Cybercrime under the New Iraqi Draft Cybercrime Law

Suad Shakir Baeewe
Faculty of Law, University of Al-Qadisiyah, Iraq
suad.alisawee@qu.edu.iq

Abstract:
Notwithstanding the big role of contemporary technologies, they are not without negatives, containing the emergence of different and modern forms of offences. In addition, determining the legal nature of these offences cannot be complete based on the general rules in criminal legislation, due to the inability of the current penal texts or its failure to apply to modern forms of these offences. In addition, the need for special procedural provisions is occasionally different from the provisions that can used in traditional offences, particularly those related to criminal evidence. The absence of a special act dealing with electronic offences leads to the widening of the judge's authority to interpret penal texts and this violates the principle of legality, which obligatory the intervention of the Iraqi criminal legislator to legislate a special act to address these offences. Providing individuals with legislative protection from misuse of these devices protects the interests of individuals, and ensures a balance between the individual's interest in using these technologies and their interest in protecting their lives, properties and private lives from misusing them. However, this act, when it was first reading in the Iraqi parliament in 2011, faced many criticisms and objections that necessitated amendments to its draft before re-discussion and approval, so we will try in our research to diagnose the most important weaknesses in it and propose its correction to meet the requirements of justice.

Keyword: Crime, Cybercrime, Punishments.

Introduction:

Since the emergence of the Internet and Iraq's participation in this global phenomenon, there has been a rapid increase in the number of crimes committed on the Internet using various platforms. Cybercrime has become widespread at present, [1] and the most common crimes are fraud and extortion, because of the high unemployment rate and other social factors that have led young people to explore their skills in cyberspace and how they can benefit from those skills without discovered by the competent government authorities.

The rate of cybercrime in Iraq has increased significantly after 2003, and many types of activities have emerged that may constitute a crime under the draft information crimes act. This act is the latest form of legislation that fights cybercrime in Iraq. Moreover, this study aims to identify cybercrime and clarify the objective provisions of it, such as the types of cybercrime dealt with by the draft law in an attempt to analyses the main provisions of this law, and to clarify the controversial provisions in it, as well as to provide several conclusions and recommendations regarding it.

The importance of this research is evident in that it will provide the government, the legislator, and policymakers in the country with a useful vision while trying to reach feasible and effective solutions to amend the disputed texts, which caused widespread controversy in the legal and popular circles when it read in the Iraqi Parliament the first time.

In addition, this research would support law enforcement agencies further to curb cybercrime by providing suggestions and recommendations regarding sound legal methods that must be follow when investigating. Moreover, electronic evidence differs from the mechanism for deal with traditional crimes regulated by the Criminal Procedure Law, as well as in preparing to confront cybercrimes in Iraq.

During this research, the descriptive approach will be adopt due to the nature of this study, which requires reliance heavily on books and research as well as articles written in this field via the Internet. As well as the analytical approach that is used to analyze the texts of the draft law understudy to show the weaknesses and strengths of its texts in an attempt to put some recommendations that enable the Iraqi legislator to correct its course before the law is approved in its final form.

Definition of Cyber Crime

Cybercrimes are among the new crimes that have appeared recently, and the reason is due to the association of these crimes with modern technologies such as computers, Internet networks and websites. [2] The definition of cybercrime varies according to the perspective through which it viewed [3] so; the researcher will touch upon a set of definitions that dealt with cybercrime (information).

1. Some researchers define it as "every unlawful behavior that uses the computer or an attempt to copy, delete or destroy computer programs, or any crime whose implementation is related to rules or information sciences" [4, 5]
2. Moreover, some of them see that "Criminal activity that uses digital electronic technology, directly or indirectly, as a means to carry out a criminal act or to facilitate the criminal process." [6, 7, 8]
3. While there are many of them that cybercrime "unlawful behavior, It is directed towards the misuse of the automated system for processing data using a computer or any other technical means" [9, 10, 11].
4. As some others see that, "every act intended, positive or negative aimed to attacking information technology, whatever the perpetrator's purpose" [12, 13].

Finally, cybercrime can be define as every unlawful behavior that takes electronic means as the object of assault or as a tool to carry out a crime punishable by law.

