International Journal of Law and Society
Volume 2, Number 2, April 2025
e-ISSN: 3046-9562; and p-ISSN: 3046-9619; Pages. 211-229
DOI: https://doi.org/10.62951/ijls.v2i2.399
Available online at: https://international.appihi.or.id/index.php/IJLS

Criminal Liability for Extremist Crimes Through Electronic Means in Modern Legislation : a Comparative Study

Haider Kazim Hattahut
Faculty of Nursing, Al-Qadisiyah University, Iraq

Abstract. *The aim of this comparative study is to identify the criminal responsibility for extremism through electronic means in modern legislation for which the researcher used the comparative analytical method. The research problem is centred on the statement of the objective provisions of criminal responsibility for the crime of extremism through electronic means in both Iraqi law and comparative laws. The study relied on a number of primary and secondary references both past and present to collect legal information. The study concluded a number of the most important results, namely that extremism using electronic means is the aggression emanating from pirates using electronic means with the aim of disrupting security and public order and extorting the authorities by seizing public and private funds and damaging property. Results also show that the competent court in considering the crime of extremism using electronic means is the State Security Court in Iraqi law, and we see the Iraqi legislator in the Iraqi Constitution of 2005 was unique in reducing the penalty until amnesty for those who provide information about cyber attacks. The study recommended that there should be a clear text for the crime to define the electronic means as per the Iraqi legislator, while the modern legislations came in conjunction and close to the Jordanian legislator, as well as the French law, the Algerian and Egyptian legislator. The study also recommends that the Iraqi legislator follow the example of the Jordanian legislator in issuing a special law for electronic crimes and contain the text of criminalising the crime of cyber extremism. The study also stresses the need for judges to have sufficient knowledge of electronic means and the Internet in order to consider cases in this regard by preparing courses for them and all those working in the field of combating cyber extremism crimes. This is particularly true since the threat is carried out through the Internet and electronic means.*

Keywords *Criminal Liability, Cyber Extremism, Electronic Extremism, Electronic Means.*

1. INTRODUCTION

Due to the great scientific development, especially in electronic communication, many people exploit electronic communication for many purposes. However, there are some individuals who practice the crimes of electronic extremism through electronic means or illegal work and thus begin to hit the interests. The penalty is the only form of criminal sanction as it has been for a long period of time. Rather, a second form has been added, which has gained great importance in the field of modern criminal studies and in the fight against crime. This form is represented by precautionary measures, as penal policy is not indispensable to utilising both punishment and precautionary measures as two forms of social reaction towards the offender, because each complements the other and each has its own field that the other cannot achieve (Bilal, 1995, p. 157). Therefore, the victim has become a commodity that is exploited by the processes of racism or extremism occurring through electronic means of various kinds. So, some cases pose a threat to the internal and external security of the state, and punishment must be imposed as one of the oldest, most widespread and applied forms of criminal sanction. However, as preventative strategies have come out as a priority that should be identified and dealt with, the contemporary perspective in the field of criminal studies on punishment has changed (Al-Zoubi, 2017, p 245).

Received: December 30, 2024; Revised: January 20, 2025; Accepted: February 10, 2025; Online Available: February 12, 2025;

The Jordanian legislator has criminalised acts of extremism and threats that occur through electronic means by the Communications Law No. 13 of 1995, and in the Jordanian Cybercrime Law of 2023, extremism and hate speech were criminalised, while the Iraqi legislator did not issue a cybercrime law and was limited to texts that include rules for criminalising the crime of extremism through electronic means in the Iraqi Penal Code No. 111 of 1969 according to Article 434 and which are adapted by the judge.

The Importance of the Research:

The importance of the research lies in the findings and recommendations of the study, which will be a starting point for new research in light of the lack of legal studies on this topic. Its importance also lies in its dealing with the crime of extremism by electronic means as it was one of the issues that occupied the penal jurisprudence in light of the swing of state practices on the development of a special law or penal texts. In view of the spread of the Internet and the consequent spread of crimes, the legislator had to intervene to contain them.

Research Problem

The main issues raised by the research topic can be listed as follows:

- Are the legal provisions contained in the Iraqi Penal Code No. 111 of 1969 sufficient to determine criminal liability for extremist crimes using electronic means?
- Is it possible to combat this type of new crime, which differs at the internal level in Iraq from the international level? At the internal level, the legislator still relies on general procedural rules for criminalisation. At the international level, some countries have developed laws to combat electronic crimes, including the crime of extremism, such as Jordan and Algeria.
- The research problem is centred on the lack of definition or clarification of electronic means for the Iraqi legislator and the failure to stipulate the substantive and procedural provisions of criminal liability for the crime of extremism using electronic means?

Objectives of the Study:

The study seeks to achieve the following objectives:

- Reaching persons or entities that use electronic means for the purpose of spreading the crime of extremism in all its forms.
- Determine the availability of criminal protection for the crime of extremism through electronic means.
- Is the Iraqi Penal Code No. 111 of 1969 sufficient or not to confront the crime of extremism through electronic means.

