorized access, which is often done by decrypting passwords and codes through encryption and encryption tools, or by affecting information technology by obstructing access to the service. This is what we will present according to the following:

Firstly: Crimes of Data Destruction, Viruses, and Encryption

The Libyan legislator specifically protected electronic data with several explicit articles. The legislator criminalized crimes of possessing and encrypting information in Articles 9, 14, and 39, while Article 10 criminalized crimes of obstructing access to services [38].

Crime of possessing encryption tools and coding in Articles 9 and 14 of the Cybercrime Law:

The Libyan legislator criminalized the possession of encryption tools in Article 9 of the Cybercrime Law, stating that: "No person or entity may produce, possess, provide, distribute, market, manufacture, import, or export encryption tools without a license or authorization from the National Authority for Information Security." It seems that the legislator did not specify the punitive aspect for criminalization. However, this punitive gap was addressed in Article 14, which states: "Anyone who produces, provides, distributes, imports, exports, possesses, or promotes any information program or device, or any information data prepared for displaying passwords or access codes or breaking blocking for the purpose of unauthorized use, shall be punished with imprisonment for a period not less than one year and a fine not less than one thousand dinars and not exceeding ten thousand dinars."

By analyzing these two texts, the term "program or device prepared for displaying passwords or access codes or breaking blocking" includes the term "possession of encryption tools" by any means, whether by producing, providing, distributing, manufacturing, importing, or exporting them, or possessing them for the purpose of marketing without authorization or license.

The legislator in Article 14 required a specific criminal intent, which is the intent of unauthorized use. So, if a person committed the previous acts and their intent was legitimate use of these programs, then it is not a crime. It would have been better for the legislator to criminalize the acts of producing, providing, distributing, importing, exporting, possessing, or promoting any information program or device, or any information data prepared for displaying passwords or access codes or breaking blocking without authorization, and to delete the phrase "for the purpose of unauthorized use" to avoid circumventing the specific intent, so that criminals do not escape punishment, and it suffices for the crime to be complete by mere possession without authorization, without resorting to the intent behind it.

Crime of affecting the electronic system by obstructing access to the service in Article 10 of the Cybercrime Law:

The legislator criminalized affecting the electronic system in Article 10 of the Libyan Law No. 5 of 2022, stating: "It is prohibited to affect any electronic system, information system, information network, electronic record, information technology tool, or computer device or system, or electronic information or tool, or electronic signature, by programming, obtaining, disclosing, transferring, or publishing a code, password, or any other confidential data or property, with the intent of obtaining an unauthorized benefit or harming others." However, a criticism of this text is that the legislator did not specify the penalty prescribed for this crime.

Secondly: Crime of Unauthorized and Unlawful Access

Unauthorized access to electronic systems and information networks is considered a digital intrusion aimed at violating the sanctity of information systems. The term "access" includes all acts that allow logging into an information network with the aim of benefiting from the services it provides without authorization or subscription. It also includes logging into an information system with the intent of disclosing information stored in it or harming the integrity of its content [39].

The Libyan Law No. 5 of 2022 included unauthorized access at the forefront of criminal acts, dedicating a separate text for it in Article 11, stating: "Access to computer systems and devices, or an information system, or an information network, or an unauthorized electronic site, is considered unlawful if the intrusion is done intentionally by completely or partially bypassing protection measures and means, or without authorization, or in violation of authorization."

This article criminalized mere unauthorized access and intrusion into protection systems, whether the access and intrusion were intentional, completely or partially bypassing protection measures, or without authorization, or in violation of authorization. For example, if a person is authorized to access for a specific period, and they remain after the expiration of the authorized period, this is considered a violation of authorization.

Unauthorized access is considered a crime according to this text only if it was intentional, as the legislator stipulated intent by saying: "if the intrusion is done intentionally."

The legislator prescribed a penalty for the crime of unauthorized access in Article 12, stating: "Anyone who violates the provisions of Article 11 of this law shall be punished with imprisonment for a period not exceeding one year and a fine not less than 100 dinars and not exceeding 500 dinars, or both penalties together."