Types of Electronic Crimes

The legitimacy of criminalization and punishment is one of the most important foundations on which the criminal law based in the framework of work to protect the fundamental interests of society; also, that criminalization is the feature that the criminal law has to protect those interests as this feature distinguished by it from other laws. [14]

The increase in cybercrime as a relatively recent criminal phenomenon constitutes a great alarm bell that requires societies to predict this danger because they target data, information, and programs of all kinds to attack them, as it considered a crime in which modern technologies are used. The stored information, as well as the information transmitted through information systems and networks, foremost of which is the Internet. [15] The victim in cybercrimes may be a natural or moral person. [16]

Therefore, the cybercrimes in the prospective information crime law divided into two categories, which are crimes against the state and its institutions, the public interest of society, crimes directed against individuals and their interests, and we address that in some detail in two requirements.

Crimes against the State, and the General Interest of Society

As it included many acts that considered under this law to be crimes, namely:

Infringement of the safety, the unity, and the independence of the state, or prejudice to the interests of the country, or cooperating with parties hostile to the country or exposing it to risks.

In addition to the use of computer devices or the information network of the security authorities to damage them or copy them, or to send their contents to a hostile party, or to benefit from them to carry out crimes against state security or facilitate the concealment of the features of those crimes. Spreading incorrect facts harm the economy and the financial confidence of the state.

Deciphering a computer, information network, an electronic card owned by the state departments. Forgery, counterfeiting concerning signatures, bonds, records, restrictions, or electronic cards related to the rights of the state and the public sector if committed by an employee or person charged with a public service while performing the duties of his job or because of it.

Refrain from providing the competent authorities with the electronic information and programs they request, in a manner that does not conflict with intellectual property rights. Establishing or managing websites to carry out or promote terrorist operations, stirring up armed rebellion, or inciting sectarian or sectarian strife.

Crimes against Individuals and Their Interests

It included many acts that considered criminal acts under this law, as follows:

Using fraudulent methods to seize programs, data in any electronic transaction or contract, or electronic signature or record related to the rights of others. In addition, use a trademark registered in the name of others with the intent to deceive, or he used his electronic card as a means of fulfillment

knowing that it was not valid, or he used the financial card of others without the knowledge of its owner.

It includes money laundering, threats, and extortion by using the electronic means. Besides, attacks on intellectual and literary rights and scientific research belonging to others using the information network that protected by special laws, and international agreements. Moreover, the use of the computer and the information network to commit defamation and insult crimes.

Moreover, creation or management of sites that promote incites prostitution, and activities contrary to public morals. It also considered among the crimes covered by this law, the use of an employee or a person charged with public service for his job to sell, transfer or circulate personal data without permission from its owners and to achieve material benefit for him or others. Finally, disclosure of the secret by an employee during or because of job without a justification issued by a competent official authority.

The Legislative Policy

The legislative policy defined as the main ideas and goals to be achieved that guide law in its creation and implementation stages. [17] As for the criminal policy, it is the set of rules and principles in the light of which determines the drafting of the provisions of the criminal law, whether with regard to criminalization, prosecution, prevention and treatment. [18]

To find out the tired legislative policy by the Iraqi legislator when proposing the draft law, and to explain its characteristics, we decided to divide this phase into two requirements. In the first requirement, we will discuss the punitive texts in the cybercrime draft. As for the second requirement, we will devote it to critical analysis of the texts of the draft law to show its aspects, weakness and strength.

Punitive Texts in the Draft of cyber Crimes

The draft act stipulated strict penalties for any violation of the provisions of the law related to the internal and external security of the state. As well as security and public order as well as the protection of the interests and rights of individuals, which indicates. The Iraqi legislator adopted a policy of strictness in punishing perpetrators of electronic crimes. And it may have a justification for that, which is to create a kind of protection and immunity for institutions and individuals that deal within the scope of the

electronic environment and deter those who are involved in this type of crime, and it was as follows;

Life imprisonment and fines

The life sentence repeated in articles (3, 4, 5, and 6) and included some crimes ranging from undermining the unity of the country and its interests. [19] As for the amount of the fine, a fine was imposed in addition to the life imprisonment between (25-50) million dinars in articles (3, 4, 6), but in the article (5) notice the fine was higher at a minimum of (30) million dinars and the maximum limit was reduced to 40 million dinars.

