أنواع الجرائم الإرهابية في الفضاء الافتراضي وتطور التشريعات لمكافحتها في القوانين العراقية والإيرانية

ابوالفتح خالقی
البروفسور فی القانون الجنائی و علم الاجرام
كلية القانون، جامعة قم، قم، ايران
ab-khaleghi@qom.ac.ir

حيدر احمد خضير
الطالب بمرحلة الدكتوراة فی القانون الجنائی و علم الاجرام كلية القانون، جامعة قم، قم، ايران
ab-khaleghi@qom.ac.ir

الكلمات المفتاحية: الجرائم الإرهابية، الفضاء الافتراضي، التشريعات العراقية، التشريعات الإيرانية، الإرهاب الرقمي.

كيفية اقتباس البحث
خالقی، ابوالفتح ، حيدر احمد خضير، أنواع الجرائم الإرهابية في الفضاء الافتراضي وتطور التشريعات لمكافحتها في القوانين العراقية والإيرانية،مجلة مركز بابل للدراسات الانسانية، نيسان٢٠٢٦، المجلد:١٦ ،العدد:٤ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Types of terrorist crimes in cyberspace and the development of legislation to combat them in Iraqi and Iranian laws

Professor of Criminal Law and Criminology, Abolfath Khaleghi
Faculty of Law, Qom University, Qom, Iran

Ph.D. Student in Criminal Law and Criminology, Haider Ahmed Khudair
Faculty of Law, Qom University, Qom, Iran

Keywords : Terrorist crimes, cyberspace, Iraqi legislation, Iranian legislation, digital terrorism, counterterrorism.

How To Cite This Article
Khaleghi, Abolfath , Haider Ahmed Khudair , Types of terrorist crimes in cyberspace and the development of legislation to combat them in Iraqi and Iranian laws,Journal Of Babylon Center For Humanities Studies, April 2026,Volume:16,Issue 4.

Abstract:

Terrorist crimes in cyberspace are among the most prominent challenges facing countries in the digital age, as the internet has become a fertile environment for the spread of extremist ideology and terrorist organizations. This research aims to study the types of terrorist crimes in cyberspace, focusing on the development of legislation related to combating them in both Iraq and Iran. The research presents the most important laws and measures taken by both countries to combat these cybercrimes, which include incitement to violence, recruitment of fighters, and the dissemination of misinformation. The study also highlights the results of these legislations and discusses the challenges that remain in the field of combating digital terrorism. In conclusion, it is proposed to enhance international cooperation, develop cybersecurity

legislation, and improve community awareness to combat this phenomenon.

المستخلص:

تعتبر الجرائم الإرهابية في الفضاء الافتراضي من أبرز التحديات التي تواجه الدول في العصر الرقمي، حيث أصبحت الإنترنت بيئة خصبة لانتشار الفكر المتطرف والتنظيمات الإرهابية. يهدف هذا البحث إلى دراسة أنواع الجرائم الإرهابية في الفضاء الافتراضي، مع التركيز على تطور التشريعات المتعلقة بمكافحتها في كل من العراق وإيران. تُعرض في البحث أهم القوانين والإجراءات التي اتخذها كلا البلدين للتصدي لهذه الجرائم الإلكترونية التي تشمل التحريض على العنف، تجنيد المقاتلين، ونشر المعلومات المضللة. كما تبرز الدراسة نتائج هذه التشريعات، وتناقش التحديات التي لا تزال قائمة في مجال مكافحة الإرهاب الرقمي. في الختام، يُقترح تعزيز التعاون الدولي، تطوير التشريعات المتعلقة بالأمن السيبراني، وتحسين الوعي المجتمعي لمكافحة هذه الظاهرة.

المقدمة:

في ظل التطور التكنولوجي المتسارع في العقدين الأخيرين، أصبح الفضاء الافتراضي يشكل جزءًا أساسيًا من الحياة اليومية على مستوى الأفراد والمجتمعات والدول. إذ أتاح هذا الفضاء، الذي يتسم بالاتصال المفتوح والمتبادل بين مستخدميه، العديد من الفرص للأفراد والكيانات لتنفيذ أهدافهم، سواء كانت إيجابية أو سلبية. وعلى الرغم من أن الإنترنت أتاح وسيلة قوية للتواصل والتعليم والعمل، إلا أنه في الوقت ذاته أفرز تهديدات جديدة تتعلق بالأمن والسلامة العامة. من أبرز هذه التهديدات هي الجرائم الإرهابية التي تجد في الفضاء الافتراضي بيئة خصبة للانتشار، حيث تمثل وسيلة للجماعات الإرهابية لنشر أفكارها المتطرفة، تجنيد أفراد جدد، والتخطيط لعمليات هجومية تؤثر على الأمن والاستقرار الوطني والدولي.

تعد الجرائم الإرهابية في الفضاء الافتراضي من أخطر أنواع الجرائم التي ظهرت في العصر الرقمي. وهي تشمل مجموعة واسعة من الأنشطة، مثل التحريض على العنف، نشر المحتوى المتطرف، تنفيذ الهجمات الإلكترونية، واستخدام الشبكات الاجتماعية للاتصال والتنسيق بين الأفراد والجماعات. وبالإضافة إلى ذلك، يستخدم الإرهابيون الإنترنت لنشر الدعاية والترويج لأيديولوجياتهم المتطرفة التي تستهدف تهديد الأنظمة السياسية والاجتماعية في الدول المختلفة. في هذا السياق، جاءت الحاجة إلى استجابة قانونية فعالة لمكافحة هذه الجرائم. في الدول العربية، بما في ذلك العراق وإيران، يتم مواجهة تحديات كبيرة في التصدي لهذه الظاهرة التي لا تقتصر آثارها على مستوى الحدود الوطنية، بل تتعداها إلى التهديد للأمن الإقليمي والدولي.

ولكون العراق وإيران دولتين تشهدان تهديدات أمنية متنوعة، فإنهما يواجهان ضغوطًا إضافية في التصدي للأنشطة الإرهابية عبر الإنترنت. لهذا السبب، ظهرت ضرورة تطوير تشريعات قانونية تواكب التطور السريع في عالم الإنترنت، وتوازي تهديدات الفضاء الافتراضي.

وعلى الرغم من أن كلا من العراق وإيران قد بدأت في اتخاذ بعض الخطوات القانونية لمكافحة الإرهاب الرقمي، إلا أن هذه التشريعات غالبًا ما تتسم بالتحديات التي تتراوح بين الثغرات القانونية، والضعف في التنفيذ، وكذلك الفجوة في التعاون الدولي. ورغم أن قوانين مكافحة الإرهاب الرقمية قد تم تطويرها بشكل مستمر، لا تزال هناك ثغرات كبيرة تتطلب معالجة من خلال تحديث مستمر للتشريعات، وتطوير آليات أفضل لرصد الجرائم الإرهابية الإلكترونية ومعاقبة مرتكبيها.

إن البحث في تطور التشريعات القانونية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في العراق وإيران يكتسب أهمية كبيرة. من خلال هذا البحث، نسعى إلى استعراض الجهود القانونية الحالية، وتقديم تحليل نقدي للتحديات التي تواجه كلا البلدين في مكافحة الإرهاب الرقمي. كما يهدف البحث إلى تقديم مقترحات لتحسين فعالية التشريعات والسياسات المتعلقة بالأمن السيبراني، بهدف تعزيز الأمن الرقمي وتحقيق استقرار أكبر في الفضاء الافتراضي. في هذا الإطار، يتطلب التصدي لهذه الجرائم فهماً عميقًا للتحديات القانونية والتقنية في كل من العراق وإيران، فضلاً عن التعاون المشترك مع الدول الأخرى في هذا المجال.

أهمية البحث:

تنبع أهمية هذا البحث من الحاجة الماسة لفهم تطور الجرائم الإرهابية في الفضاء الافتراضي وكيفية تطور التشريعات في كل من العراق وإيران لمكافحتها. في ظل تزايد استخدام الإنترنت من قبل الجماعات الإرهابية، يعد هذا البحث ذا أهمية كبيرة في تسليط الضوء على القوانين الحالية، وتقييم فعاليتها في مواجهة هذه الجرائم الرقمية. كما أن البحث يهدف إلى تقديم مقترحات لتطوير التشريعات والأدوات القانونية والتقنية، وذلك من خلال تسليط الضوء على التحديات التي تواجهها الدول في التعامل مع هذه الجرائم. ويكتسب البحث أهمية خاصة في تقديم رؤية شاملة للظاهرة من خلال دراسات مقارنة بين العراق وإيران، والتي قد تكون مرجعية لدول أخرى.

مشكلة البحث

تتمثل مشكلة البحث في تصاعد استخدام الفضاء الافتراضي كبيئة خصبة لارتكاب الجرائم الإرهابية، سواء من خلال التجنيد الإلكتروني، أو نشر الفكر المتطرف، أو التخطيط والتنسيق للعمليات الإرهابية، أو تمويلها عبر الوسائل الرقمية. وفي المقابل، يثار التساؤل حول مدى كفاية

وفعالية التشريعات الوطنية، وبخاصة في كل من العراق وإيران، في مواكبة هذا التطور التقني المتسارع.

وعليه، تتمحور المشكلة حول:

مدى قدرة التشريعات العراقية والإيرانية على مواجهة الجرائم الإرهابية في الفضاء الافتراضي، ومدى مواكبتها للتطورات التقنية وأساليب الجماعات الإرهابية الحديثة.

أسباب اختيار البحث

يمكن تبرير اختيار هذا الموضوع من خلال عدة اعتبارات:

١. **التطور التكنولوجي:** الاستخدام المتنامي للإنترنت ووسائل التواصل الاجتماعي من قبل الجماعات الإرهابية .

٢. **الحاجة التشريعية:** ضرورة تقييم كفاءة القوانين الحالية في العراق وإيران ومدى ملاءمتها للتحديات الحديثة .