2. RESEARCH METHODOLOGY

We followed in this study the analytical and comparative method because of its suitability for the nature of the study. We collected information and laws, analysed them and assessed the opinions of legal scholars in order to weight the best and then indicate the results, and compare this all between the positive criminal jurisprudence, in order to indicate the crimes of electronic extremism and its risks and the availability of criminal liability.

The Structure of the Research

We opted to study the criminal liability for crimes of extremism through electronic means in the light of modern legislation. In the first section, we will address the concept of criminal liability and the crime of extremism through electronic means. In the second section, we will examine the elements of electronic crimes and extremism, as well as the position of criminal legislation on them. Our study concludes with a summary that includes a set of conclusions and proposals.

The First Chapter: The Concept of Criminal Liability and The Crime of Extremism Through Electronic Means

The sense and feeling of security and reassurance in life, money, and reputation is one of the most important basic things that modern societies seek to achieve. This can only come through the law that guarantees this. Acts of violent extremism that are active at the present time pose a serious threat to society. Their essence is the desire of the perpetrators of crimes to intimidate the safe community and threaten to spread false ideas and news. The purpose is to force public authorities, that is, governments, to take measures or decisions that are important to extremist organisations or persons. Thus, extremist crimes spread and this naturally leads to violent extremist activity (Korolev, 2022, p. 24).

In order to clarify the concept of criminal liability and the crime of extremism, we divide this research into two requirements. In the first, we will address the definition of criminal liability and its elements, while in the second, we will address the definition of the crime of cyber extremism and its seriousness, as follows.

First Requirement: Definition and Elements of Criminal Liability

The research on criminal liability is related to a number of important issues, starting with its definition and elements. So, we will discuss it in two sections. The first section deals with the definition of criminal liability and the second section outlines its elements and as follows:

The First Section: Defining Criminal Liability

Neither the Iraqi nor the Jordanian legislature has addressed the definition of criminal liability, but it can be defined jurisprudentially as follows: It is the responsibility of a person to bear the consequences of his or her actions: A person bears the consequences of the prohibited acts that he or she chooses to commit and is aware of their meanings and consequences (Al-Haidari, 2010, p. 57).

It is worth noting that criminal liability differs significantly from moral liability. Criminal liability can only be realised if the offence was committed against a rule of law. If the offence was committed against a moral rule only, without touching any legal rule, the liability here is considered a moral liability. Its penalty is limited to disapproval and disapproval. Criminal responsibility is one of the aspects of legal responsibility. Except with regard to the definition of criminal responsibility, and with reference to the writings and writings of legal jurisprudence in this regard, we found that criminal responsibility has been defined by the jurisprudence in more than one definition. The most important of these definitions are: It is the qualification of the individual to bear the consequences of his or her action. Some of them defined it as: "(Al-Saeed, 2002, p. 127) it is permissible and thus the legislator in the case of criminalising an act the purpose of which is to protect social interests and noble goals. (Abdul Rahman, 1995, p. 109), and these provisions include criminalisation. They are not absolute, but have restrictions that limit their scope. This is represented by the transformation of criminal acts in the legally considered interests into legally permissible acts (Najm, 2000, p. 130). Based on the above, it can be said that responsibility in criminal law is the set of conditions that arise from the crime. A personal blame is directed against the perpetrator of the crime. These conditions are those by which the act appears legally as a rejected expression of the personality of the perpetrator. Responsibility in this sense constitutes an element of the crime. Responsibility in its simplest sense means (bearing the consequence or responsibility). It denotes the obligation of a person to bear the consequences of his or her act that violates a rule or a penal provision (Al-Haidari, 2010, p. 61).

Section 2: Elements of Criminal Liability

Modern criminal legislation has established certain characteristics of criminal liability and considered them as elements that cannot be fulfilled without their availability, the most important elements of which are: The material element and the psychological element.

Firstly: The material element

This element expresses the causal relationship between the perpetrator's act and the criminal result, and this requires us to explain the meaning of the act and the result and then the causal relationship between them.

1) It is the apparent face of the offence, and is considered an assault that affects the interest protected by the law.

The content of the act is determined by (positive behaviour and negative behaviour), and the positive behaviour may be a single temporal act. This includes shooting bullets in murder, or it may consist of more than one act, such as beating the victim and stealing his or her money, and in this case the responsibility of the perpetrator is determined according to whether the acts are related to the unity of purpose and constitute a single criminal behaviour or not (Surour, 1996, p. 411).

2) Criminal Consequence: This refers to the effect that results from the criminal behaviour embodied in the aggression that affects the interest, right or right that the legislator has determined the duty to protect criminally, and it should be noted that the criminal or harmful result as an element of the material element of the crime is not always required to be achieved to say that there is a crime. It should be noted that the criminal or harmful result as an element of the material element of the crime is not always required to be achieved to say that there is a crime and then punish it, as it is sufficient to achieve and punish it once the criminal agreement occurs, even if the crime that was agreed to commit does not actually occur (Al-Mandlawi, 2017, p. 53).