Temporary imprisonment without specifying the period with a fine

Articles (7, 8) dealt with imposing temporary imprisonment with a fine in the case of using computer systems or an information network to seize the money of others by using electronic means or using fraudulent methods to seize program, information, data, or codes in any electronic transaction or contract.

Also, forgery and imitation for signatures, bonds, records and electronic cards, [20] as well as when destroying, removing or decrypting an electronic signature or computer devices or information network or card belonging to state departments and public institutions. [21]

As for crimes related to prostitution and activities contrary to public morals, the legislator imposed, in addition to a prison sentence, a fine between (10-30) million dinars in Articles (22, 17 / Second) of the law, and in Article (8 / First, 17 / Second) in addition to imprisonment, a fine between (10-15) million dinars was imposed.

Temporary imprisonment for a limited period of no less than or more than ten years with a fine

Article 8, stipulates the crime of forgery ,imitation, and Artificiality for signatures, bonds, records, and electronic cards, with an increased penalty to imprisonment for a period not exceeding (10) years and a fine between (10-30) million dinars in two cases;

The first case, if the crime related to the rights of the state, the public sector, or private entities of public benefit.

The second case, if an employee committed the crime charged while performing his job or because of it.

As for Article 9, the legislator stipulated that, in the case of deliberate seizure, a signature, document, or electronic record related to the rights of others. As for Article (20 / Second), it included imposing a prison sentence of no more than (10) years and a fine of between (5-10) million dinars, if he used with intent to fraud for a trademark registered in Iraq in the name of others. Or used his electronic card, as an instrument of fulfillment with his knowledge it was not valid due to the expiration of the validity period, lack of balance in it, cancel it if the perpetrator is an employee or assigned to public service.

Temporary imprisonment for period of no less than or more than seven years with the fine

The legislator has singled out Article 10 of the draft law to deal with the crime of money laundering using electronic means. It punished by imprisonment for no less than (7) years and a fine of between (10-30) million dinars. Divulging a secret crime by an employee through his job or because it. Or, using his capacity to sell, transfer or circulate personal data without the permission of its owners, it shall be punished with imprisonment for a period not exceeding (7) years and a fine between (5-10) million dinars. [22]

The legislator dealt in Article (11 / First) with the crime of threatening and extorting a person to intimidate him or to compel him to do or refrain from doing an act and this threat is to use the information network or electronic means, imposing a prison sentence of no more than (7) years with a fine between (3-5) million dinars. Likewise, the imposition of imprisonment for a period not exceeding (7) and a fine of between (25-50) million dinars or one of these two penalties in the case that correspondence is intercepted through computers or information network without any right, and used to achieve a financial benefit. [23]

Article (18/Third) dealt with the employee providing electronic information or data to the judicial and administrative authorities, knowing that they are not correct, refusing to provide them, or impersonating a capacity or name that he does not have with the intention of fraud. Or his establishment or use of a fictitious website on the information network to commit one of the crimes stipulated in this law, if the false information, name or characteristic relates to a public employee or government department, the

penalty will be imprisonment for a period not exceeding (7) years And a fine ranging between (15-20) million dinars.

Unlimited Imprisonment with a Fine

The legislator deals with the crime of breach of trust committed by the guardian or trustee to misappropriate, use or disposing of it for his benefit or the interest of others in it, and according to Article (9/Second), he shall be punished with imprisonment with a fine ranging between (3-5) million dinars. In addition, the legislator sought to protect the electronic certification certificate in two cases:

In the first case, a prison sentence imposed with a fine of between (3-5) million dinars, for anyone who created, published, or provided an invalid electronic certificate. [24]

The second case provides incorrect information to an entity that conducts the activities of issuing an electronic certification to obtain the electronic certificate, cancel it, or stop its validity by imposing a prison punishment with a fine of between (3-10) million dinars. [25]

Article (15/First) dealt with the crime of intercepting data and information during their exchange, the case of deliberately exceeding the scope of the authorized permit, eavesdropping and monitoring data and information stored or exchanged in the information system by imposing a prison sentence with a fine between (10-15) million dinars.

Likewise, in Article (18/First), the legislator imposed on anyone who provides electronic information or data to the judicial and administrative authorities with knowledge of their inaccuracy or reluctance to provide data and information with a penalty of imprisonment with a fine between (5-10) million dinars.