٣. **الطابع المقارن:** المقارنة بين نظامين قانونيين مختلفين تثري البحث وتكشف عن نقاط القوة والضعف .

فرضيات البحث

يمكن صياغة الفرضيات على النحو التالي:

١. **الفرضية الأولى:** التشريعات العراقية والإيرانية لا تزال تعاني من قصور نسبي في مواكبة الجرائم الإرهابية في الفضاء الافتراضي .

٢. **الفرضية الثانية:** هناك تفاوت في مستوى التنظيم القانوني بين العراق وإيران في مجال مكافحة الإرهاب الإلكتروني .

٣. **الفرضية الثالثة:** التطور السريع في وسائل التكنولوجيا يفوق سرعة تطور التشريعات القانونية.

٤. **الفرضية الرابعة:** اعتماد آليات قانونية حديثة (مثل التعاون الدولي والتشريعات السيبرانية المتخصصة) يسهم في الحد من هذه الجرائم .

منهجية البحث:

تعتمد هذه الدراسة على منهجية علمية متعددة تجمع بين المنهج الوصفي والتحليلي والمقارن، إذ يتم أولاً وصف طبيعة الجرائم الإرهابية المرتكبة في الفضاء الافتراضي وأساليبها الحديثة. كما يُعتمد المنهج التحليلي لدراسة النصوص القانونية المنظمة لمكافحة الإرهاب الإلكتروني في كل من العراق وإيران، وبيان مدى كفايتها. إضافة إلى ذلك، يُستخدم المنهج المقارن لإبراز أوجه التشابه والاختلاف بين التشريعين محل الدراسة. ويستند البحث كذلك إلى المنهج الاستقرائي من

خلال تتبع التطبيقات القانونية والآراء الفقهية ذات الصلة. وتهدف هذه المناهج مجتمعة إلى الوصول إلى نتائج دقيقة وتقديم توصيات تسهم في تطوير الإطار التشريعي لمواجهة هذه الجرائم.

هيكلية البحث:

تم تقسيم البحث إلى مبحثين، تناولنا في المبحث الأول مفهوم الجرائم الإرهابية في الفضاء الافتراضي وأنواعها، والذي قسمناه إلى مطلبين، جاء المطلب الأول بعنوان ماهية الجرائم الإرهابية في الفضاء الافتراضي، بينما جاء المطلب الثاني بعنوان أنواع الجرائم الإرهابية في الفضاء الافتراضي. أما المبحث الثاني فقد تناول التطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانونين العراقي والإيراني، والذي قُسِّم بدوره إلى مطلبين، جاء المطلب الأول بعنوان التطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون العراقي، في حين جاء المطلب الثاني بعنوان التطور القانوني لمكافحة الجرائم الإرهابية في إيران.

المبحث الأول

مفهوم الجرائم الإرهابية في الفضاء الافتراضي وانواعها

تعددت صور الجرائم الإرهابية في الفضاء الافتراضي مع تطور وسائل التكنولوجيا الرقمية وانتشار استخدام الإنترنت وشبكات التواصل الاجتماعي، حتى أصبحت هذه الفضاءات الافتراضية بيئة خصبة لنشاط التنظيمات الإرهابية وترويج أفكارها، والتخطيط لهجماتها، والتجنيد والتمويل والتواصل السري بعيدًا عن الرقابة المباشرة. فقد ساهم الطابع اللامركزي والمفتوح للفضاء الرقمي في تمكين الفاعلين الإرهابيين من تجاوز حدود الدول، واستهداف أمنها ومؤسساتها دون الحاجة إلى الحضور المادي أو استخدام الوسائل التقليدية. وهذا ما جعل من الفضاء الافتراضي ساحة موازية وخطيرة للجريمة الإرهابية.

إن طبيعة هذه الجرائم تأخذ أشكالًا متعددة ومعقدة يصعب أحيانًا تصنيفها ضمن القوالب التقليدية للجريمة، فهي تجمع بين الجرائم في الفضاء الافتراضي من حيث الوسيلة، والجرائم الإرهابية من حيث الغاية والنتيجة. فقد تتجلى هذه الجرائم في اختراق المواقع الحكومية الحساسة أو شبكات البنى التحتية، أو التحريض على العنف، أو نشر المحتوى المتطرف، أو تجنيد الأفراد عبر الإنترنت، أو جمع التبرعات وتمويل الأنشطة الإرهابية بوسائل رقمية يصعب تتبعها.

ولأن هذه الأفعال تمثل تهديدًا حقيقيًا للأمن القومي والسيادة الرقمية للدول، فقد بات من الضروري الوقوف على أنواع هذه الجرائم بشكل منهجي، للكشف عن خصائصها القانونية،

وتمييزها عن غيرها من الجرائم الإلكترونية، وتحديد أركانها وآثارها، وهو ما يساعد في بلورة سياسة جنائية فعالة لمواجهتها. إن تسليط الضوء على أنواع الجرائم الإرهابية في الفضاء الافتراضي يمثل مدخلاً أساسياً لفهم طبيعتها المركبة، ويؤسس لفهم أعمق للإطار القانوني الذي تتعامل به الدول مع هذه الظاهرة المتصاعدة.

المطلب الأول: ماهية الجرائم الإرهابية في الفضاء الافتراضي

تشكل الجرائم الإرهابية عبر الفضاء الافتراضي الخاصة بالمعلومات نمطًا جديدًا من الأنشطة الإجرامية التي تستهدف جوهر المنظومة المعلوماتية للدول والمؤسسات، من خلال التلاعب بالبيانات أو تعطيلها أو الاستيلاء عليها لأغراض إرهابية. ففي ظل الاعتماد المتزايد على المعلومات الرقمية في إدارة المرافق الحيوية، باتت هذه المعلومات تمثل هدفًا رئيسيًا للجماعات الإرهابية التي تسعى إلى زعزعة الأمن والاستقرار عبر الوسائل غير التقليدية. وتتمثل خطورة هذا النوع من الجرائم في أنه لا يستهدف فقط البنية التقنية، بل يهدد أيضًا سلامة القرارات السيادية والأنظمة الأمنية والاقتصادية، الأمر الذي يجعل من هذه الجرائم صورة متقدمة للإرهاب الرقمي تتطلب تنظيمًا قانونيًا دقيقًا ومرونة عالية في ملاحقتها وكشفها.

ويقصد بذلك الجرائم التي تستهدف معطيات الحاسوب المعنوية من برامج وتطبيقات وبيانات، والتي ترتكب من خلال برامج الحاسوب، أو عن طريق الإنترنت وكذلك الاعتداء على بعض الأجهزة الإلكترونية الخاصة بالاتصال، ومن أهم هذه الجرائم جرائم الاختراق التي وإن كانت هي بذاتها جرائم، فإن هناك أثراً يترتب عليها ويتمثل بارتكاب جريمة أخرى؛ حيث إن المخترق – إثر ارتكاب الاختراق – يمكن أن يقوم بارتكاب جرائم متواصلة عدة في نظام الحاسوب.[١]

الفرع الأول: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

عندما يلتقي الإرهابيون والمجرمون في مكان معين للتعرف على الجريمة وطريقة عمل الإرهاب، وحيث يكون من الصعب عمليا تبادل الأفكار والمعلومات، يتم تسهيل هذه العملية بشكل كبير من خلال شبكات المعلومات والتجمع في أوقات محددة في مواقع متعددة وتبادل المحادثات من خلال شبكات المعلومات، وحتى لقاء بعضهم البعض، ويمكنهم جمع المتابعين ونشر الأفكار والمبادئ من خلال مواقع الويب والمنتديات وغرف الحوار الإلكترونية.[٢]

أصبح البريد الإلكتروني من أكثر المركبات استخداما في مختلف المجالات خاصة في مجال الأعمال لأنه يجعل توصيل الرسائل أسهل وأكثر أمانا وأسرع وهو من أكبر الوسائل المستخدمة في البريد الإلكتروني للتواصل بين الإرهابيين وتبادل المعلومات بينهم، وفي العديد من العمليات الإرهابية الأخيرة، تم استخدام البريد الإلكتروني لتبادل المعلومات بين منفذي العملية الإرهابية

ومخططيها، كما يحتل الإرهابيون البريد الإلكتروني بهدف الانتشار والترويج لأفكارهم وكسب المزيد من المتابعين والمتعاطفين عبر البريد الإلكتروني.[٣]

وتستطيع المنظمات والجماعات الإرهابية عبر شبكات المعلومات نشر الأفكار المتطرفة والدفاع عن المبادئ المنحرفة والسيطرة على الضمائر الفردية واستغلال معاناتهم لتحقيق أهداف غير مشروعة تتعارض مع مصالح المجتمع، ويستخدم الإرهابيون بشكل روتيني شبكات المعلومات العالمية لنشر الأفكار الهدامة وتحقيق أهدافهم الشريرة عن طريق:

١- التواصل وعدم الرؤية:

تستخدم الجماعات والمنظمات الإرهابية المختلفة شبكات المعلومات العالمية للتواصل والتنسيق مع بعضها البعض بسبب انخفاض تكلفة الاتصال ووسائل استخدام الشبكة مقارنة بالوسائل الأخرى إذا لم تكن بحاجة إلى الكشف عنها، فلن تجتذب الانتباه.[٤]

٢- جمع المعلومات الإرهابية:

تتميز شبكات المعلومات بوفرة المعلومات التي تحتويها، وتعتبر موسوعة إلكترونية للمعلومات المتعلقة بتوليد الطاقة، ومواقع القيادة والتحكم والاتصالات وأوقات الطيران، وكيفية مكافحة الإرهاب، يحتوي على معلومات مفصلة مدعومة بصورة بصرية.[٥]

٣- التخطيط والتنسيق للعلميات الإرهابية:

العمليات الإرهابية مهمات معقدة وصعبة فهي تتطلب تخطيطا دقيقا وتنسيقا شاملا وشبكات المعلومات العالمية حرة في التنسيق بعناية وشاملة لشن هجمات إرهابية محددة، وهي وسيلة اتصال مهمة جدا للجماعات الإرهابية لأنها تتيح لها تنسيق تحركاتهم ووقت هجماتهم في جو مريح بعيدا عن المتفرجين.[٦]

٤- إنشاء المواقع الإرهابية الإلكترونية:

ينشئ الإرهابيون ويصممون مواقع على الإنترنت وشبكة المعلومات العالمية لنشر الأفكار المنحرفة واستدعاء المبادئ المنحرفة وتسليط الضوء على قوة المنظمات الإرهابية وتعبئة إرهابيين بذكاء لصنع قنابل ومتفجرات وأسلحة كيماوية قاتلة وشرح كيفية اختراق رسائل البريد الإلكتروني وكيفية اختراق المواقع الإلكترونية وتدميرها وكيفية الوصول إلى المواقع المحجوبة[٧]، فالموقع عبارة عن معلومات مخزنة في شكل صفحات وتحتوي كل صفحة على معلومات محددة تم إنشاؤها بواسطة مصمم الصفحة باستخدام مجموعة من الرموز وتسمى لغة اختيار النص المثلى، ويتم إجراء طلب استعراض لعرض صفحة على شبكات المعلومات العالمية بالإضافة إلى ذلك إذا كان من الصعب على الإرهابيين الحصول على تعليمات لعرض صفحات مكتوبة ومواقع

افتراضية ووسائل إعلام مثل القنوات الإذاعية والتلفزيونية فيمكنهم إنشاء مواقعهم الخاصة على الإنترنت وهي شبكة معلومات عالمية لتحقيق الأهداف وتعزيز المعتقدات الخاطئة، لهذا السبب تمتلك معظم المنظمات الإرهابية مواقع ويب تشبه مقارها الرئيسية الافتراضية.[٨]

إن تواجد الإرهابيين العاملين على شبكات المعلومات متنوع للغاية ومراوغ فإذا ظهر موقع إرهابي اليوم فسيغير عنوانه الإلكتروني على الفور غدا، ثم يختفي بشكل جديد، وتصميم متلف وسيظهر مرة أخرى بشكل إلكتروني مختلف، بعض المنظمات الإرهابية لديها الآلاف من صفحات الويب لضمان انتشار أوسع حتى لو كانت هناك مواقع تم رفض الوصول إليها او تدميرها. وقد وجد الإرهابيون غايتهم في تلك الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، فأصبح للمنظمات العديد من المواقع على الشبكة العالمية للمعلومات وصارت تلك المواقع من أبرز مظاهر وأشكال الإرهاب الإلكتروني.[٩]

: ويقصد بذلك الجرائم التي تتم من خلال استخدام

الحاسوب أو الإنترنت، بوصفها بيئة صالحة لارتكاب هذه الجرائم، عن طريق إيصالها إلى المتلقي، من دون أن يكون هناك إعتداء على النظام المعلوماتي، أو استخدامه لارتكاب جريمة أخرى، ومن أهم هذه الجرائم، إنشاء المواقع الإباحية، واستغلال القاصرين جنسياً، وقد وفرت خدمات الإنترنت أكثر الوسائل فاعلية وجاذبية الصناعة الإباحية ونشرها بشتى وسائل عرضها من صور وفيديوات وحوارات في متداول الجميع، وحتى الأطفال وهذا بالطبع يعد أكبر الجوانب السلبية للإنترنت، وبخاصة في مجتمع محافظ على دينه وتقاليده كالمجتمعات العربية والإسلامية، كما ظهرت مؤخراً جرائم خطيرة مثل التحرش الجنسي بالقاصرين عبر الحاسوب والوسائل التقنية، وتصويرهم وإظهارهم ضمن نشاطات جنسية ومن هذه الجرائم كذلك محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم، وتشويه سمعتهم إذا لم يرضخوا أو لم يدفعوا مقابلاً مادياً وقد يكون الهدف هو الانتقام لأسباب مختلفة.[١٠]

السطو على الأموال المصرفية المعلوماتي: تعد جريمة السطو على أرقام البطاقات الائتمانية، من أوضح الجرائم من ناحية المعرفة كونها مجرمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل المسمى نفسه، والتي يعرف الجميع أنها مخالفة للنظام وللشرع كونهم من الجرائم التي اشتهر محاربتها جنائيا، فقد بدأ مفهوم التجارة الإلكترونية ينتشر في سبعينات القرن الماضي وذلك السهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية فضلا عن السرعة في أرسال البيانات وتخفيض تكلفة التشغيل والأهم هو إيجاد أسواق أكثر اتساعا، ونتيجة لذلك فقد تحول العديد من شركات الأعمال إلى استخدام الإنترنت والاستفادة من مزايا

التجارة الإلكترونية، كما نحول تبعا لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطرا متوافقا مع التجارة الإلكترونية، ومن طرق القرصنة التي تقع على هذه البنوك الافتراضية، تسجيل المعاملات التي تدور بين البنك والعميل عن طريق توصيل جهاز تصنت أو سماعات صغيرة بالخط التليفوني الذي يشغل شبكة الإنترنت، التي يعمل البنك الإليكتروني من خلالها، ثم الحصول من خلال هذه التسجيلات على المعلومات المراد التلاعب بها واستغلالها على نحو غير مشروع، ويمكن كذلك التجسس على المعاملات التي تدور بين البنك والعميل عن طريق توصيل خطوط تحويل ترسل إشارات إليكترونية تحتوي على المعلومات المسروقة، وليس ذلك فحسب، بل هناك بعض الأجهزة الدقيقة التي يستخدمها القراصنة، والتي تمكنهم من ترجمة الإشعاعات الصادرة عن الكومبيوتر إلى معلومات.[١١]

الفرع الثاني: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية:

تشن المنظمات الإرهابية هجمات إلكترونية إرهابية عبر شبكات المعلومات تهدف الهجمات الإرهابية في عصر المعلومات إلى تدمير مواقع الويب والبيانات الإلكترونية وأنظمة المعلومات وإتلاف البنية التحتية للمعلومات وتدميرها وغالبا ما تتضمن ثلاث قوى أساسية هدف عسكري وسياسي واقتصادي مثل مرافق الكهرباء والمياه والبنوك والأسواق المالية هذا لقهر إرادة الشعب والمجتمع الدولي.[١٢]

تتم عملية القرصنة الإلكترونية عن طريق استخراج البيانات الرئيسية وكود برامج الإنترنت وهي عملية يمكن إجراؤها من أي مكا في العالم دون الحاجة إلى وجود المخترق في البلد الذي يتم فيه اختراق الموقع نظرا لتعقيد أنظمة تشغيل الكمبيوتر وشبكات المعلومات لم يتم اكتشاف معدل التطفل بعد. حيث يمكن للإرهابيين شن هجمات مدمرة لإغلاق المواقع الهامة على شبكات المعلومات وشل القيادة والسيطرة على أنظمة الاتصالات ومحطات الطاقة وبالتالي تدمير المواقع الإلكترونية وتشغيلها ومن الممكن تيل هجوم إلكتروني يهدف إلى شل حركة وتحقيق أثر مدمر أكبر من الذي تسببه القنابل والمتفجرات التي تجعل مواقع الأسواق المالية غير صالحة للعمل.[١٣]

فإحدى الطرق المستخدمة حاليا لتخريب المواقع هي إرسال مئات الآلاف من الوسائل الإلكترونية من كمبيوتر المخرب إلى الموقع المستهدف، هذه الكمية الهائلة من الوسائل الإلكترونية المستخدمة للتأثير على سعة تخزين الموقع تخلق ضغطا تؤدي في النهاية إلى انفجار مواقع التشغيل على الشبكة والبيانات المخزنة على الموقع وإرسالها بسبب توزيع المعلومات يسمح لهم بالتسلل إلى جهاز المهاجم والتجول بحرية في موقع مستهدف بكل سهولة ويسر والحصول على كل ما يحتاجون إليه من أرقام ومعلومات وبيانات متعلقة بالموقع المهاجم تعتبر من أخطر آفات

شبكات المعلومات الفيروسات هي برامج حاسوبية تلحق الضرر بنظم المعلومات والبيانات وقادرة على التكاثر والانتشار والتنقل بين الأجهزة.[١٤]

إن الشبكة المعلوماتية الدولية (الإنترنت) تتيح للمنظمات والجماعات الإرهابية نشر أفكارها المتطرفة والدعوة إلى مبادئها المنحرفة والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراض غير مشروعة والتي تتعارض مع مصلحة المجتمع، إذ يستخدم الإرهابيون الشبكة الدولية للمعلومات الإنترنت بشكل يومي لنشر أفكارهم الهدامة وتحقيق أهدافهم السيئة ويمكن إن يتم ذلك من خلال التدريب الإلكتروني إذ يعد أهم هواجس التنظيمات الإرهابية إذ يتم إنشاء معسكرات تدريبية سرية لكن دائما ما تكون عرضة للخطر ويمكن اكتشافها ومداهمتها في أي وقت، كما قامت الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي وكيفية تصنيع القنابل والمتفجرات والمواد الخارقة والأسلحة المدمرة.[١٥]

ومن أبرز الجرائم في الفضاء الإلكتروني التحويلات المصرفية والتزوير والمخالفات الإدارية. فإذا كان الإرهابيون المتطرفون يستخدمون في الماضي أسلحةً مادية، فإن قوتهم العسكرية اليوم تكمن في بناء نظام معلوماتي قادر على الوصول إلى أي مكان في العالم، وتدريب أتباع جدد في أماكن إقامتهم، وتجنيد أعضاء جدد، والضغط على الرأي العام.