3) Causal relationship: The criminal behaviour and the criminal result are not sufficient for the existence of the material element of the crime, but the criminal result must be the result of this criminal behaviour, i.e. there must be a causal relationship represented in the link that connects the offender's behaviour and the criminal result so that it proves that the criminal behaviour that led to the occurrence of the result. Based on the above, the causal relationship can be defined as the link between the cause and the effect, and this assumes the occurrence of the act and the result together, so if the act occurs and no material result is achieved, there is no causal relationship (Al-Barzat, 2023, p. 45).

Secondly: The psychological element

This element relates to the mind of the perpetrator of wrongful acts. It is basically a psychological force that can create and control. This force is (will). There is no will for those who have no choice. The psychological element can be defined as a psychological relationship between the perpetrator and the criminal incident that was achieved in the real world. This relationship does not differ in its nature according to the different crimes. Its nature is the same

whether the moral element is represented in the form of intentionality or error. In light of this, it can be said that the psychological element is the direction of the offender's will to achieve the incident that created the crime (Al-Haidari, 2010, p. 78).

Second Requirement: Definition and Severity of the Crime of Extremism

In order to identify the definition of the crime of extremism and its seriousness, it is necessary to address this requirement in two consecutive sections, the first of which we devote to the statement of the meaning of the crime of extremism while the second concerns the statement of the extent of the seriousness of the crime.

The First Section: Definition of The Crime of Cyber Extremism

Firstly, extremism in language: Lack of consistency in the matter, departure from the middle, and departure from the familiar, from what the group is on (Al-Zubaidi, 1994, p. 24).

Etymological definition: According to the researcher's modest knowledge, the comparative penal legislations did not define the act of extremism. This was left to the jurists who defined this behaviour with many definitions that agree in their content that extremism is the adoption by the individual of a position characterised by rigidity. It is a departure from moderation. It is a distance from the familiar. It is exceeding the intellectual and behavioural standards and moral values defined by the legislator and accepted by society (Al-Ghamdi, 2022, p. 354).

Extremism under the influence of this fear may lead to the perpetrator answering what he or she wants. This occurs when extremism is accompanied by a request. Extremism may mean "frightening the victim, putting him or her in a state of terror, and disturbing him or her from a specific harm that is intended to be inflicted on him or her (Hanash, 2020, p. 20).

In this definition, extremism is associated with terrorism. We see that crimes by their nature exist with the existence of man. They develop with his or her development. Since man is always in constant development thanks to the information revolution and advanced technology, we find scientists and good people trying to benefit from it. On the other hand, we find that criminals also try to benefit from technical progress. Technology has become a free for all good and bad. Criminals are many and were able to acquire more experiences and skills in dealing with the Internet. They commit electronic crimes via satellite. Their crimes are no longer limited to the territory of one particular country. They exceed the state borders (Ataya, 2016, p. 360).

As for cybercrime according to the broad concept that accommodates a sufficient amount of criminal acts, it means (all forms of illegal behaviour committed using computers).

Another went to define it as (any criminal activity in which the computer system plays a role to complete it, provided that this role is of some importance) (Al-Baghdadi, 2018, p. 9).

The Second Section: The Severity of the Crime of Cyber Extremism

The convergence between radicalisation and violence leading to terrorism and cybercrime poses an enormous challenge. This is especially true with the use of electronic means. The United Nations has expressed in its plans to combat extremist terrorism through the growing concern over the use of the Internet and other information and communication technologies and electronic means by violent extremist groups and individuals. These individuals are terrorists. However, the relationship between terrorism and violent extremism remains complex. Cybercrime remains vague, especially in the dark corners of the Internet world (United Nations Organization, 2024).

Against this backdrop, the United States has created a programme to reduce the risk of radicalisation by creating a cyberattack database. This database uses manual extraction procedures to better understand how different ideological movements operate in online spaces. This database takes as its focus a kaleidescope of ideologies that range from right-wing extremism and jihadism to environmental extremism, left-wing adherents, and secular extremism. At least one of a set of attack methods must be used. These also range from data breaches and DDoS attacks to web defacement and defamation as well as some other attack methods. These methods include e.g. sending spam emails or hacking social media (Freilich et al., 2024).

The most dangerous type of radicalisation is violent extremism through electronic means. Terrorists use the Internet and electronic means to spread propaganda and encourage recruits to violent extremism. In this anthology, which includes various topics, a study was conducted in the United States of America on cyber jihad. The study examined how terrorists use the Internet as a means of spreading their ideas and message. The study mentioned how Anwar al-Awlaki, the leader of Al-Qaeda in the Arabian Peninsula (AQAP), used the Internet to spread his or her ideas and the message of AQAP. his or her aim was to spread values, expand the organisation, and spread beliefs. Al-Awlaki produced propaganda videos and a global e-magazine to recruit, influence, and train new members. As an online jihadist, al-Awlaki saved a fortune in printing costs. He or she worked to develop a virtual community of interest with a global reach (Aly et al., 2016, p. 103).

Based on the above, we call on the Iraqi legislator to enact the draft cybercrime law. This law should combat these crimes of all kinds, especially violent extremist crimes using electronic means. These crimes are considered one of the most dangerous types of crimes that

affect the internal and external security of the state. The law must keep pace with the development in the world.