Article (20/First), it includes imposing a prison sentence and a fine of between (2-5) million dinars, for everyone use a trademark registered in the name of others with the intent to cheat. Or use his electronic card as a means of fulfillment, knowing that it is not valid due, or using a third party's financial card without the knowledge of its owner.

Fixed-term imprisonment of no less than four years and a fine

Article (15/second), deals with the intercepting data, information during their exchange. And the case of deliberately exceeding the scope of the authorized permit, eavesdropping, monitoring data and information stored

or exchanged in the information system if it results to sabotage, alteration or re-publication of data and information belonging to others without right, by imposing a prison sentence with fine between (15-25) million dinars.

Fixed-term imprisonment of no more than three years with a fine

Article (14 / First) deals with the protection of individuals financial and moral rights in bonds, documents, electronic cards that prove rights, as well as commercial and financial papers, electronic records and the like.

Likewise, (14/third) dealt with the crime of the computer operator or his supervisor intentionally destroying, disrupting or impeding computer hardware, systems, programs, or networks, as well, hackers who access computers or the information network without permission, and anyone who prevents their users from using them, is punished with imprisonment and a fine of between (2-5) million dinars.

As for Article (17/First), it includes imprisonment as well as a fine of between (5-10) million dinars for the crime of destroying, removing or decoding an electronic signature, computer devices, information network, or an electronic card belonging to others. Moreover, the legislature has dealt with the crime of violating the intellectual and literary rights and scientific research of others that protected by special laws and international agreements by using the information network and copying or publishing it.

Unauthorized access to the website of any company or institution to change design of the site, modifying, destroying or exploit without right, and imposing a penalty of imprisonment for no less than (2) years and not more than (3) years with a fine between (10-20) million dinars. [26]

The legislator also dealt with the crime of establishing or assisting in establishing or managing an information network site for gambling or promoting it, by imposing a prison sentence for a period not exceeding (3) years with a fine of between (3-6) million dinars [27].

Determination of imprisonment for no more than two years and a fine

The legislator punished the crime of insulting and defamation using electronic means according to Article (22/third), where it imposed a prison sentence of no more than two years and a fine of between (3-5) million dinars.

Detention for a fixed period of not less than one year and a fine

The legislator tried to organize the protection of religious, ethical, social and family principles and values and the sanctity of private life from assaulting it using the information network or computer equipment and in any form of the forms, by imposing a prison sentence with a fine of between (2-5) million dinars. [28]

In addition, a prison sentence of no less than (1) year and no more than (2) years, along with a fine between (3-5) million dinars, for the production, sale, import or distribution of any device, tools or computer programs, or passwords or entry codes used to commit one of the crimes stipulated in this law. [29]

The Fine

Article (13/3) included the crime of refraining from providing the security authorities and the competent authorities to grant licenses with what they require of electronic information, reports and data, whenever they are relate to the activity they are practicing and not in conflict with intellectual property rights, by imposing a fine between (3-5) Million dinars. As for Article (21/Second), a fine was imposed between (500 thousand - one million) dinars for copying, publishing or circulating programs or information without a license**.**

A Critical Analysis of the Punitive Texts

This part of the study aims mainly at a critical analysis of the punitive texts of the draft information crimes law. However, before starting to describe the draft law, we must carefully consider the designation of the law itself, which should be ***"Cyber Crime Law"***. Because the term information crimes relate only to crimes committed concerning the information.

Thus does not cover all the crimes mentioned in the draft law that relied on criminalizing forms of behavior and acts that carried out using devices and means of communication to commit crimes contained therein. The draft law contains (31) legal articles distributed as follows;

The First Section

It included only two articles, namely, definitions and objectives, and in reality one legal article for definitions. It is the first article and included fifteen definitions of the terms mentioned in the law. These definitions characterized by the testimony of the International Organization for Human

Rights, that they are broad definitions. [30] It did not define information crime or cybercrime.

The purpose of the law was also included in one legal article, which is the second article of the law, providing the necessary legal protection for the legitimate use of the computer and the information network, as well as punishing the perpetrators of acts that constitute an assault on the rights of users. However, this is incomplete in the draft law because it accepted in Iraqi laws that the purpose of any specific legislation is for positive reasons. The purpose of the legislation stated again in positive reasons. Therefore, we see that Article (2) of the draft is not necessary.