أولى هذه الجرائم: التعدي على البيانات الخاصة، ويشمل ذلك تجاوز استخدام المعلومات المجمعة عن الفرد لغرض مقصود، والدخول والتداول غير المرخص به للمعلومات، وكذلك الأخطاء في المعلومات والبيانات، والتشهير والإساءة إلى السمعة، والضغط والابتزاز السياسي[١٦]، ويعد تسهيل جهود عصابات الجريمة المنظمة من أبرز الجرائم التي تقع باستخدام النظام المعلوماتي، وقد كشفت باحثة بريطانية عن استغلال شبكة الإنترنت في تجارة الرقيق الأبيض، من خلال عقد صفقات لبيع الفتيات من أربعين دولة نامية، ومن أوربا الشرقية لمواطنين في دول الغرب من أجل المتعة والجنس، ومن ذلك أيضاً غسل الأموال، وترويج المخدرات، وجرائم الإرهاب، والجرائم ضد الحكومة، وتهديد الأمن القومي والعسكري، والتحويل الإلكتروني، والاحتيال المعلوماتي، والقرصنة الفكرية، والتزوير المعلوماتي، وإنشاء المعلومات، والاستخدام غير المشروع لبطاقات الائتمان، وسرقة المعلومات، والجرائم المتعلقة بالتجارة الإلكترونية

المطلب الثاني: أنواع الجرائم الإرهابية في الفضاء الافتراضي

تُعد الجرائم الإرهابية عبر الفضاء الافتراضي الخاصة بالترهيب من أخطر صور التهديدات الرقمية التي تستهدف زعزعة الشعور بالأمن لدى الأفراد والجماعات والدول، وذلك من خلال

استخدام الوسائل التكنولوجية الحديثة لبث الخوف والرعب أو ممارسة الضغط النفسي والعقلي بغرض تحقيق أهداف إرهابية. وتندرج ضمن هذا النوع من الجرائم أفعال متعددة، من أبرزها التجسس الإلكتروني الذي يستهدف جمع معلومات سرية تتعلق بالأمن القومي أو بالبنى التحتية الحيوية، وكذلك التهديد بنشر معلومات حساسة أو التشهير أو القرصنة لأغراض التخويف، ونشر مشاهد العنف أو البيانات التحريضية ذات الطابع الإرهابي. وتكمن الخطورة الحقيقية لهذه الجرائم في قدرتها على إحداث تأثير نفسي واسع النطاق، وبوسائل يصعب اكتشافها أو مواجهتها بالطرق التقليدية، ما يجعل من مواجهتها تحديًا كبيرًا على المستويين القانوني والأمني.

الفرع الأول: التهديد الإلكتروني:

لاشك في ان شعور الإنسان بالأمان على حياته، واطمئنانه على ماله واعتباره، من أهم المصالح التي يجب على القانون ان يصونها، وأن يعمل على حمايتها بالجزاء الجنائي، لذا فإن مجرد التهديد بارتكاب جريمة تقع على النفس أو المال، أو بإفشاء أمور ماسة بالشرف يعد في ذاته جريمة لِما يثيره في نفس المهدد من الرعب والخوف. فإذا اقترن التهديد بطلب شيء معين أو بتكليف بأمر كان خطره أشد درجة وأبعد عمقا[١٧].

ويشكل التهديد اعتداءً على الطمأنينة وإكراهاً معنوياً للشخص المهدد[١٨]، كما انه يعد من أعمال العنف المعنوي، فهو ينزع الطمأنينة من الشخص الذي يوجه إليه.

أمّا التهديد في الاصطلاح فيُعَرَّف بأنه: "فعل الشخص الذي يُنذر آخر بخطر يريد إيقاعه بشخصه أو بماله"[١٩]. وعرفه آخر بأنه: " توجيه عبارة أو ما في حكمها الى المجني عليه عمداً يكون من شأنها إحداث الخوف عنده من ارتكاب جريمة أو إفشاء أمور أو نسبة أمور مخدشة بالشرف، إذا وجهت بالطريقة التي يعاقب عليها القانون"[٢٠] وعُرِّفَ بأنه: " كل قول أو كتابة من شانها إلقاء الرعب والخوف في قلب الشخص المُهدَّد من ارتكاب الجاني لجريمة ضد النفس والمال أو نسبه أمور مخدشة بالشرف، وقد يحمله التهديد تحت تأثير ذلك الخوف الى إجابة الجاني الى ما ابتغى متى صُحِبَ التهديد بطلب"[٢١] في حين يرى آخر بأن التهديد هو" كل فعل من شأنه بث الرعب أو الخوف في نفس شخص آخر من خطر يراد إيقاعه بشخصه أو بماله أو بأحد أفراد أُسرته"

مما لا شك فيه أن التهديد عبر الدول وتداول المعلومات البسيطة غير المبرمجة وسرعة انتشار شبكة المعلومات أدى إلى التغيير التقني المطرد والمتعاظم في هذا المجال وإلى سهولة تداول المعلومات التي باتت تساعد الإرهاب في الفضاء الافتراضي عن طريق استعمال الحاسوب الشخصي أو الحواسيب الأخرى المستخدمة في دول معينة على الرغم من أن النتيجة الجرمية قد

تتحقق في دولة أخرى، إذ أصبحت جريمة الإرهاب في الفضاء الافتراضي تمثل شكلا جديدا من الجرائم العابرة للحدود وهذه الصور تتخذ طابعا يميزها عن غيرها من الجرائم[٢٢].

أن التهديد الإلكتروني يعد عملا من أعمال العنف المعنوي[٢٣]، فهو ينزع الطمأنينة من الشخص الذي يوجه إليه إذ تعددت الأساليب الإرهابية في التهديد عبر الإنترنت من التهديد بالقتل لشخصيات سياسية إلى التهديد بالتفجيرات والتهديد بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم٢٤، ومن الأمثلة التطبيقية للتهديد الإلكتروني هو ما قام به شاب أمريكي يدعي (Gaher Gwell) البالغ من العمر (١٨) عاما، إذ هدد مدير شركة مايكروسوفت والمدير التنفيذي لتبادل الرسائل وبرمجة التطبيقات بنسف شركتيهما إذا لم يدفع له خمسة ملايين دولار وتم تفتيش منزله بعض القبض عليه وعثروا على حاسبه الآلي على عدة ملفات رقمية تحتوي على معلومات تصنع قنبال تم إنزالها عبر الإنترنت.[٢٥]

أما القصف الإلكتروني فهو أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على استقبال رسائل من المتعاملين معها والذي يؤدي إلى وقف عمل الشركة. وعادة ما تلجأ هذه المنظمات الإرهابية إلى تدمير البنى التحتية الخاصة بأنظمة المعلومات في العالم بأسره. ومثال لمواقع تعرضت للقصف الإلكتروني هو " موقع شركة "أمازون" لبيع الكتب على الإنترنت وأيضا شركة "سي ان ان " للأخبار على الإنترنت مما أدى إلى بطء تدفق المعلومات لمدة ساعتين.[٢٦]

الفرع الثاني: التجسس الإلكتروني

وهو استخدام وسائل تقنية المعلومات الحديثة لسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات والتصنت على هذه المعلومات، أيا كان نوعها، حيث يأخذ أبعاد جديدة فتتعدد أهدافها من معلومات اقتصادية إلى معلومات سياسية وعسكرية وشخصية٢٧، ومن الأمثلة التطبيقية للتجسس الإلكتروني هي التي مارستها بعض الجهات الإرهابية للحصول على المعلومات العسكرية المخزونة في ذكارة الحسابات الآلية التابعة لوزارة الدفاع بالدول المستهدفة وهذا ما حصل في صيف عام (١٩٩٤) عندما تمكنت إحدى هذه الجهات الإرهابية من سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها الجيوش التابعة لدول أعضاء حلف الشمال الأطلنطي من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية مما أثار حفيظة قيادة أركان الحلف وحمل السلطات العسكرية الفرنسية وتصميم برامج جديدة لحماية حاسباتها الآلية.[٢٨]

إن استخدام برنامج في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى

جهاز المعتدى عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغرية يزورها المعتدي عليه فيقوم بتنزيل بعض البرامج ومنها برامج التنصت، أو استخدام برامج المحادثة فيقوم المجرم بإغراء المعتدي عليه بأن هذا البرنامج يحتوي على ألعاب مثيرة أو غير ذلك فيقوم الضحية باستقبال الملف، ولجريمة التنصت المعلوماتي ركيزتان هما[٢٩]:-

أ.الالتقاط: هو مشاهدة البيانات عبر الشبكة المعلوماتية أو أحد أجهزة الحاسوب.

ب.بياء الاعتراض: هو ما مرسل عبر الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي بحيث يتم عمل إجرام كتحويل الأموال

ويتضح مما تقدم أن للإرهاب الإلكتروني نوع من أنواع الإرهاب وشكلا من أشكاله كما أن هناك عوامل عديدة تجعل من ظاهرة الإرهاب في الفضاء الافتراضي موضوعا مناسبا وسلاحا سهلا للجماعات والمنظمات الإرهابية حيث أن من أبرز وأهم مظاهر الإرهاب في الفضاء الافتراضي وأشكاله تتمثل في تبادل المعلومات ونشرها من خلال الشبكة المعلوماتية والتهديد والترويع والتجسس الإلكتروني.

وبالمقارنة بين الجرائم التقليدية والجرائم الإرهابية عبر الفضاء الافتراضي نجد أن **شكل ارتكاب الجريمة** في الجرائم التقليدية بالنسبة للجرائم التقليدية، يكون شكل ارتكاب الجريمة هو نفسه عادةً بناءً على نوع الجريمة. يستخدم المجرمون أسلوبًا وتقنية اعتادوا عليها، ولكن في الجرائم الإلكترونية يختلف شكل ارتكاب الجريمة تمامًا ويتنوع بناءً على التقدم السريع للتكنولوجيا وله اختلافات ملحوظة.