The Second Chapter: The Elements of Cybercrime and The Position of Criminal Legislation

In order to clarify the elements of electronic crimes and the position of criminal legislation on them, we will divide this research into two requirements. In the first, we will address the elements of electronic crimes and in the second, we will address the position of the Iraqi legislator and modern criminal legislation on them as follows.

First Requirement

Elements of cybercrimes and the crime of extremism is one of its types.

Each crime has its own elements, that is, certain elements within the limits of the legislation for punishment. If one of them disappears, the crime does not exist. In the end these elements all derive from the general theory of criminalisation. It is the elements of the crime that define its scope and draw the boundary that separates it from other crimes. Electronic crimes have three elements. The first of which is the material element, which means the external manifestation of the perpetrator's activity, and the moral element. The second of which is the criminal intent, i.e. knowledge of the subject matter of the electronic crime and the will to commit the crime. The third is the legal element. So we will discuss this requirement in two sections. The first section deals with the material element, while the second section shows the moral element as follows:

The First Section: The Physical Element

The physical element of the offence, whether it is the act of stopping or disrupting the hypothesis processing system from performing its activity for which it was designed or the act of corrupting the activity or function of the automated processing of the outputs and images of this assault are as follows:

Firstly: The act of disruption (obstruction)

This behaviour assumes the presence of a positive act. It falls within the obstruction of the system without requiring a specific means of obstruction, as it may be done in a physical way using violence or without it on the computer or communication network by damaging or breaking it, smashing the disc, cutting communication networks, or preventing workers on the systems from accessing the place where the systems are located. The means of obstruction or disruption is moral if it occurs on the logical entities of the system and leads to the system slowing down in performing its function, either by manipulating the inputs or manipulating the programmes (Qara, 2006, p. 115), by following one of the following techniques:

- Introducing a virus programme.
- Introducing a virus programme.
- The use of logic bombs.
- Use of stop cards (stopping the execution of the programme).
- Filling the system with more outputs than it can handle.
- Making the system slowdown in performing its functions.

Secondly: Corruption (Defective):

Corruption refers to the act that makes the automated output processing system unable to function properly, by giving, for example, results other than those that are supposed to be obtained, and corruption in this sense is close to the defect that we saw in the unlawful in their aggravated form does not require them to be intentional, while In this crime, it is required that the corruption be intentional, and therefore, it is called the crime of intentional or causal assault on the automated output processing system. Therefore, corruption is not a result, but the content of the criminal behaviour in this crime (Hegazy, 2004, p. 42), as for the techniques of defects and corruption, they are multiple, including: -

The electronic bomb, through which a set of assumptions are introduced that multiply within the system and make it unusable.

The use of a virus the function of which is to make an imperceptible change in the programme or assumptions that make the output of the system other than the one that was supposed to be obtained.

The Second Section: Moral Element

Cybercrime is one of the intentional crimes that are based on the criminal cause with the elements of knowledge and will, where the offender ends up knowing an act of infringement on the scope of the protected right and that his or her will is directed to cause an act of corruption or disruption and disability and achieve its result. This is different from if the one who is legally authorised to deal with the system causes the result of corruption or disability as a mistake in dealing with the system, the responsibility is excluded from him or her and the criminal description is not investigated in his or her activity due to the absence of the criminal reason (Masoud, 2008, p. 97).

The moral element is represented in the intentional origins of the material of the crime. It is represented in control over it in its psychological face, i.e. the subconscious. A person cannot be held accountable for a crime unless a link is established between the material of the crime and its will. The crime of extremism using electronic means is one of the intentional crimes. These crimes require the availability of criminal intent in the case of other electronic

crimes. The criminal intent that is required in this crime is the special criminal intent. In this section, we will address the moral element in the electronic crime. This includes the crime of extremism using electronic means.

Firstly: Knowledge / The law assumes in the criminal intent in intentional crimes the knowledge of the perpetrator of the act constituting the crime. This assumption requires the availability of its elements. Therefore, the will and knowledge must be directed to the elements required for the crime as defined by the law. What the will is directed to must be surrounded by knowledge first. This necessitates that the knowledge applies to all the legal elements in the crime. The criminal's intention must be directed to the intent to commit the electronic crime (Taha, 2014, p. 289). The crime of extremism using electronic means is one of the intentional crimes.

In these crimes, the availability of criminal intent is required if the error is incompatible with the crime of extremism using electronic means. The criminal intent in the crime of violent extremism using electronic means requires that the perpetrator be aware of the electronic means.

He or she must be aware of the truth of the criminal incident. This awareness occurs while he or she is engaged in the activity of the crime of extremism using electronic means. his or her act is an aggression against the right protected by the law. In the crime of extremism using electronic means directed against persons, the perpetrator must inform himself that his or her actions would prejudice the right of the victim (Hanash, 2020, p. 79).

II: Will.

The essence of the will is choice and is represented in a psychological activity that embodies the ability of a person to direct himself to an act or refrain from an act, so the criminal intent in the crime of extremism in electronic means is available in the direction of the will of the perpetrator. As it is a psychological activity directed towards achieving a certain result, and it is a force used by humans to influence people, it is issued with awareness and awareness, so it assumes knowledge of the targeted purpose and the means used to achieve this goal (Al-Barzat, 2023, p. 51).