The Second Section

Includes punitive articles, 21 penal articles were included in Article (3-23), which included a sum of acts and forms of conduct that were considered crimes under the draft law and the penalties prescribed for each were included. When reading the draft law, we note; the life imprisonment penalty mentioned in Articles (3, 4, 5, and 6).

Article (3/First-B) included the phrase (in any form of forms), which was a broad term and loosely interpreted and explicable, and the hermeneutics, which may make the citizen placed under penalty of criminal responsibility without specifically addressing the type of criminal behavior that is considered under the concept of this article is cooperation with entities hostile to the country.

Articles (4 and 5), we believe that the legislator was successful in providing a harsh punishment with a fine, for the person who runs or establishes a site to spread terrorist ideas or to contact the leaders of terrorist groups, or to promote them, because of what the country has suffered and is suffering from terrorist acts. As well as in related crimes Human and drug trafficking and promoting them as one of the most serious crimes in society.

Article (6) listed a set of acts and forms of criminal behavior, some of them do not require cruel punishment, like its first and third paragraph, it can prevent any discussion about the economic, administrative, financial system of the state. In addition to criticizing it, because it came with vague terms that cannot be predicted in the interpretation of its meaning, or a mechanism to verify it and the competent authority to do so, such as (disturbing security and public order) as well as (insulting the reputation of the country). It also

threatens debate based on facts and documents aimed at encouraging reform and the advancement of the country.

Article (11) punished for the crimes of intimidation and extortion that affect individuals using electronic means, which is a successful step towards creating a legal legislative framework to confront the crimes of extortion and electronic threats. It also helps the judicial authorities to get rid of the state of analogy with their traditional crimes counterparts, which may sometimes be difficult to adapt to these traditional texts to confront these non-traditional crimes.

Article (21/first) in its current form, it is capable of imposing most of the recipients of information (researchers and writers) and others under penalty of this article and punishable by a penalty of up to (3) years and a fine of up to (20) million dinars. Therefore, this text must amended by adding the phrase (without permission, or without a clear reference to the owner of those intellectual or literary works or scientific research). The purpose of this legal article is to protect intellectual property, but this protection must formulate in a manner that does not prevent others from benefiting from it with reference to the actual owner of that intellectual property.

The third paragraph of the same article came in vague and unspecified terms by criminalizing every assault on any of the religious, ethical, social and family principles or values and the sanctity of private life using the information network or computer devices and in any form. we noticed that the phrase (assault on any of the principles ....) and the phrase (in any form) had appeared, because these expressions are vague and floating, if the legislator does not refrain to setting specific definitions for them, they may lead to the possibility of placing persons under legal liability.

Article (23) came in broad and indeterminate terms, for many of the acts that include imposing criminal liability on anyone who produced, sold, imported, or distributed any device, tools, computer programs, passwords, or access codes that led to the commission of one of the crimes stipulated in this law. Without specifying the parameters, that enable citizens to know the criminal acts.

The Third Section

Contains (3) legal articles related to procedures for collecting evidence, investigation and trial. Committing cybercrime leaves digital footprints. Unlike physical evidence, these digital fingerprints are not visible, or they are visible by default, and of a fluctuating nature. [31]

Article (24) does not include a reference to addressing investigation procedures and collecting evidence by a competent authority for this type of crimes, meaning that the specificity of these crimes does not take into account, meaning the necessity for specialized bodies to deal with investigation tasks and collect evidence in this type of crimes.

Article (25) of it has entrusted the task of adjudicating in this type of crimes to the misdemeanor and felony courts for (3) years from the date of the law's enforcement, with one or more judges with experience to look into these cases after undergoing special training, each according to his jurisdiction.

Article (26) included the powers of the competent judge to order the preservation of data or to order the submission of subscription or traffic data to the investigating authorities with access to computers, networks and stored data. It has the power to track information, computer systems and networks, with the power to control computers, any part of them or any means by which data is stored. It is clear to us from the content of the above article that the legislator has given very broad powers to the judge without referring to controls for the use of these powers, which are regulated by special instructions,

The Fourth Section

It contains the final judgments, which are as follows:

Article (27) referred to the application of the penalties stipulated in this law without prejudice to the possibility of increasing the penalty that may be contained in the laws in force. This reference considered one of the advantages of this law, as this law did not consider an obstacle to imposing the most severe penalties contained in the relevant laws. [31], included provisions of liability for the legal person, and referred them to the Penal Code, regarding the crimes contained in this law.