أداة ارتكاب الجريمة على الرغم من تنوع أدوات الجريمة وأدواتها في الجرائم التقليدية، إلا أن جميع هذه الأدوات ملموسة، بينما في الجرائم الإلكترونية تتخذ الأدوات شكلًا أحدث كل يوم وفقًا لتطور التكنولوجيا وتكون في الغالب في شكل برامج برمجية وهي غير ملموسة وملموسة.

اختيار الهدف في الجرائم التقليدية أهداف هجمات المجرمين ملموسة ومادية تمامًا، وتشير جميع مناقشات الشرطة العلمية في البيئة المادية إلى أهداف وأشياء مادية، ولكن في الفضاء الإلكتروني لا توجد هذه الأهداف والأشياء خارجيًا، على الرغم من أن لها مظهرًا خارجيًا. ت. وقت ارتكاب الجريمة. وقت ارتكاب الجريمة في الجرائم التقليدية هو أوقات محددة من اليوم، وحتى مدة ارتكاب الجريمة تعتمد على نوع الجريمة، وتتراوح من بضع دقائق إلى عدة ساعات، بينما الجريمة في الفضاء الإلكتروني لا تعتمد على الوقت. إمكانية ارتكاب جريمة في أي ساعة من اليوم وفي وقت أدنى.

مكان ارتكاب الجريمة. يمكن ارتكاب الجرائم التقليدية في عدة مناطق من المدينة أو تنفيذها في عدة مدن بطريقة منسقة أو عصابة ومنظمة. تعتمد هذه الجرائم على مكان ارتكابها، والطريقة والتقنية، وعدد المجرمين، والأدوات، وعدد الأهداف والغايات، ولكن في الجرائم الإلكترونية يتم استبعاد جميع هذه الحالات ووضعها جانبًا؛ لأن الفضاء الإلكتروني عابر للحدود وليس له جغرافيا، وهناك إمكانية لارتكاب جريمة في منطقة أخرى من أي منطقة من العالم.

مدى ارتكاب عدة جرائم مختلفة في عدة مناطق وفي نفس الوقت أمر مستحيل في الجرائم التقليدية، بينما سيكون ذلك ممكنًا في الجرائم الإلكترونية مع نطاق أكبر من حيث الوقت والمكان وعدد الجرائم.

تحدث المشاركة في جريمة اختيار شريك في كثير من الأحيان في الجرائم التقليدية، وقد يستغرق تحديد الشريك شهورًا وسنوات، بينما تُنفذ الجرائم الإلكترونية في الغالب بشكل فردي، باستثناء الجرائم المنظمة المحددة التي تتطلب تخصصات مختلفة.

الضحية في الجرائم التقليدية هي عادةً ضحية بشرية. في الجرائم ضد الأشخاص، يكون إنسانًا. فتكون السلامة الجسدية والروحية للشخص هي هدف الجريمة، وفي الجرائم ضد الممتلكات، تُرتكب الجريمة ضد ممتلكات محددة ومحددة تخص إنسانًا، ويمكن الحد من الأشخاص الذين فقدوا ممتلكاتهم. بينما في الجرائم الإلكترونية، وبغض النظر عن هوية الضحية وما إذا كان المجرم قد قابله أم لا، فإنه يرتكب جريمة ضده، ويتضرر العديد من الضحايا أو الممتلكات في أقصر وقت ممكن. الهوية في الجرائم الإلكترونية، عادة ما يتم إخفاء هوية المجرم أو المجرمين قبل وأثناء وبعد ارتكاب الجريمة، بينما في معظم الجرائم التقليدية، يتم تحديد هوية المجرم من خلال وجود المجرم في مكان الجريمة أو يتم تحديده في أقصر وقت ممكن أثناء التحقيق في مكان الجريمة.

المبحث الثاني

تطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون العراقي والايراني

أصبح التطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي ضرورة حتمية تمليها التحولات العميقة في طبيعة الجريمة وأساليب ارتكابها، حيث لم تعد الجرائم الإرهابية تقتصر على الأساليب التقليدية، بل انتقلت إلى الفضاء الرقمي، مستفيدة من أدوات التكنولوجيا الحديثة لتوسيع نطاق تأثيرها، والتخفي خلف حدود وهمية لا تعترف بالجغرافيا أو السيادة الوطنية. وبناءً على ذلك، سارعت الدول إلى مراجعة أطرها القانونية لمواكبة هذا التهديد، فظهر توجه عالمي

نحو إدراج الجرائم الإلكترونية ذات الطابع الإرهابي ضمن قوانين العقوبات، أو إصدار قوانين خاصة بمكافحة الجرائم السيبرانية، ومنها العراق وإيران.

في العراق، جاء التطور القانوني استجابةً للتحديات الأمنية التي شهدها البلد، ولا سيما بعد تصاعد النشاط الإرهابي عقب عام ٢٠٠٣، إذ بدأت الجهود التشريعية تتجه نحو تجريم الأفعال الإرهابية الرقمية، وإنْ بشكل تدريجي وغير شامل، من خلال القوانين الخاصة بمكافحة الإرهاب، وبعض التعديلات التي طالت قانون العقوبات، ومشروعات قوانين قيد التشريع تتعلق بالجريمة الإلكترونية.

أما في إيران، فقد اتخذ التطور القانوني طابعاً أكثر مؤسسية، إذ أُنشئت هيئات مختصة بمكافحة الجرائم الإلكترونية، وتم سن قوانين صريحة في مجال الجرائم المعلوماتية والأمن السيبراني، تتضمن نصوصاً تعالج صراحة صوراً متعددة من الأفعال الإرهابية في الفضاء الافتراضي. كما أن السياسة الجنائية الإيرانية تُظهر اتجاهاً واضحاً نحو تشديد العقوبات، وتعزيز الرقابة الحكومية على الفضاء الرقمي، مع التركيز على حماية البنية التحتية للمعلومات والاتصالات من التهديدات الإرهابية. إن دراسة التطور القانوني في كلا النظامين تُبرز الفروقات في الرؤية التشريعية، ومستوى الاستجابة القانونية والفنية لهذه الظاهرة المعقدة، كما تسلط الضوء على أوجه القصور التي ما زالت قائمة، والحاجة إلى تحديث النصوص القانونية وتوسيع نطاقها بما يواكب تسارع الابتكار الرقمي، وارتفاع وتيرة التهديدات الإرهابية العابرة للحدود،

المطلب الأول: تطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون العراقي

شهد الإطار القانوني العراقي تطورًا ملحوظًا في مواجهة الجرائم الإرهابية في الفضاء الافتراضي، نتيجة لتزايد التهديدات التي باتت تشكلها هذه الجرائم على الأمن الوطني والسلم المجتمعي. فقد أدرك المشرع العراقي أهمية التصدي لهذا النوع من الإجرام المتقدم، فبدأ بإدراج نصوص تتعلق بالإرهاب في الفضاء الافتراضي ضمن التشريعات الخاصة بمكافحة الإرهاب، وضمن بعض التشريعات التقنية والمعلوماتية، رغم غياب قانون خاص بالجرائم الإلكترونية حتى وقت قريب. وقد سعى العراق، خصوصًا بعد عام ٢٠٠٣، إلى تحديث بنيته القانونية لتتواكب مع المستجدات التكنولوجية التي استغلها الإرهابيون لنشر أفكارهم وتنفيذ مخططاتهم، مما دفع إلى إدخال تعديلات تشريعية تعزز من قدرة الدولة على الملاحقة والعقاب، إلا أن هذا التطور لا يخلو من التحديات المتعلقة بالضبط التشريعي وصياغة الأحكام بما يحقق التوازن بين مكافحة الإرهاب وحماية الحريات الرقمية.

الفرع الأول: تطور الجرائم الإرهابية في الفضاء الافتراضي في العراق

اما بالنسبة للعراق وبالنظر لكونه من أكثر الدول التي عانت من ويلات الارهاب وما خلفه من عنف وترويع للمواطنين الابرياء مما حدا بالمشرع العراقي إلى تشريع قانون مكافحة الارهاب رقم (١٣) لسنة ٢٠٠٥[٣٠] حيث نصت المادة (٣/١) منه على اعتبار " كل فعل ذو دوافع ارهابية من شأنه تهديد الوحدة الوطنية ويمس امن الدولة واستقرارها أو يضعف من قدرة الاجهزة الامنية في الدفاع والحفاظ على امن المواطنين وممتلكاتهم وحدود الدولة ومؤسساتها سواء بالصدام المسلح مع قوات الدولة أو اي شكل من الاشكال التي تخرج عن حرية التعبير التي يكفلها القانون " وكما اشارت المادة (٣/٢) من قانون جهاز مكافحة الارهاب رقم (٣١) لسنة ٢٠١٦[٣١] على ان " تنفيذ العمليات الامنية والخطط الاستراتيجية فيما يتعلق بفعاليات مكافحة الارهاب وله في سبيل ذلك وفق القانون:.... ب – مراقبة الاتصالات ومواقع التواصل الاجتماعي والمواقع الالكترونية بناء على امر قضائي " ويتضح من ذلك ان المشرع العراقي منح الاجهزة الامنية سلطات واسعة تساعدهم في مواجهة جرائم الارهاب بصورة عامة، والارهاب السيبراني بصورة خاصة، واشترط صدور اذن بإجراء عمليات مراقبة شبكات الاتصالات والانترنت من السلطة القضائية مع توافر التدابير الاجرائية المصرح بها كضمانات اجرائية مناسبة في تلك العمليات.