Article (3, 8, 10) of the Budapest Convention of 2001 (27), and what the French legislator stipulated in Article 323/3 of this law came what is known as penalties, as the material element of this crime became the behaviour in general in this crime is limited to one of these The physical element of the offence of intentional or causal assault on the output of e-commerce data processing systems, as the result of the occurrence of one of these acts is that it involves the manipulation of the assumptions contained in the information processing system

The criminal behaviour in this offence is to control the information that has been automatically processed and transformed into symbols and signals, i.e. outputs related to information, i.e. the offence falls on the assumptions, i.e. the information that has been processed The information that has not yet been processed, or has not entered the information processing system, as well as the information that has entered the system and has not started to be processed or has left the system, is outside the framework of the process (Masoud, 2008, p. 98).

The text protects the information processed within the system or those that are in the process of being processed, and the criminal act on these assumptions is the act of inserting, erasing and modifying the information installed in the system, which can be included in what is known as electronic hacking, and it is not required that the acts of insertion, erasure and modification occur directly, but may occur indirectly, such as by a third party or by remote control (Qara, 2006, p. 121). The physical element of this offence may be illustrated by showing the forms of criminal behaviour, such as insertion, erasure and modification.

Entry means any intrusion of a person who enters the system and is usually among those who have the right to enter with control over all parts of the system, contrary to the will of the owner of the system or those who have the right to control it, such as systems related to state security or systems related to private life that may not be accessed, or that the perpetrator has violated the entry restriction set or that the perpetrator has not paid a sum of money. The French legislator punished the mere act of access without specifying the means of access to the system, whether through a password, a special encryption program or the exploitation of an authorised person, and the mere act of accessing the information system commits the offence or does not achieve the benefit of access and criminalises each person for unlawful access from the program (Qahwaji, 1999, pp. 131-132). The aim is to criminalise the act of unlawful stay within the available automated data processing systems is to make the offender responsible for a deliberate crime because his or her will was directed to stay with sabotage or damage within the system knowing that his or her entry is unauthorised and the ruling applies to those who are allowed to enter As for the opinion of the jurisprudence, it indicated that the perpetrator, although his or her entry into the system was done by accident and he or she has no criminal cause, but despite knowing that this act is not allowed, he or she refuses to leave the system and refuses to leave it (Tammam, 2000, p. 299).

Where the act of staying inside the system takes the form of a continuous crime because, according to the above-mentioned view, the act of staying is one of the punishable forms of staying if the offender remains inside the system after the period specified for him or her to stay inside it or in the case of copying information displayed only for viewing or the

offender obtains a service without paying the prescribed fee for it, and this idea may also adjust the idea of unauthorised entry as "infiltration within the information system"(Hegazy, 2004, p. 32). It also includes what falls within the scope of information extremism, in which the attack does not occur by interfering with the normal functions of the computer or modifying the processing data, but rather by entering the information processing centre of the computer with an electronic device the function of which is to capture information or eavesdropping, for example.

Second Requirement: The Position of the Iraqi Legislator and Modern Criminal Legislation On Cybercrime.

The First Section: The Iraqi Legislator's Position On Cybercrime

Article (156) of the Iraqi Penal Code No. 111 of 1969 defines crimes that affect the security of the state. It defines the penalties that apply to the perpetrators of these crimes. It also defines exemptions, legal excuses and mitigating judicial circumstances.

It can be said that the electronic crime in the light of Iraqi legislation has two basic elements, the psychological element and the physical element. The crime is not a place, but a tangible physical place such as hacking, access and distortion of information and data. Here we can consider what is related to the issues, prosecution and pursuit of that individual or that hacker. This is defined as a person for committing the crime unless a link or relationship is established between the material of the crime and its will. If it is proven that the person did not want those materials did not want the acts and effects issued by him, the attribution of those materials to this person is prevented. It follows that both the material and moral elements are absent. The crime of violent extremism using electronic means is one of those crimes that require the existence of the criminal cause. The criminal cause that is required in this crime is the special criminal cause.

Article 33 of the Iraqi Penal Code stipulates that:

1 – Criminal intent is the direction of the perpetrator to cause the act constituting the offence with the aim of the result of the crime that occurred or any other criminal result or in conjunction with premeditation. The reason may be simple.

2- Premeditation is the effective or determined thinking based on it in causing the offence before working on execution. This is provided that it is a type far from what is known from instant anger or what is known from psychological agitation to a specific person or to achieve premeditation. This applies whether the perpetrator's intention of the offence is directed to the occurrence of a matter or is suspended.

Jurisprudence has defined the criminal cause as a complete and integrated science that specialises in studying the elements of crime and the will directed to the realisation or acceptance of these elements. It is also deduced from the previous definition that the moral element consists of two elements, namely knowledge and will (Al-Saeed, 2002, p. 272), as we explained earlier.

The Iraqi legislator also criminalises accessing a website or using a computer "with the intention of obtaining and controlling the concept of data or working to possess information that affects the national security or national economy of the country". These acts are subject to a maximum penalty of ten years imprisonment in addition to fines.