Article (29), the legislator gave the court the power to confiscate or destroy tools, devices, or programs used in committing electronic crimes

without prejudice to the rights of the other in good faith. It noted that the legislator in this article recognizes the rights of the other in good faith, the owner of those tools or programs that used in the commission of this type of crime and preserves them from destruction or confiscation if it proven before the court that he was in good faith.

Article (30) referred to the application of the provisions of the Penal Code and the Code of Criminal Procedure in every case for which no provision made in this law. This article is also in addition to the advantages of the law, which it did not leave a legislative void when one of its provisions was deficient, so it becomes possible to refer to the above-mentioned organizing laws.

Article (31) there of indicated that the law would come into effect after the lapse of (90) days after the date of its publication in the official newspaper. This is an important and necessary point, especially if we look at the nature of the law and the acts that criminalize it. This period is sufficient for individuals to acquaint themselves with its content to know the criminal acts therein to avoid falling under penalty of criminal responsibility .

Conclusions and Recommendations

The naming of the act as "the Information Crimes Law" is unsuccessful because the term "***information crimes***" relates only to crimes committed concerning the information. Thus does not cover all the crimes mentioned in the draft act that relied on the criminalization of forms of behavior and actions taken from the use of devices and means of communication a means to commit the crimes contained therein.

The provisions contained therein are not clear in prohibiting a specific behavior, but rather depend on a vague description statement that government officials will decide on its application in the event of its occurrence, without referring to any specific standards that can guide behavior in advance in any litigation under the law. Cybercrime does not differ from other only in terms of the method of its commission (by using means Electronic).Therefore**,**

Recommendations of this research that:

Redefining the terms, and making sure of their correctness. Moreover, the accuracy of the vocabulary, concepts contained therein, and removing the ambiguity and ambiguity that afflicts many of its clauses. In addition, the competent authorities should set policies and programs as guides for

investigating cybercrime and what should do if the security of the state exposed to danger. Finally, Training police personnel on modern information and communication technology, and creating awareness about the steps that must take to prevent and protect the electronic system from electronic attacks.

References

1- Rabhi, Aziza, 2018, ***Information Secrets and their Criminal Protection***, Abu Bakr Belkaid University, Faculty of Law and Political Science, Algeria, P 95.
2- Al- Hawamdeh, Lawrence Said, 2017, Informatics Crimes and The Control Of Combating It (Comparative Analytical Study), ***Al-Mezan Journal of Islamic and Legal Studies***, Volume 4, Issue 1, Jordan, pp (183-220), P 188.
3- Al-Thunayan, Thunayan Nasser, 2012, ***Evidence of Electronic Crime (An Applied Fundamental Study***, Naif Arab University for Security Sciences, P 19.
4- Al-Rasheed, Ghazi Abdel-Rahman Hayan, 2004, ***Legal Protection from Information Crimes (Computer and Internet)***, Islamic University of Lebanon, Faculty of Law, P 106.
5- Omar, Nair Nabil, 2012, ***Criminal Protection of the Electronic Shop in Information Crimes***, New University House, Cairo, P 23.
6- Al-Yousef, Abdullah bin Abdul Aziz, 1999, ***New Criminal Phenomena and Ways to Confront them***, Naif Arab University for Security Sciences, Saudi Arabia, P 13.
7- Moussa, Mustafa Mohamed, 2003, ***Criminal methods of digital technology, what it is, and combating it***, Dar Al-Nahda Al-Arabiya, Cairo, P 56.
8- Hegazy, Abdel-Fattah Bayoumi, 2006, ***Criminal Evidence and Forgery in Computer and Internet Crimes***, Dar Al-Kotob Al-Legal, Egypt, P 1&2.
9- Rustum, Hisham Mohamed, 1994, ***Procedural aspects of information crimes***, Modern Machines Library, Assiut, Egypt, P 29&30.
10- AL- Safu, Nofal Ali Abdullah, 2015, The Crime of Establishing a Site or Publishing Information That Violates Public Morals Through Information Technology (Comparative Study), ***The Egyptian Journal of Legal and Economic Studies***, Issue 3, Egypt, pp.8-59, P 19.
11- Fatih, Raad Fajr & Awad, Yasser, 21017, Evidence of Electronic Crime by Scientific Evidence, ***Tikrit University Journal of Law***, Year 1, Volume 1, Issue 3, Part (2), p. 476-506, P 478.