الا ان التساؤل الذي يثار هنا هو كيفية مواجهة البرامج الالكترونية التي تقوم بهجمات ارهابية، وهي غالبا ما تدار من خارج العراق، لاسيما وان قانون مكافحة الارهاب رقم ١٣ لسنة ٢٠٠٥ وقانون جهاز مكافحة الارهاب رقم ٣١ لسنة ٢٠١٦ لم ينصا صراحة أو يتطرقا إلى تلك الحالات وهذا دليل على وجود قصور تشريعي يجب معالجته؛ كذلك في حالة القاء القبض على شخص يدير صفحة تابعة لتنظيم أو جماعة ارهابية كيف يمكن اثبات تلك الجريمة؟ حتى لو تم اثبات آثار الجريمة فان قانون اصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل[٣٢]، سيقف عائقا امام اثبات الجريمة السيبرانية، لان القضاء العراقي لا يأخذ بالأدلة الالكترونية وهذا ما أكدته المادة ٢١٣ من ذات القانون، وهذا يدل أيضًا على وجود قصور ينبغي معالجته اما بخصوص عدم تشريع قانون الجرائم المعلوماتية والمقترح من مدة ليست بالقليلة، نلحظ ان سبب التأخير بتشريع القانون، هو ان فقرات القانون المقترح وحسب ما نعتقد بانه تم صياغتها من خبراء القانون فقط دون الاستعانة بخبراء الأمن المعلوماتي أو الأمن السيبراني، وبالتالي نلحظ ان روح الفقرات فيه هي قانونية عقابية أكثر مما هي تركز على التقنية وامكانياتها وتأثيراتها وصورها؛ اما اهم المعالجات المقترحة لمواجهة الجريمة السيبرانية وبالأخص الارهاب السيبراني

من وجهة نظرنا، فهي تشريع القانون بصورة عاجلة وكذلك التركيز على الثقافة الالكترونية، وبناء بوابات نفاذ وطنية آمنة، اضافة إلى الاستعانة بتجارب الدول في هذا المجال.[٣٣]

واجه العراق تحديات جسيمة في تطوير إطار قانوني يتعلق بالجرائم الإلكترونية بسبب الأزمات السياسية والأمنية التي شهدها خلال العقود القليلة الماضية. وبالمقارنة مع إيران، تُعتبر قوانين الإنترنت العراقية مجزأة وغير كافية. من أهم العوائق التي تعترض تطبيق قوانين الفضاء الإلكتروني في العراق ضعف البنية التحتية القانونية، ونقص الموارد البشرية المتخصصة، وضعف التنسيق بين أجهزة إنفاذ القانون. كما يفتقر العراق إلى قانون شامل لمكافحة التهديدات السيبرانية، مما يُصعّب تطبيق سياسات جنائية فعّالة. وتُشير الأبحاث إلى أن العراق بحاجة إلى تعاون دولي لوضع هذه القوانين وتطبيقها.[٣٤]

الفرع الثاني: التطور القانوني لمكافحة الجرائم الإرهابية في الفضاء في العراق

يرى المشرع الوطني العراقي أن الإرهاب في الفضاء الافتراضي جريمة جنائية نظرا لما يتوافر فيها من أبعاد مختلفة من الجرائم مثل القتل واستخدام المفرقعات والاغتصاب والسطو والسرقة والإتلاف فهي على هذا الأساس جريمة فوقية تتميز بالعنف الذي وصفه بعضهم بأنه من خصائص الحرب أو النزاع المسلح. ويتطلب التكييف القانوني لجريمة الإرهاب في الفضاء الافتراضي تعريفا قانونيا للجريمة يحدد أركانها؛ يتبناه المشرع وفقا لمبدأ شرعية الجرائم والعقوبات مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب للأفعال التي يتضمنها هذا التعريف، وهو ما فعله المشرع العراقي في قانون مكافحة الإرهاب ذي الرقم (١٣) لسنة ٢٠٠٥ الذي عرف المراد بالإرهاب محددا الأفعال التي تعد إعمالا إرهابية فضلاً عن تحديد العقاب المقرر لكل عمل من هذه الإعمال الإرهابية. وتتميز هذه الجريمة بذاتية خاصة من الناحية القانونية نظرا إلى جسامتها، وهو ما ينعكس بوجه خاص في تجريم مجرد تأسيس الجماعات الإجرامية ومختلف الأعمال التي تساعد على وقوع الإرهاب ومن بينها التمويل.

وفي هذا الصدد يثور السؤال إذا كان الإرهاب في الفضاء الافتراضي في حد ذاته يعتبر جريمة جنائية أم مجرد ظرف مشدد، بالنظر إلى وسائله أو أهدافه أو ضحاياه، فلا شك أن العامل الإرهابي يتجاوز مجرد كونه ظرفا مشددا في جريمة عادية. ويندمج فيها اندماجاً حتى يصبح مكوناً طبيعياً فيها كاشفا لخطورتها وخطورة مرتكبيها.

وأمام خطورة هذه الجريمة يخضع الإرهاب لنظام إجرائي متميز يراعى فيه مدى جسامتها ومختلف أبعادها، ومنها البعد الدولي إذا ما تجاوزت أفعاله حدود دولة معنية، وليس الإقليمية حاسما في تحديد الاختصاص القضائي، بل ينظر عند تجاوز أعمال الإرهاب الإقليم الدولة إلى

جنسية كل من الجناة والضحايا والى عبور وسائله للأوطان والى تنظيماته التي قد تصل إلى حد تكوين الخلايا المنظمة في بعض الدول.[٣٥]

ويهتم هذا الاتجاه بالمعلومات في حد ذاتها؛ ذلك أن الهدف من هذا الاتجاه هو حماية سرية المعلومات مانعا من الاطلاع عليها وسواء أكانت هذه المعلومات متعلقة بأشخاص أو كانت متعلقة بأشياء لها قيمة اقتصادية أو أية معلومة يخشى من الاطلاع عليها. لم يقف الاختلاف بين التشريعات الوطنية في التعامل مع جرائم المعلوماتية عند ما تقدم فحسب، بل أيضا يظهر هذا الاختلاف بوضوح في نمط هذا التدخل والذي قد يأخذ عدة أشكال تتمثل إما بتشريع نصوص قانونية جديدة مضافا إليها البعد الخاص بالنظم المعلوماتية والجرائم الواقعة عليها، أو بتعديل بعض النصوص القانونية القائمة بطريقة تواءم هذه الجرائم المستحدثة، أو أن يلجأ المشرع إلى إفراد قوانين خاصة بهذه الجرائم؛ مواكبة لتطورات ثورة المعلوماتية والتكنولوجية وبالإضافة إلى ما تقدم فإن التصدي لجرائم المعلوماتية على المستوى التشريعي لم تقف عند التشريعات الوطنية المختلفة فحسب، بل وامتدت هذا التصدي إلى المستوى التشريعي الدولي والإقليمي؛ فبسبب خطورة هذه الجرائم وما تتميز به من طبيعة العبور للحدود الدولية بسهولة وخلال لحظات وعجز الدول عن التصدي لها فرادى جعل منها ذلك ذي شأن دولي، ولذا فقد تعاونت العديد من الدول والمنظمات الدولية والإقليمية في ما بينها من خلال ابرام الاتفاقيات الخاصة بتسليم المجرمين وامتداد اجراءات التفتيش إلى العديد من الدول بهدف كشف ومكافحة هذه الجرائم.[٣٦]

أما بشأن مشروع قانون الجرائم المعلوماتية فقد نص المشرع العراقي على تجريم العديد من الجرائم والتي تعد من قبيل جرائم المعلومات في المواد (٥ (٨) وهي جرائم (أولاً: جرائم التعدي على سرية وسلامة البيانات والمعلومات الإلكترونية ونظم المعلومات. ثانياً: جرائم التهديد والابتزاز. ثالثاً: الجرائم الواقعة على البطاقات الإلكترونية. رابعاً: جرائم النظام العام والآداب). كما صادق العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، وذلك بموجب القانون رقم (٣١) لسنة ٢٠١٣ قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد نصت هذه الاتفاقية في المادة (الخامسة) على " تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية

المطلب الثاني: تطور القانوني لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في إيران

شهدت الجمهورية الإسلامية الإيرانية تطوراً ملحوظاً في بنيتها التشريعية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي، نتيجة إدراكها المتنامي لخطورة هذا النوع من الجرائم وارتباطه

المباشر بالأمن القومي والسيادة الوطنية. وقد سعت السلطات الإيرانية إلى مواكبة التحديات الرقمية من خلال سن تشريعات خاصة تتعلق بالأمن السيبراني والجرائم المعلوماتية، فضلاً عن إدراج بعض الأفعال الإلكترونية ذات الطابع الإرهابي ضمن قوانين العقوبات والأمن القومي. ويُظهر هذا التطور القانوني توجهاً واضحاً نحو تبني سياسة جنائية متكاملة تعتمد على تجريم الأفعال الإلكترونية التي تهدد الأمن العام وتؤدي إلى إثارة الرعب أو زعزعة الاستقرار، مع منح الأجهزة المختصة صلاحيات واسعة لرصد ومتابعة هذه الجرائم ضمن إطار قانوني منظم..