The penalty is imprisonment for a period not less than one year and a fine not less than 500 dinars and not exceeding 5,000 dinars if the access was for the purpose of deleting, adding, destroying, disclosing, or modifying data, or copying or transferring data, or obstructing the operation of a system, or changing an electronic site, or canceling or destroying its contents, or impersonating its owner.

If this unauthorized access results in a serious disruption or damage to the technical infrastructure, by obstructing the operation of the information system, or disrupting the information network or the electronic site, or corrupting their contents, the penalty shall be increased to imprisonment with a fine not less than 10,000 dinars.

Through the analysis of Article 12, it is noted that the legislator differentiated between forms of unauthorized access. The article graduated into three cases depending on the damage.

In the case of mere unauthorized access without sabotage, which is when the criminal act stops at mere unauthorized access intentionally, without tampering with it. If the crime stops at the point of access, the legislator considered it simple damage if the access to devices was without tampering with data, or disrupting them. The penalty is imprisonment for a period not exceeding one year, or a fine not less than 100 dinars and not exceeding 500 dinars, or both penalties together.

In the second case, if the access was for the purpose of deleting, adding, destroying, disclosing, or modifying data, or copying or transferring data, or obstructing the operation of a system, or changing an electronic site, or canceling or destroying its contents, or impersonating its owner, the penalty is imprisonment for a period not less than one year and a fine not less than 500 dinars and not exceeding 5,000 dinars.

In the third case, if unauthorized access results in a serious disruption to the technical infrastructure, the legislator intensified the punishment if the crime caused damage, according to the third paragraph, stating: "If this unauthorized access results in a serious disruption or damage to the technical infrastructure, by obstructing the operation of the information system, or disrupting the information network or the electronic site, or corrupting their contents, the penalty shall be increased to imprisonment with a fine not less than 10,000 dinars."

Second Branch: Crimes of Attacking Electronic Mail and Private Accounts

The Libyan legislator addressed crimes of attacking electronic mail and private accounts through the texts of Articles 5, 15, and 16. It also criminalized information forgery of electronic mail in Article 16 and the third paragraph of Article 15. In addition, Article 18 criminalized electronic impersonation of others. This is according to the following:

Firstly: Crime of Electronic Mail by Attacking Digital Data

Electronic mail by attacking data in an electronic context refers to any act aimed at attacking identity and identification tools belonging to others without legitimate authorization. This type of crime is usually committed through

hacking and piracy by accessing systems remotely. The Libyan legislator realized the seriousness of these acts and stipulated their criminalization according to the following:

Crime of Digital Identity Impersonation: The legislator criminalized the seizure of identity and identification tools, even without actual use of the data. If the perpetrator used the electronic identity and identification tools belonging to another person, the legislator intensified the punishment. This is stated in Article 18: "Anyone who seizes identity and identification tools belonging to another person used in an information system shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 3000 dinars."

"Anyone who orders the use of identity and identification tools belonging to another person in an information system unlawfully, with their knowledge, shall be punished with imprisonment for a period not less than one year and a fine not less than 1000 dinars and not exceeding 10,000 dinars."

Crime of Altering Information Data: The legislator stipulated in Article 15: "Anyone who causes material damage to another by introducing, altering, deleting, or destroying information data, or any form of tampering with the operation of an information system to obtain an unauthorized material benefit for themselves or others." Through this text, it is clear that the legislator criminalized the alteration of information data by any form of tampering that leads to harming others. The legislator stipulated the occurrence of material damage to others for the elements of this crime to be complete. It is one of the crimes of damage that the law required the occurrence of a result. The legislator also required a specific intent, which is to obtain an unauthorized material benefit for themselves or others.

Secondly: Crime of Information Forgery of Electronic Mail

Information forgery refers to the imitation of digital works and piracy, which is any act that leads to unauthorized copying, modification, or re-publication of works protected by intellectual property laws, and the forgery of data and documents existing on a device, by placing information that replaces the real information. Among its forms:

Crime of Digital Identity Forgery: Article 18 criminalized information forgery of digital identity by seizing and using identity and identification tools, stating: "Anyone who seizes identity and identification tools belonging to another person used in an information system." It also criminalized: "Anyone who orders the use of identity and identification tools belonging to another person in an information system unlawfully, with their knowledge."