12- Al-Hiti, Muhammad Hammad Maharaj, 2004, ***Modern Technology and Criminal Law***, Dar the culture For Publishing and Distribution, 1st Edition, Amman, P 152.
13- Yusef, Amir Farag, 2008, ***Cybercrime on the Internet***, University Press House, first edition, Alexandria, Egypt, P 106.
14- Rabiaa, Abdul Latif, 2016, ***Cybercrime (criminalization, prosecution and Evidence)*** , research presented to the first conference on cybercrime held at An-Najah University, Palestine, P 6.
15- Arab, Younis, 2002, ***computer and internet crimes***, working paper submitted to the Arab Security Conference, Organization of the Arab Center for Criminal Studies and Research, United Arab Emirates, P 10.
16- Bou El-Tameen, Elham, 2018, ***Criminal Evidence in Cybercrime***, Al-Arabi Mehidi University, Faculty of Law and Political Science, Algeria, P 17.
17- Rabiaa, Abdul Latif, 2016, ***Cybercrime (criminalization, prosecution and Evidence)*** , research presented to the first conference on cybercrime held at An-Najah University, Palestine, P 18.
18- Sorour, Ahmed Fathy, 1972, ***the Origins of Criminal Policy***, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, P 10.
19- Article 4 / first, draft information crimes law.
20- Article 8 / first, draft information crimes law.
21- Article 17/ second, draft information crimes law.
22- Article 19/ second, draft information crimes law.
23- Article 16, draft information crimes law.
24- Article 12 / first, draft information crimes law.
25- Article 13/ second, draft information crimes law.
26- Article 21 / first, draft information crimes law.
27- Article 22 / first, draft information crimes law.
28- Article 21 / third, draft information crimes law.
29- Article 23, draft information crimes law.
30- Human Rights Watch, 2012, Iraq: ***The Cybercrime Law Violates Freedom of Expression Vague provisions and harsh penalties threaten media and activists, p1.***
31- Abdul-Baqi, Mustafa, 2018, the Investigative and Evidence of Cybercrime in Palestine: A Comparative Study, ***Journal of Sharia and Law Studies***, Volume 45, Issue 4, Appendix 2, pp. 284-29, p. 292

32- Article 23, draft information crimes law.

Sources

Abdul-Baqi, Mustafa, 2018, the Investigative and Evidence of Cybercrime in Palestine: A Comparative Study, ***Journal of Sharia and Law Studies***, Volume 45, Issue 4, Appendix 2, pp. 284-29.

Al- Hawamdeh, Lawrence Said, 2017, Informatics Crimes and The Control Of Combating It (Comparative Analytical Study), ***Al-Mezan Journal of Islamic and Legal Studies***, Volume 4, Issue 1, Jordan, pp (183-220).

Al-Hiti, Muhammad Hammad Maharaj, 2004, ***Modern Technology and Criminal Law***, Dar the culture For Publishing and Distribution, 1st Edition, Amman.

Al-Rasheed, Ghazi Abdel-Rahman Hayan, 2004, ***Legal Protection from Information Crimes (Computer and Internet)***, Islamic University of Lebanon, Faculty of Law.

AL- Safu, Nofal Ali Abdullah, 2015, The Crime of Establishing a Site or Publishing Information That Violates Public Morals Through Information Technology (Comparative Study), ***The Egyptian Journal of Legal and Economic Studies***, Issue 3, Egypt, pp.8-59.

Al-Thunayan, Thunayan Nasser, 2012, ***Evidence of Electronic Crime (An Applied Fundamental Study***, Naif Arab University for Security Sciences.

Al-Yousef, Abdullah bin Abdul Aziz, 1999, ***New Criminal Phenomena and Ways to Confront them***, Naif Arab University for Security Sciences, Saudi Arabia.