الفرع الأول: تطور الجرائم الإرهابية في الفضاء الافتراضي في إيران

مع ظهور الحواسيب، ظهرت جرائم الحاسوب. صُوِّغ مصطلح الإرهاب الافتراضي لأول مرة عام ١٩٩٦ بدمج كلمتي الإرهاب والفضاء الإلكتروني. في الواقع، يعود تاريخ هذه الظاهرة إلى تاريخ الجرائم الإلكترونية، وذلك منذ دخول الإنترنت إلى حياة البشر. بمعنى آخر، يعود تاريخ الإرهاب الافتراضي إلى تاريخ الجرائم الإلكترونية. وبما أن هذه الجرائم نشأت منذ ظهور الإنترنت، فهي ليست قديمة جدًا. علاوة على ذلك، ولأن الإرهاب في الفضاء الافتراضي بحد ذاته ظاهرة جديدة ومثال جديد على الجرائم الإلكترونية، فليس له تاريخ عملي يُذكر. اليوم، يُعد الإرهاب في الفضاء الافتراضي أخطر من الإرهاب التقليدي؛ إذ يُظهر ترابط الإنترنت العالمي وترابطه بوضوح أن الدمار والخراب يمكن أن ينتشرا في جميع أنحاء العالم في لحظة. إن إساءة استخدام تقنيات الحاسوب والإنترنت يمكن أن تُهدد الأمن القومي والسلامة العامة ووجود المجتمع، وتُخلف آثارًا سلبية لا حصر لها على حياة الأفراد في المجتمع. واستخدام الإنترنت وشبكات الحاسوب والمرافق بهدف تدمير شبكات البنية التحتية للمجتمع، كالطاقة والنقل والأنشطة الحكومية، والتأثير على الحكومة والمواطنين والجماعات وما شابه ذلك مما تُنشئه هذه الشبكات. ويرى بعض الخبراء أن الفضاء الإلكتروني أيضًا عامل مؤثر في هذه الجرائم.[٣٧]

وفقًا لأفتانا، فإن الإرهاب الإلكتروني، الذي دخل عقده الرابع هذه الأيام، قد انتشر الآن على نطاق واسع لدرجة أن عام ٢٠١٢ قد أُطلق عليه عام الجحيم في هذا المجال، ويُقال إنه في هذا المجال، سيتمكن أشخاص بمليار دولار وأقل من خمسين فردًا متخصصًا من تعطيل دولة. لم تكن هذه القضية خالية من التأثير على بلدنا، وخلال هذه الفترة، تعرضت إيران أيضًا لهجمات مختلفة في الفضاء الإلكتروني، وبُذلت محاولات لتعطيل أو تعطيل قطاعات مختلفة مثل النفط والصناعة والخدمات المصرفية، إلخ[٣٨]. كان عدد الهجمات الصغيرة والكبيرة التي تم تنفيذها في هذا المجال كبيرًا لدرجة أن وزير الاتصالات قد قدر عددها ذات مرة بما يصل إلى ١٤٠٠٠

هجوم. في غضون ذلك، في حالة لم تتأخر فيها هجمات مثل Flame of Fire و Mini-Film، تتحدث وسائل الإعلام حاليًا عن هجوم ضار جديد يسمى Narilam.[٣٩]

وفي منتصف عام ٢٠٠٨، أفادت وسائل إعلام مختلفة حول العالم بهجوم فيروس تجسس يُدعى ستوكسنت، مؤكدةً أن هذا الفيروس هاجم القطاع الصناعي في عدد من الدول، وأصاب أيضًا بعض أجهزة الكمبيوتر في إيران. وفي الفترة نفسها، أشار محسن حاتم إلى أن هجوم فيروس ستوكسنت على أجهزة الكمبيوتر الإيرانية قد يكون لأسباب اقتصادية أو سياسية، قائلاً: "بدأت الإصابة بهذا الفيروس في إيران قبل حوالي ثمانية أشهر، وليس من الواضح سبب إثارة وسائل الإعلام الأجنبية لهذه القضية الآن". واعتبر أن المراكز الرئيسية التي هاجمها هذا الفيروس هي الصناعات المرتبطة بقطاعي النفط والطاقة، وأفاد بتحديد عناوين IP المصابة وتصميم برنامج مكافحة فيروسات. وبالطبع، هاجم هذا الفيروس الخبيث أيضًا عدة دول مثل الهند وإندونيسيا وباكستان. ويمكن اعتبار فيروس غاوس والنظام المصرفي هجومًا إلكترونيًا آخر استهدف دول الشرق الأوسط بشكل رئيسي. هذا الفيروس، الذي يعتقد العديد من الخبراء في العالم أنه من تصميم نفس مصممي ستوكسنت، كان قادرًا على مهاجمة البنى التحتية الرئيسية للدول. تم التعرف على هذا البرنامج الخبيث في ١٠ أغسطس ٢٠١٢ ضمن عائلة أحصنة طروادة، واستخدمه المهاجمون في منتصف عام ٢٠١١ كحصان طروادة مصرفي، وقُيِّمت الأنظمة المستهدفة بهذا البرنامج الخبيث على أنها أنظمة من عائلة ويندوز. في الواقع، صُمم هذا البرنامج الخبيث للوصول إلى معلومات من أنظمة الضحايا وسرقة معلومات الائتمان من البريد الإلكتروني وشبكات التواصل الاجتماعي، ولم يكن هدفه تخزين جميع أنواع المعلومات التي يمكن جمعها، بل خصائص النظام المستخدم ومعلومات الخدمات المصرفية ومعلومات الإنترنت للمتصفح المُختار لهذا البرنامج الخبيث. هجوم Flame على معدات النفط. ومع ذلك، خلال هذه الفترة، كان أحد أخطر الهجمات الإلكترونية هجومًا على معدات النفط في الشرق الأوسط. هذا البرنامج الخبيث، الذي أُرسل إلى دول مختلفة تحت اسم Flame، كان معقدًا للغاية، واعتُبر فيروسًا مدمرًا بالإضافة إلى كونه تجسسًا. في هذا الصدد، قبل تقرير سيمانتك، كان يُعتقد أن فيروس Flame مجرد أداة تجسس وسرقة بيانات، لكن المتحدث باسم سيمانتك، فيكرام ثاكور، صرّح بأن الشركة حددت جزءًا من فيروس Flame يمكنه إزالة الملفات من أجهزة الكمبيوتر. أولاً، يُستخدم Flame أو Gauss لإصابة أكبر عدد ممكن من الضحايا وجمع كمية كبيرة من المعلومات. بعد جمع البيانات ومراجعتها، يتم اختيار ضحية مثيرة للاهتمام وتحديد هويتها. بعد ذلك، يتم تثبيت Mini Flame على نظام الضحية المحددة لمواصلة المراقبة الأعمق والتجسس

الأكثر تفصيلاً. Clean، مما يعني أن فيروس Flame يمكنه إصابة بعض برامج Apple المهمة وتعطيل تشغيلها، ويمكنه حتى تعطيل نظام التشغيل تمامًا. بعد أيام قليلة من نشر خبر هذا البرنامج الخبيث، ادعى مركز ماهر أنه أنتج أول أداة لإزالة البرامج الضارة Flame في العالم وسيتيحها قريبًا للمستخدمين من خلال موقع مركز ماهر. يُعتبر Flame of Fire أحد أكثر البرامج الضارة تطوراً حيث لم يتمكن ٤٣ برنامج مكافحة فيروسات مختلف من اكتشافه. بالإضافة إلى إيران، كانت فلسطين والمجر ولبنان وأستراليا وسوريا وروسيا وهونغ كونغ والإمارات العربية المتحدة من بين الدول المستهدفة بهذا البرنامج الخبيث.[٤٠]

وفي أواخر يوليو من من العام السابق، اكتُشف فيروس نشط لأكثر من ثمانية أشهر، وأُعلن عن إصابة حوالي ٨٠٠ جهاز كمبيوتر به. وكانت شركة كاسبرسكي أول من أعلن عن إطلاق هذا الفيروس، زاعمةً أنه أصاب أكثر من ٨٠٠ جهاز كمبيوتر وأنه نشط لأكثر من ثمانية أشهر. ولم يتضح بعد سبب انتشار هذا الفيروس البسيط، الذي اكتشفته شركات مكافحة فيروسات مرموقة منذ فترة طويلة، على نطاق واسع في الأخبار في وقت معين. ومن بين وظائف هذا الفيروس تسجيل معلومات لوحة المفاتيح، والتقاط صور لشاشة العرض على فترات زمنية محددة، والتقاط صور أثناء استخدامه، وإنشاء ثغرات تسمح للمهاجم بالتسلل والوصول، وتسجيل وتخزين وإرسال ملفات جيميل أو فيسبوك، ومكالمات سكايب الصوتية. وقد نصح وزير الاتصالات وتكنولوجيا المعلومات المستخدمين بشأن هذا الفيروس بالامتناع عن فتح رسائل البريد الإلكتروني والملفات المرسلة إليهم من مستخدمين مجهولين. ويشير هذا إلى أنه برنامج خبيث بسيط ومنخفض التكلفة، وأنه لم تُجرَ أي دراسات على عينات محددة من نقاط الضعف التي قد تنتشر وتضر بالأنظمة[٤١]. لذلك، وعلى عكس الادعاءات المقدمة، فإن اعتباره تهديدًا إلكترونيًا مستهدفًا يبدو بعيد المنال عند مقارنة هذا البرنامج الضار بتهديدات مثل Miniflame. Flame في أوائل أكتوبر ٢٠١٤، بعد بضعة أشهر فقط من إصدار برامج ضارة مثل Flame وGauss، بدأ برنامج ضار يسمى Miniflame تجسسه[٤٢]. وفيما يتعلق بهذا البرنامج الضار، أُعلن أن Miniflame هو في الواقع شكل جديد من برامج Flame الضارة التي تدعمها الحكومات ومصممة خصيصًا للتجسس، ويبدأ هذا البرنامج الضار في العمل حيث ينتهي عمل Flame. وذكر شرح كاسبرسكي لـ Miniflame: أولاً، يتم استخدام Flame أو Gauss لإصابة أكبر عدد ممكن من الضحايا وجمع كمية كبيرة من المعلومات. بعد جمع البيانات ومراجعتها، يتم اختيار ضحية مثيرة للاهتمام وتحديد هويتها. ثم يتم تثبيت Miniflame على نظام الضحية المحددة لمواصلة المراقبة الأعمق والتجسس الأكثر دقة. وفقًا لمركز ماهر، يُرجَّح أن يكون