Crime of Digital Works Forgery: Article 25 criminalized the imitation of digital works, piracy of software, and technical programs, stating: "Anyone who imitates any literary, artistic, scientific, or digital work, or commits software piracy, and copying software is considered an act of imitation."

The elements of the crime of attacking intellectual property in the digital medium can be determined as follows:

The presumed element: A digital content or program that has the characteristic of creativity and is protected by publishing rights.

The material element: The act of unauthorized publishing, imitation, or copying, which includes selling, distributing, or downloading a protected digital work. The result is achieved by the mere occurrence of unauthorized circulation or imitation, even if no damage occurs. There must be a causal link between the conduct and the result.

The moral element: Knowledge of the elements of the crime and the intent to commit the act, with the intent of unauthorized use.

Second Requirement: Crimes Using the Computer

The development in the digital field has led to the evolution of traditional crime, to be committed through digital platforms. Through this requirement, we will divide these crimes into two branches: the first branch for crimes of attacking private life, and the second branch for crimes of attacking public morals and the state.

First Branch: Crimes of Attacking Private Life

The right to private life is one of the most important human rights, as it protects human freedom, dignity, property, and privacy. Attacking it through digital platforms is a very serious matter. The forms of attacking private life are represented in the following:

Firstly: Crimes of Attacking Individuals

Crimes of attacking individuals are those crimes that target or threaten individuals closely related to them. These crimes are now committed through digital platforms.

Crime of photographing, recording, or broadcasting conversations or images without permission: Article 21 criminalized photographing, recording, or broadcasting conversations or images without the permission of the owner, stating: "Anyone who photographs, records, or broadcasts conversations or images without the permission of the owner, or combines or mixes images and voices with obscene content, with the intent of harming others, and publishes them through any electronic means, shall be punished with imprisonment for a period not less than one year and a fine not less than 1000 dinars and not exceeding 5000 dinars. If the act is done with the intent of harming others, and the images and voices are combined or mixed with obscene content, and published through any electronic means, the penalty shall be intensified to imprisonment for a period not less than five years."

Crimes of electronic blackmail and harassment: Electronic blackmail is the process of threatening the victim with leaking information or publishing compromising materials, or exploiting the victim to disclose information in exchange for financial sums or other secrets [40]. The crime of electronic blackmail has evolved with the development of hacking tools for electronic devices, which facilitates access to and seizure of their contents and threatening the victim. The legislator criminalized the crime of harassment in Article 22, stating: "Anyone who harasses another on the international information network or by any other electronic means, with the intent of satisfying their sexual desire, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 30000 dinars. Anyone who uses an electronic means to send or explain unwanted sexual content shall be punished with imprisonment and a fine." The legislator in this text limited the protection to sexual blackmail, which is considered a legislative shortcoming in protecting the rights of others from harassment in general.

Crime of digital identity impersonation: Digital identity impersonation is considered one of the most widespread cybercrimes, especially in cases of impersonating a specific individual. This crime begins with collecting the largest amount of information, photos, and personal data of the victim to use it in creating accounts in the victim's name to mislead others to obtain a benefit. It may occur by impersonating one of the sites by hacking and controlling it [41]. The legislator stipulated in Article 46 the protection of digital identity and the prevention of impersonating characteristics, commercial marks, and trademarks, stating: "Anyone who changes the address of a site, or uses a commercial mark registered in the state in the name of others, or uses special slogans and marks for their site on the international information network, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 5000 dinars, along with the obligation to remove it. The penalty shall be imprisonment for anyone who leaks, destroys, seizes, or exploits any industrial property of value, such as a patent or design." Article 18 also criminalized the seizure of identity and identification tools.

Crime of electronic eavesdropping and recording of private conversations: Eavesdropping on conversations refers to listening to spoken words that have a private nature by any means [42]. Recording is the preservation of spoken words exchanged on a device. The purpose of criminalizing electronic recording and eavesdropping is to protect conversations and individuals from auditory assault. The legislator criminalized eavesdropping through electronic means in Article 47, stating: "Anyone who eavesdrops on any communication that takes place through the international information network or any other electronic means, with the intent of obtaining secrets, shall be punished with imprisonment for a period not less than one year. If the intent is to obtain banking, military, security, or governmental secrets, the penalty shall be intensified to imprisonment for a period not less than three years. If the perpetrator publishes these secrets through information networks or any other electronic means, the penalty shall be intensified to life imprisonment."