The draft Iraqi Cybercrime Law stipulates that "whoever uses an electronic network or a computer device and the like with the intention of attacking religious, family or social principles and values shall be punished with a term of imprisonment of not less than seven years and not more than ten years, and a fine of not less than 10 million Iraqi dinars (approximately $8,380) and not more than 10 million Iraqi dinars (approximately $8,380)."

The criminalisation of vague and imprecise acts, subject to wide interpretation by the judge (MENA Rights Center, 2020)), does not meet the criteria of legal clarity and predictability. This is clearly contrary to Article 38(1) of the Iraqi Constitution, which affirms that the state must guarantee "freedom of expression by all means".

We remain deeply concerned about these provisions, which give the authorities excessive discretionary power. These enable them to stifle the right to freedom of expression online. Article 19(3) of the International Covenant on Civil and Political Rights states that no restriction on freedom of expression shall be permitted. These are necessary to protect "the rights or reputations of others" or "the security of the State, public order, public health or morals", which is not the case in the articles mentioned above. In fact, only individuals who criticise the government can face prosecution under these provisions. In this regard, we refer to the Human Rights Committee's General Comment No. 34, which states: "A rule must be formulated, which is regarded as a 'law'.

Section Two: The Position of Modern Criminal Legislation On Cybercrime

According to Article 13 of the 2001 Budapest Convention on Combating Cybercrime, in order to be effective, the prescribed penalties must be deterrent and include penalties of deprivation of liberty. These are original and supplementary penalties, applicable to the natural person. Article 12 includes the principle of accountability of the person concerned.

As for the French legislator, its experience in the penal policy against cybercrime or electronic crime appeared since the seventies. The most important of these attempts was in

1975, the so-called Deputy's Project on the Law of Information Fraud (Boure, 2003, January 23).

After a year and a half of discussions, the project was approved after amendments in the French Penal Code. This is related to felonies and misdemeanours, and included articles 462/2 to 462/9, based on the content of the articles, especially in the system of automated processing of outputs. It is considered an aggravating circumstance in the case of erasing or modifying the assumptions in it or the methods of processing or transferring it. These texts punish every act of obstruction or corruption intentionally and without regard for the rights of others. They punish the offences of forgery and the use of a forged document, as well as the offences of attempt and criminal agreement.

As for the amendment contained in the 1994 law, it amended the text of Article 441/1. Under this amendment, the offence of forgery of machine-processed documents only was changed to the offence of forgery and use of electronic documents. This was independent of providing for offences against the automated output processing system (Hegazy, 2004, p. 20). First: Cybercrime in French legislation.

Many countries have been keen in their legal legislation, and since 1994 until 1996, the law was officially introduced to curb the perpetrators of cybercrime. Article 2-232 of the French law stipulates, while Article 2-223 of the French Penal Code stipulates. 323 of the Penal Code stipulates that "Whoever obstructs or disrupts the operation of a programmed information system shall be punished." The third paragraph of the same article stipulates that "Whoever surreptitiously provides information to a system to arrange and retrieve information, or cancels or modifies information in it in an unauthorised manner in order to gain."

The French legislator, prior to issuing the new Penal Code, had amended the text of Article 462/4 of the 1977 Penal Code to criminalise the erasure and modification of automatically processed information or interference with its processing methods. This was punishable by a term of imprisonment ranging from three months to three years or a fine. It also criminalises the deliberate disruption or corruption of the operation of an automated data processing system. This is punishable by the same penalties referred to in Article 462/3.

France passed a bill after the murder of history teacher (Samuel Paty) in the Parisian suburb of Conflans Saint Honorine. The French authorities began to pay close attention to combating the crime of violent extremism through electronic means, especially social networks. The French parliament approved it in May 2020, a bill that requires social media platforms and search engines to remove content that incites violent extremism and hate speech within 24 hours of its publication. Violators are subject to penalties and fines of up to 1.25

million euros. The bill also places restrictions on websites and search engines and obliges them to cooperate effectively with justice, under the supervision of the French High Council for Audiovisual Media (Nazif, 2020, November 26).

Secondly: Egyptian legislation and its position on cybercrime.

Given that the Egyptian legislation that criminalises computer-related criminal activities is limited to those related to civil status and electronic signature, we refer to the traditional texts. Article 361 of the Egyptian Penal Code stipulates that "whoever deliberately destroys or damages fixed or movable property that is not his or her property and does not own it, or makes it unfit for use or disrupts it in any way (Taha, 2016, p. 47).

Violent extremism leading to terrorism at the present time is one of the most dangerous things facing countries and individuals alike. It has become the concern that frightens the international community through extremist and terrorist attacks, the activities of which operate via the Internet. Terrorist risks have increased over time with the speed of technological developments, which led to risks to countries, organizations and individuals. Hardly a day passes without hearing about a terrorist operation taking place here and there.