Arab, Younis, 2002, ***computer and internet crimes***, working paper submitted to the Arab Security Conference, Organization of the Arab Center for Criminal Studies and Research, United Arab Emirates.

Bou El-Tameen, Elham, 2018, ***Criminal Evidence in Cybercrime***, Al-Arabi Mehidi University, Faculty of Law and Political Science, Algeria.

Fatih, Raad Fajr & Awad, Yasser, 21017, Evidence of Electronic Crime by Scientific Evidence, ***Tikrit University Journal of Law***, Year 1, Volume 1, Issue 3, Part (2), p. 476-506.

Hegazy, Abdel-Fattah Bayoumi, 2006, ***Criminal Evidence and Forgery in Computer and Internet Crimes***, Dar Al-Kotob Al-Legal, Egypt.

Human Rights Watch, 2012, Iraq: ***The Cybercrime Law Violates Freedom of Expression Vague provisions and harsh penalties threaten media and activists***

Kandil, Ashraf Abdel Qader, 2015**,** ***Criminal Evidence in Cybercrime***, Dar the New University, Alexandria.

Moussa, Mustafa Mohamed, 2003, ***Criminal methods of digital technology, what it is, and combating it***, Dar Al-Nahda Al-Arabiya, Cairo.

Omar, Nair Nabil, 2012, ***Criminal Protection of the Electronic Shop in Information Crimes***, New University House, Cairo.

Rabhi, Aziza, 2018, ***Information Secrets and their Criminal Protection***, Abu Bakr Belkaid University, Faculty of Law and Political Science, Algeria.

Rabiaa, Abdul Latif, 2016, ***Cybercrime (criminalization, prosecution and Evidence)*** , research presented to the first conference on cybercrime held at An-Najah University, Palestine

Rustum, Hisham Mohamed, 1994, ***Procedural aspects of information crimes***, Modern Machines Library, Assiut, Egypt.

Sorour, Ahmed Fathy, 1972, ***the Origins of Criminal Policy***, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

Yusef, Amir Farag, 2008, ***Cybercrime on the Internet***, University Press House, first edition, Alexandria, Egypt.

الجرائم الالكترونية في ظل مسودة قانون الجرائم الالكترونية الجديد

م.م سعاد شاكر بعيوي
كلية القانون، جامعة القادسية، العراق
suad.alisawee@qu.edu.iq
009647825814505

مستخلص البحث:
على الرغم من الدور الكبير للتقنيات المعاصرة ، فهي لا تخلو من السلبيات ، حيث تحتوي على ظهور أشكال مختلفة وحديثة من الجرائم. بالإضافة إلى ذلك، لا يمكن تحديد الطبيعة القانونية لهذه الجرائم بناءً على القواعد العامة في التشريع الجنائي، بسبب عدم قدرة النصوص الجنائية الحالية أو عدم تطبيقها على الأشكال الحديثة لهذه الجرائم. بالإضافة إلى ذلك ، فإن الحاجة إلى أحكام إجرائية خاصة تختلف أحيانًا عن الأحكام التي يمكن استخدامها في الجرائم التقليدية، لا سيما تلك المتعلقة بالأدلة الجنائية. يؤدي عدم وجود قانون خاص بالتعامل مع الجرائم الإلكترونية إلى توسيع صلاحيات القاضي في تفسير النصوص الجزائية، وهذا يخالف مبدأ الشرعية الذي يلزم المشرع الجنائي العراقي بتدخل تشريع خاص لمعالجة هذه الجرائم. إن توفير الحماية التشريعية للأفراد من سوء استخدام هذه الأجهزة يحمي مصالح الأفراد، ويضمن تحقيق التوازن بين مصلحة الفرد في استخدام هذه التقنيات واهتمامهم بحماية حياتهم وممتلكاتهم وحياتهم الخاصة من إساءة استخدامها. إلا أن هذا القانون عند قراءته الأولى في مجلس النواب العراقي عام 2011 واجه العديد من الانتقادات والاعتراضات التي استدعت تعديله قبل إعادة مناقشته وإقراره، لذلك سنحاول في بحثنا تشخيص أهم نقاط الضعف فيه. واقتراح تصحيحه بما يتلاءم مع مقتضيات العدالة.

الكلمات المفتاحية: الجريمة، الجرائم الالكترونية، العقوبات