Crime of attacking intellectual property: Article 24 criminalized anyone who attacks copyright by any electronic means, or counterfeits the electronic signature of the author, or orders another to do so. Article 25 also criminalized the imitation of technical programs and digital works, stating: "Anyone who imitates any literary, artistic, scientific, or digital work, or commits software piracy, and copying software is considered an act of imitation."

Secondly: Crimes of Attacking Money through Digital Means

The technological development has led to the invention of credit payment methods for money transactions, foremost among them electronic money and cards. These cards have become a target for electronic manipulation, including:

Crime of counterfeiting and using electronic bank cards: Counterfeiting a bank card means the perpetrator changing its data and the electronic information available on it. The legislator stipulated in Article 28 the penalty of imprisonment for a period not less than one year and a fine not less than 1000 dinars and not exceeding 10,000 dinars for anyone who counterfeits an electronic bank card, or seizes it, or uses a counterfeit electronic card, even if they do not obtain money, or uses a stolen card, even if they do not obtain money, or accepts payment with a counterfeit electronic bank card with their knowledge, or counterfeits electronic money. Article 41 also states: "Anyone who uses card numbers or service

sales cards without legitimate right to obtain available services shall be punished with imprisonment for a period not less than one year." It is noted through these two texts that the legislator is confused in confronting electronic card crimes. Both texts address the same criminal behavior, despite the difference in the criminal result. However, the legislator stipulated different penalties. In Article 28, the penalty is imprisonment for a period not less than one year for anyone who counterfeits or accepts or seizes electronic money and cards. In Article 41, the penalty is imprisonment for a period not less than one year for anyone who uses electronic cards without legitimate right. This is an issue that should not occur, as we notice an overlap of texts here, which should not happen in legislation.

Crimes of electronic banking fraud: Electronic fraud occurs by manipulating data in the financial processing system. Manipulation involves using encryption tools in a complete or partial distortion, by deleting, or distorting the processing system to obstruct its performance [43]. The legislator stipulated the criminalization of possessing and encrypting banking encryption tools, out of concern for preventing the occurrence of banking manipulation crimes. This is in the second paragraph of Article 39, stating: "The penalty shall be imprisonment for a period not less than ten years and a fine not less than fifty thousand dinars and not exceeding one hundred thousand dinars if the acts are related to encryption tools belonging to the government, banks, or military or security institutions."

Crime of promoting unwanted goods: Article 17 states: "Anyone who sends promotional messages for unwanted goods to others, without enabling the recipient to stop receiving these messages if they wish, shall be punished with imprisonment or a fine not less than 1000 dinars and not exceeding 10,000 dinars."

Secondly: Information Crimes Against Public Morals and the State

In light of what the electronic space witnesses from the collapse of barriers between countries, it has become possible to promote or broadcast anything that violates public morals and values. The legislator was keen to criminalize every use of electronic means that violates ethical, social, and religious controls.

Crime of publishing or producing obscene materials or promoting them: Article 19 criminalized the production or promotion of obscene materials. It also criminalized the crime of combining and mixing images and voices of individuals in obscene forms, and publishing them by any electronic means in Article 21.

Crime of incitement to prostitution: The legislator criminalized incitement to prostitution in Article 20, stating: "Anyone who encourages or incites another to engage in sexual activities, or contributes to preparing for this matter through the international information network or any other electronic means, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 10,000 dinars." The legislator also criminalized the crime of harassing others to satisfy sexual desire in Article 22.

Crime of exploiting minors: The legislator criminalized the exploitation of minors and mentally and psychologically disabled persons in unethical acts for obscene purposes, using any electronic system in Article 23.

Crime of electronic gambling: Gambling is considered an unethical crime that contradicts our religious teachings. The extension of gambling activities to the internet represents a transformation in means, not in nature. Therefore, the legislator stipulated in Article 31: "Anyone who owns or manages a gambling project, or offers, encourages, or facilitates the establishment of a gambling project on the international information network or by any other electronic means, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 10,000 dinars."