Although the phenomenon of international terrorism is not modern in linguistic and legal terminology and the natural and industrial barriers erected by States in order to protect their internal security and safety and thus protect international peace and security. The emergence of the Internet has helped in committing crimes of electronic terrorism on a large scale through hacking, fake accounts, espionage, publishing through fake webpages and websites. This includes hacking the accounts of security and military officials and the accounts of other security and sovereign ministries.

Extremist groups destructive operations on countries and individuals. Therefore, pirates and criminals are the first and last reason for spreading risks and breaking into public and private sites, chambers of commerce, important chambers, security and economic information and other sensitive places.

Accordingly, there should be a major role from everyone, both the government and private sectors, so that everyone reaches safety away from the policy of intimidation, threats, and revealing shortcomings and mistakes as the goal of pirates is clear. The law came clear by enacting direct penalties. Therefore, it should be necessary to make inroads into breaking the obstacles facing the investigation and investigation authorities in proving cybercrimes. This is especially true of those related to the privacy of electronic evidence and the privacy of the investigation, represented in the non-appearance of electronic evidence and the ease of erasing or destroying it, and the difficulty of investigating it.

In uncovering the mystery of crime and reaching it, as well as the weakness of international cooperation in combating and pursuing pirates and those who strike the interests of individuals in all the world, as they are invisible, manifold and transnational and require the use of special investigation methods. The Egyptian legislator has addressed the crime of extremism by electronic means by issuing the Egyptian Anti-Cybercrime Law No. 175 of 2018.

FINAL REMARKS

We can conclude that crime is the presumption of development and what is known as the technological shift. It is self-evident that the legislator's responsibilities are growing, which must address the fight against it and ensure the rights of individuals and maintain them. This is only possible by developing its competencies and improving its performance. We see that the legislative system must be affected by modernization. Otherwise its adherence to traditional rules will not be of any benefit to hope. As it is in its current state I am unable to apply its texts to crimes of this nature and privacy. The call exists and it is desirable to respond to it immediately. The update includes rules of the same nature as electronic crimes and the same privacy of its criminal, where the criminal does not leave a trace. The evidence of the crime is hidden or not of a material nature. The necessity exists to take into account the continuous development that occurs in the technology of digital transactions and the adequacy of the texts regulating them and gaining more flexibility to accommodate their continuous movement.

Accordingly, in light of the great scientific revolution that has taken place, it has contributed to this revolution on the establishment of very large interests. This established the rules of the game again. Therefore, we should, as the researcher sees it, expand our thinking abilities, as long as the crime.

3. CONCLUSIONS

Terrorism using electronic means constitutes an act of aggression, intimidation, or physical and moral threats carried out by cybercriminals with the aim of disturbing security and public order, blackmailing authorities, seizing public and private funds, and damaging property. The competent court for adjudicating such crimes in Iraq is the State Security Court, and the prosecution of these offenses falls under the jurisdiction of the Prosecutor of the State Security Court. The crime requires both a special and a general criminal motive, yet the Iraqi Anti-Terrorism Law does not explicitly define or specify electronic means within its provisions. Upon reviewing the special procedural provisions of the Iraqi Anti-Terrorism Law, it is evident that the legislation on combating terrorism generally includes procedural rules to regulate the powers of seizure, investigation, and prosecution. However, the initiation of the

crime of terrorism using electronic means is not explicitly addressed in the existing legal framework.

The penalty for electronic terrorism is stipulated in the Penal Code, including imprisonment and fines, as outlined in Article 394 bis of the Penal Code, which was amended by Law No. 5/4 of 11/2004. Notably, the penal legislator refrained from providing a general definition of the crime, following the approach of various criminal legislations, including that of Algeria, which lacks a comprehensive definition of criminal offenses, instead relying on specific legal provisions defining each crime individually. In Algeria, the Penal Code includes provisions addressing internet crimes, particularly financial offenses such as theft, fraud, and breach of trust, as well as crimes affecting the public interest, such as forgery. However, it exhibits shortcomings in addressing numerous other electronic crimes that pose risks to individual privacy and societal security. Furthermore, many legal texts have been amended to criminalize cyber offenses, yet they remain focused solely on computer-related crimes, failing to encompass the broader and more comprehensive concept of electronic means.

4. RECOMMENDATIONS

1. It is recommended that the Iraqi legislator explicitly define the crime of extremism and provide a clear legal definition of electronic means to ensure comprehensive legal coverage.
2. The Iraqi legislator should enact procedural rules governing the prosecution and investigation of extremism-related crimes, ensuring due process and legal clarity.
3. Contemporary legislative approaches, such as those adopted by the Jordanian, French, and Algerian legal systems, demonstrate an integrated and coherent approach to addressing cyber-related extremism. It is advisable for Iraq to adopt similar legal provisions to ensure consistency with international best practices.
4. The Iraqi legislator is urged to develop and implement a specialized law addressing cybercrime, including extremism perpetrated through electronic means. The law should draw upon the legislative models established in Jordan, Egypt, and France to effectively combat cyber threats.
5. In line with best practices, it is recommended that Jordanian, Egyptian, and French legislators consider adopting provisions similar to those in Iraqi law that exempt individuals from punishment if they report a cybercrime before its discovery and assist law enforcement in identifying and apprehending perpetrators. This measure would enhance preventive efforts against cyber offenses.