Crime of obstructing government operations through electronic means: Article 34 criminalized any act that contributes to obstructing the work of any governmental entity, stating: "Anyone who obstructs the work of public authorities or governmental operations, or hinders them by using any electronic means, shall be punished with imprisonment and a fine not less than 10,000 dinars and not exceeding 100,000 dinars." "Anyone who possesses, plants, or produces programs prepared for this purpose shall be punished with the same penalty." The legislator dealt with this crime from the perspective of the supreme interest of the state, considering any infringement on government operations as a cyber attack on it. The legislator stipulated in Article 39 the criminalization of possessing encryption tools, and in the second paragraph of this article, it stipulated the intensification of the penalty to be imprisonment for a period not less than ten years and a fine not less than fifty thousand dinars and not exceeding one hundred thousand dinars if the acts are related to encryption tools belonging to the government, banks, or military or security institutions. By analyzing the texts of Article 34 and Article 39, we find that the legislator stipulated a harsher penalty for the crime of anyone who produces, possesses, provides, distributes, markets, manufactures, imports, or exports encryption tools belonging to the government, banks, or military or security institutions, compared to the penalty prescribed for the crime of obstructing government operations. This makes the attempt to obstruct government operations, which is represented in obstructing

government operations, harsher than the penalty of the crime itself. The legislator also added in the second paragraph of Article 34: "Anyone who possesses, plants, or produces programs prepared for this purpose shall be punished with the same penalty," which leads to a conflict of legal texts regarding the crime of possessing encryption tools prepared for obstructing government operations in one law, which should not occur in legislation.

Crime of breaking blocking: Article 14 criminalized the possession of decryption programs or tools for unauthorized use, stating: "Anyone who produces, provides, distributes, imports, exports, possesses, or promotes any information program or device, or any information data prepared for displaying passwords or access codes or breaking blocking for the purpose of unauthorized use, shall be punished with imprisonment for a period not less than one year and a fine not less than 1000 dinars and not exceeding 10,000 dinars."

Crime of information trafficking in historical artifacts and antiquities: Article 27 states: "Anyone who establishes or manages a site, or uses an electronic means or the international information network to traffic in historical artifacts or antiquities in unauthorized circumstances, shall be punished with imprisonment." We believe that it would have been better for the legislator to add the penalty of a fine along with imprisonment, to be a greater deterrent for anyone who seeks to obtain illicit money, tampering with the capabilities of the homeland.

Crimes of money laundering through electronic financial transfers: Criminal gangs use money laundering crimes through the internet to evade regulatory and legislative restrictions and control over the sources of money [44]. The legislator criminalized electronic money laundering in Article 44, stating: "Anyone who transfers, moves, or conceals the source of illicit money, or acquires, possesses, or uses such money, knowing that it is derived from an illicit source, by using any electronic means, with the intent of giving it a legitimate character, shall be punished with imprisonment and a fine not less than 10,000 dinars and not exceeding 100,000 dinars." Thus, money laundering crimes committed through the electronic network receive special attention, despite the existence of a specific law to combat money laundering crimes. However, the legislator dedicated a specific text for this crime if it is committed using the international information network, without prejudice to the harsher penalties in other laws.

Crime of assisting terrorist groups: Article 45 states: "Anyone who establishes a site or publishes information on the international information network or any of the electronic means for a terrorist group, shall be punished with imprisonment." We believe that it would have been better for the legislator to intensify the penalty to life imprisonment, as promoting terrorist ideas through electronic platforms is extremely dangerous, affecting the minds of youth and harming the security of the state.

Secondly: Information Crimes Against Public Morals and Ethics

In light of what the electronic space witnesses from the collapse of barriers between countries, it has become possible to promote or broadcast anything that violates public morals and values. The legislator was keen to criminalize every use of electronic means that violates ethical, social, and religious controls.

Crime of publishing or producing obscene materials or promoting them: Article 19 criminalized the production or promotion of obscene materials. It also criminalized the crime of combining and mixing images and voices of individuals in obscene forms, and publishing them by any electronic means in Article 21.