6. Legal frameworks should emphasize the principle of mitigating legal excuses for individuals who take proactive measures to prevent criminal acts before their commission. This could serve as a deterrent to potential offenders.
7. It is essential to broaden the definition of electronic means to include social media platforms, online communication tools, chat applications, and digital service platforms. This would ensure that legal provisions are not restricted solely to computer-based offenses but encompass a wide range of electronic interactions used in extremism-related activities.

REFERENCES

Abdul Rahman, S. N. (1995). *Lectures on general coercive penal law* (1st ed.). Dar Al-Fikr.

Al-Baghdadi, A. B. (2018). *Means of investigating cybercrimes* [Master's thesis, An-Najah National University].

Al-Barzat, M. O. (2023). *The governing provisions of election crimes in light of Jordanian and Algerian legislation.* Dar Al-Khaleej.

Al-Ghamdi, A. A. M. (2022). Contemporary religious extremism: Its definition, causes, manifestations, and treatment methods. *Journal of the College of Islamic Studies, 39*(1), 352.

Al-Haidari, J. I. (2010). *Provisions of criminal responsibility* (1st ed.). Al-Sanhuri Library.

Al-Mandlawi, M. M. (2017). *Crimes of kidnapping women and their impact on society.* Dar Al-Marefa.

Al-Saeed, K. K. (2002). *Explanation of general provisions in penal law: A comparative study* (1st ed.). Al-Dar Al-Alamiyya and Dar Al-Thaqafa.

Aly, A., MacDonald, S., Jarvis, L., & Chen, T. (2016). Violent extremism online: New perspectives on terrorism and the Internet. *Journal of Strategic Security, 10*(3).

Al-Zoubi, J. (2017). *Information technology crimes: A comparative study* (3rd ed.). Dar Al-Thaqafa.

Al-Zubaidi, M. M. (1994). *Taj al-Arus min Jawahir al-Qamus* (1st ed.). Dar Al-Fikr.

Ataya, I. R. (2016). Cybercrime and the means of confronting it in Islamic law and international systems. *Journal of Tanta University College of Sharia and Law, 33*, 360.

Bilal, A. (1995). *The general theory of criminal sanction.* Dar Al-Nahda Al-Arabiya.

Boure, P. (2003, January 23). Internet et la lutte contre la cybercriminalité [Internet and the fight against cybercrime]. *Gazette du Palais*, *23*(23), 19.

Council of Europe. (2001). *Convention on Cybercrime.* Retrieved from https://rm.coe.int/budapest-convention-in-arabic/1680739173

Freilich, J. D., Chermak, S. M., & Frank, R. (2024). *Data collection in online terrorism and extremism research: Strengths, limitations, and future directions.* Retrieved from https://www.tandfonline.com/doi/full/10.1080/1057610X.2024.2361957

Hanash, S. M. (2020). *Criminal responsibility for threat via electronic means: A comparative study* [Master's thesis, Middle East University].

Hegazy, A. B. (2004). *E-commerce and its legal protection* (Vol. 2). Dar Al-Fikr Al-Jamei.

Korolev, Y. A. (2022). *Differentiation of criminal liability for crimes of an extremist nature* [Abstract of PhD dissertation, Ural State Law University named after V.F. Yakovlev].

Masoud, K. (2008). *Criminal protection of computer software* [Master's thesis, University of Tlemcen].

MENA Rights Center. (2020). *The new Iraqi draft law on combating cybercrime still contains problematic provisions restricting fundamental freedoms.* Retrieved from https://menarights.org/ar/articles/la-yzal-mshrw-alqanwn-alraqy-aljdyd-lmkafht-aljraym

Najm, M. S. (2000). *Penal code: The general theory of crime* (1st ed., 4th issue). Maktabat Dar Al-Thaqafa.

Nazif, A. (2020, November 26). France combats electronic extremism with counter-public discourse. *Sky News Arabia.* Retrieved from https://www.skynewsarabia.com/world/139553

Qahwaji, A. A. Q. (1999). *Criminal protection of computer programs.* Al-Maktaba Al-Qanuniyya.

Qara, A. (2006). *Electronic criminal protection in Algerian legislation.* Dar Houma.

Surour, A. F. (1996). *The mediator in penal law: General part* (Vol. 1). Dar Al-Nahda Al-Arabiya.

Taha, M. A. (2014). *The jurisprudential and judicial encyclopedia: Explanation of the general part of the penal code* (Vol. 2). Dar Al-Kutub Al-Qanuniyya and Dar Shatat.

Taha, M. A. (2016). *Legislative confrontation of computer and internet crimes.* Dar Al-Fikr and Al-Qanun.

Tammam, A. H. T. (2000). *Crimes arising from the use of computers: A comparative study* [Doctoral dissertation, Tanta University].

United Nations Organization. (2024). *Under the surface: The use of the dark web and cybercrime as a service by terrorists and violent extremists.* Retrieved December 29, 2024, from https://unicri.it/Pubblications/Terrorist_and_Violent_Extremist_Use_of_the_Dark_Web_and_Cybercrime-as-a-Service