Crime of incitement to prostitution: The legislator criminalized incitement to prostitution in Article 20, stating: "Anyone who encourages or incites another to engage in sexual activities, or contributes to preparing for this matter through the international information network or any other electronic means, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 10,000 dinars." The legislator also criminalized the crime of harassing others to satisfy sexual desire in Article 22.

Crime of exploiting minors: The legislator criminalized the exploitation of minors and mentally and psychologically disabled persons in unethical acts for obscene purposes, using any electronic system in Article 23.

Crime of electronic gambling: Gambling is considered an unethical crime that contradicts our religious teachings. The extension of gambling activities to the internet represents a transformation in means, not in nature. Therefore, the legislator stipulated in Article 31: "Anyone who owns or manages a gambling project, or offers, encourages, or facilitates the establishment of a gambling project on the international information network or by any other electronic means, shall be punished with imprisonment and a fine not less than 1000 dinars and not exceeding 10,000 dinars."

4. CONCLUSION

4.1. FIRSTLY: RESULTS

Weakness of traditional criminal texts in confronting cybercrimes: The Libyan legislator improved by issuing Law No. 5 of 2022 concerning combating cybercrimes, which is considered a step in recognizing the seriousness of this criminal phenomenon and its technical nature.

Fragility of the criminal policy of the Libyan legislator in the Cybercrime Combat Law: It is marred by much contradiction, in addition to the absence of the criminalization aspect for some crimes, and the inadequacy of some penalties for the seriousness of some crimes.

Lack of alignment of Libyan legislation with regional and international agreements: Such as the Budapest Convention and the model Arab legislation, which weakens international cooperation in combating them.

Weakness of infrastructure in data bases in some countries: Some countries lack centers for data response and analysis.

Countries that integrated cybercrimes within their existing laws: These countries sought to preserve the unity of the general criminal law. However, this approach leads to a delay in accommodating the new forms of digital crime.

4.2. SECONDLY: RECOMMENDATIONS

Moving away from the traditional view of criminal legislation: To keep pace with the continuous development in cybercrimes, given its dynamic nature.

Re-drafting the texts of the Libyan Cybercrime Combat Law: To align with regional and international agreements, while avoiding the fragility of drafting, the conflict of texts, and the neglect of the punitive aspect in them, and emphasizing the proportionality of penalties with the seriousness of crimes.

Activating the role of electronic judicial police and establishing specialized courts and prosecutions: To be adequately qualified to keep pace with the rapid development in the commission of these crimes.

Emphasizing the strengthening of international cooperation through binding agreements.

Emphasizing the protection of electronic transfers and deposits by a specialized committee: In each banking institution, to combat electronic crime in the banking sectors.

Paying attention to the development of digital protection programs: As much as attention is paid to technological development.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Abdel-Haq Bassou, Information Terrorism in Moroccan and International Law, Research for the Special Course on Combating Information Crimes, Naif Arab University for Security Sciences, 2006, p. 15.

Dr. Abdel-Fattah Bayoumi Hegazy, Principles of Criminal Procedures in Computer and Internet Crimes, Dar Al-Fikr Al-Jami'i, First Edition, 2006.

Dr. Abdel-Wahab Mohamed Abdel-Wahab, Legal Aspects of Artificial Intelligence.

Dr. Ahmed El-Sayed Mohamed El-Husseini, Procedural Aspects of Crimes Arising from the Use of Electronic Networks, Dar Al-Jame'a Al-Jadeeda, 2019.

Dr. Ahmed Jaber Al-Gazzar, Cybersecurity, Dar Al-Majmoua Al-Ilmiyya for Printing, Publishing and Distribution, 2024, p. 30.

Dr. Ahmed Lotfi El-Sayed Marei, Digital Evidence Obtained from Electronic Criminal Inspection, Dar Al-Ahram, 2024.
Dr. Ahmed Mohamed El-Sayed, Dr. Mohamed El-Gendy, Cybercrimes between Theory and Practice, Dar Al-Sahab for Publishing and Distribution, 2023.
Dr. Ali Ne'ma Jawad Al-Zarqi, Information Crime Affecting Private Life: A Comparative Study, Modern University Office, Iraq, 2020.
Dr. Amir Faraj, The Authority of the Criminal Judge in Evaluating Electronic Evidence, Dar Al-Matbou'at Al-Jami'iyya, 2024.
Dr. Arab Younis, Computer and Internet Crimes, 2001, Union of Banks Publications, 2001.
Dr. Ashraf Abdel-Qader Qandil, Electronic Means and Their Role in Criminal Evidence: A Comparative Study, Dar Al-Jame'a Al-Jadeeda, 2018.
Dr. Chokri Al-Derbali, Ali Al-Alawi, Provisions of the Crime of Defamation via Social Media Sites in Islamic Jurisprudence and Tunisian Legislation, Majma' Al-Atrash, 2020, Tunisia.
Dr. El-Said Abdel-Hamid Ibrahim, International Laws and Agreements in Confronting the Risks of Cyber Attacks, Dar Al-Ilm wa Al-Iman, 2025.
Dr. Emad Hussein Al-Freihat, Criminal Responsibility for Crimes of Electronic Blackmail of Persons in Light of Jordanian and Tunisian Law (A Comparative Study), Majma' Al-Atrash, 2024.
Dr. Fathi Tawfiq Al-Faouri, Explanation of the Cybercrime Law, Dar Wael for Publishing.
Dr. Hussein Abdel-Karim Younis, Dr. Khalil Youssef Al-Gendy, Electronic Blackmail and Cybercrimes: Concept and Causes, Dar Kafa'at Al-Ma'rifa, 2021.
Dr. Jamal Mohamed Gheitass, Information Security and National Security, Dar Al-Nahda Al-Arabiya, First Edition, 2007.
Dr. Khaled Mamdouh Ibrahim, Information Crimes, Dar Al-Fikr Al-Jami'i, 2019.
Dr. Mahmoud Ragab Fathallah, The Mediator in Electronic Crimes, Dar Al-Jame'a Al-Jadeeda, 2019.
Dr. Mohamed Abdel-Rahim Sultan, Internet Crimes and Fraud, Conference on Law, Computer and Internet from May 1 to 3, 2000, United Arab Emirates University, Faculty of Sharia and Law, Volume Three / Third Edition / 2004.
Dr. Mohamed Abdullah Al-Owa, Internet Fraud and Credit Card Crimes between Legislation and the UAE Judiciary, Dar Al-Nahda Al-Arabiya, 2019.
Dr. Mohamed Al-Shalabi Al-Ma'toum, Information Technology Crimes: General Theory of Electronic Crimes, Dar Al-Thaqafa Al-Arabiya for Publishing and Distribution, 2023, Amman, Jordan.
Dr. Mohamed Amin Al-Shawabkeh, Computer and Internet Crimes, Dar Al-Thaqafa for Publishing and Distribution, Fourth Edition, 2011.
Dr. Mohamed Oulad Belhaj, Scientific Evidence and Its Legitimacy in Criminal Evidence, Dar Al-Afaq Al-Maghribiya, 2023.
Dr. Monia Bin Tradit Ghamarsa, Informatics and Tunisian Penal Law through the Window and Decree No. 54 of 2022, Dar Al-Kitab Al-Tunisi, 2024.
Dr. Mounir Mohamed Al-Janbihi, Difficulties of Investigation and Extraction of Evidence in Information Crimes, Dar Al-Fikr Al-Jami'i, 2019.
Dr. Nahla Abdel-Qader Al-Momani, Information Crimes, Dar Al-Thaqafa, First Edition, Amman, 2007. Laws, Journals, and Conferences:
Dr. Naila Fouda, Economic Computer Crimes, Halabi Legal Publications, Beirut.
Dr. Nisreen Mohsen Ne'ma Al-Husseini, Mohamed Hassan Marei, Electronic Crimes Against Property, New University Office, 2020.
Laws of the House of Representatives for the year 2022 - Libyan House of Representatives (ly.parliament), see also the Official Gazette of the Libyan House of Representatives (ly.parliament).
Lawyer Nasr Shoman, Modern Criminal Technology and Its Importance in Criminal Evidence, 2011, All rights reserved to the author.
Maghreb Law Journal, Issue 32, September 2016, Dar Al-Salam Al-Najem Koban Press, Rabat.