مطورو Miniflame قد بدأوا عملهم عام ٢٠٠٧. ومن النقاط الأخرى أنه قيل إن معدل الإصابة بهذا البرنامج الخبيث كان منخفضًا، خاصةً مقارنةً ببرنامجي Gauss وFlame، وأن ٥٠ إلى ٦٠ جهاز كمبيوتر فقط حول العالم قد أُصيب بهذا البرنامج الخبيث. ومع ذلك، في هذا النوع من الهجمات، لا ينصب التركيز على عدد الضحايا، بل على أهداف محددة. في أوائل عام ٢٠١١، كان هناك حديث عن ظهور برنامج خبيث جديد يُسمى Narilam، على الرغم من أن مركز ماهر يؤكد أن هذا البرنامج الخبيث تم تحديده والإبلاغ عنه عام ٢٠١٠ من قِبل مراكز وشركات نشطة في مجال أمن تكنولوجيا المعلومات في البلاد. ينص إعلان مركز إدارة الكوارث وتنسيق عمليات حوادث الكمبيوتر على ما يلي: تُظهر التحقيقات الأولية حتى الآن أن البرنامج الخبيث المذكور أعلاه لا يُشكِّل تهديدًا إلكترونيًا خطيرًا، على عكس الأخبار المنشورة، ولكنه برنامج خبيث محلي يُرجَّح أنه صُمِّم لإلحاق الضرر بمستخدمي منتجات برامج شركة مُحدَّدة. لا يتسم تصميم وتنفيذ هذا البرنامج الخبيث بتعقيد الهجمات الإلكترونية أو حتى البرامج الضارة القوية التي تنتجها مجموعات التخريب الإلكتروني، بل يُشبه إلى حد كبير البرامج الضارة للهواة. نطاق هذا البرنامج الخبيث وانتشاره محدود للغاية، ولا يمكن فحص النظام باستخدام برامج مكافحة الفيروسات المُحدثة إلا لمستخدمي برامج المالية والمحاسبة. ومع ذلك، أقرّ بعض نشطاء الفضاء الإلكتروني في هذا الصدد بأنه بغض النظر عما إذا كان يُمكن اعتبار النسخة الجديدة من فيروس "ناريلام" برنامجًا خبيثًا مُعاديًا لإيران لأغراض سياسية، تم إنتاجه ونشره بهدف مهاجمة البنية التحتية المعلوماتية للبلاد، أو ما إذا كانت مُبالغة وسائل الإعلام في تصوير هذا الفيروس مجرد حيلة إعلانية تجارية، يجب على مديري الشبكات التنظيمية في البلاد إيلاء أقصى درجات الاهتمام واليقظة في مراعاة جوانب الحماية والأمن في الشبكة لتقليل احتمالية اختراق هذا البرنامج الخبيث أو أي عدوى فيروسية مُماثلة.[٤٣]

وسيطر ستوكسنت على الأجهزة، وكان هدفه أجهزة الطرد المركزي النووية في منشأة نطنز في إيران. صُممت الأداة لتكون سرية للغاية حتى لا تُعتبر عملاً حربياً، وهو أمرٌ بديهي عادةً. ووفقًا لشبكة CNN، أكد أليكس جيبني، منتج فيلم "أيام الصفر"، في مقابلة مع هذه الشبكة أن ستوكسنت من عمل الموساد ووكالة المخابرات المركزية الأمريكية. وفي حديثها عن القضية النووية الإيرانية والهجوم على هذا البرنامج قبل بضع سنوات باستخدام برنامج ستوكسنت الخبيث، قالت كريستيان أمانبور إن هذا البرنامج الخبيث قوي لدرجة أنه يمكن وصفه بوضوح بأنه سلاح إلكتروني. وقد أنتج المخرج الأمريكي أليكس جيبني فيلمًا وثائقيًا عن ستوكسنت والحرب الإلكترونية بعنوان "أيام الصفر". وفي هذا الصدد، قال جيبني إنه في البداية لم يكن أحد

على علم ببرنامج ستوكسنت حتى تحدث عنه خبراء الأمن السيبراني ونُشرت عنه مقالات في الصحف. كما كتب ديفيد سانجر عنه في صحيفة نيويورك تايمز. ومنذ ذلك الحين، بدأنا أيضًا بدراسة ستوكسنت بشكل أعمق.[٤٤]

الفرع الثاني: التطور القانوني لمكافحة الجرائم الإرهابية في إيران

أولا: قانون مكافحة الدعم المالي للإرهاب

في عام ٢٠٠٣، أُعِدَّ مشروع قانون بعنوان "مكافحة الإرهاب" لأول مرة في حكومة جمهورية إيران الإسلامية، وأُجريت عليه العديد من الآراء من قِبَل الخبراء؛ إلا أنه نظرًا لاعتقاد البعض بأنه على الرغم من تجريم الجرائم شبه الإرهابية مثل المحاربة والفساد في الأرض، لم يُقرَّ هذا القانون؛ إلا أنه منذ أوائل التسعينيات، عادت قضية الإرهاب وضرورة تجريمه كجريمة أو سلوك إجرامي إلى جدول الأعمال. بناءً على الظروف الخاصة السائدة آنذاك، وتأثرًا بضرورة الفترة الانتقالية من قرارات العقوبات المفروضة على جمهورية إيران الإسلامية، أولت السياسة الجنائية التشريعية اهتمامًا بمكافحة تمويل الإرهاب، كجزء من مجمل مكافحة الإرهاب، وتمت الموافقة على "قانون مكافحة تمويل الإرهاب" في ٢٢ ديسمبر ١٩٩٤ وإصداره في ١٠ فروردين ١٣٩٥. ومما لا شك فيه، وبغض النظر عن استمرار الاعتراض الأساسي على عدم وجود تجريم مستقل ومعاقبة دقيقة للجرائم والجرائم الإرهابية، فإن إقرار القانون المذكور، مع استثناءات عديدة في مجال مكافحة غسل الأموال، يُعد مؤشرًا على عزم جمهورية إيران الإسلامية على مكافحة جذور ودوافع الأعمال الإرهابية. وفي ظل عولمة القانون الجنائي، يتمتع النظام القانوني الإيراني بأكبر قدر من التقارب في القضايا المتعلقة بمختلف الأبعاد الاقتصادية. وبناءً على ذلك، أصبح تمويل الإرهاب، مثله مثل غسل الأموال، قضيةً من قضايا القانون الجنائي الإيراني من خلال الضغط على المؤسسات الاقتصادية وملاحقتها. إن العوامل والمؤسسات المشاركة في مكافحة تمويل الإرهاب واسعة النطاق وشاملة، وفي الوقت نفسه فإن البنك المركزي، باعتباره السلطة النقدية للدول، من أجل القيام بواجباته، وخاصة تنظيم حجم السيولة والسيطرة على معدل التضخم، يواجه حتما أبعادا مختلفة من الاقتصاد الموازي، والتي يعد تمويل الإرهاب مثالا عليها.[٤٥]

عند مراجعة القانون، تجدر الإشارة إلى أن أهم ما ورد في نصه ليس تعريف تمويل الإرهاب، بل تعريف الإرهاب نفسه. يُعرّف هذا القانون الإرهاب لأول مرة في النظام القانوني الإيراني. سابقًا، لم يكن الإرهاب مُعرّفًا في القانون الإيراني، وكان التعامل القانوني مع شخص إرهابي يعتمد على مسميات جنائية أخرى مثل مكافحة الفساد في الأرض والانقلاب وما شابه. يُقدّم هذا القانون تعريفًا مُعقّدًا نسبيًا للإرهاب، مُستمد من اتفاقية الأمم المتحدة لقمع تمويل الإرهاب. يختلف

التعريف الوارد في القانون الإيراني لقمع تمويل الإرهاب في نقطة واحدة عن التعريف الوارد في الاتفاقية الدولية لقمع تمويل الإرهاب. فبينما تنص الاتفاقية الدولية على أن ضحية العمليات الإرهابية هو الشخص الذي لا يكون عضوًا نشطًا في القوات المسلحة أثناء نزاع مسلح، ينص القانون المُقرّ في إيران على أن ضحية العمليات الإرهابية هو الشخص الذي يتمتع بالحصانة القانونية. ويبدو أن خطأً في الترجمة أدى إلى إقرار القانون الإيراني بهذه الطريقة. من الناحية القانونية، من يقتل شخصًا آخر في الحرب، لا يُعتبر إرهابيًا، بل مُحاربًا أو مُقاتلًا، وإذا أُسر، لا يُمكن اعتقاله ومحاكمته كإرهابيين. تخيّل أن الحكومة الإيرانية في حالة حرب مع حكومة أجنبية. أُسر مُقاتل إيراني. لا يحق للحكومة الأجنبية مُحاكمة ومعاقبة أسير حرب باعتباره إرهابيًا في محاكمها، والعكس صحيح، لا يحق لإيران فعل الشيء نفسه مع أسرى الطرف الآخر.

لذلك، على الرغم من أن المقاتل الإيراني يرتكب عملاً من أعمال العنف (الحرب) ضد دولة أجنبية وكان هدفه التأثير على سياسة الدولة المعادية وخطها، إلا أنه لا يمكن اعتبار هذا العمل إرهابيًا؛ لأنه قاتل مع مقاتلي الدولة المعادية، وليس مع مواطنين عاديين. في قانون الحرب، تُقال هذه العبارة على النحو التالي: المقاتل هو شخص يمكنه القتل ويمكن قتله. أي أنه إذا قتل، فهو ليس إرهابيًا، وإذا قُتل، فلا يُعتبر قاتله إرهابيًا. لذلك، إذا ارتكب أعمال عنف ضد شخص آخر، فسيُعتبر عمله إرهابيًا إذا لم يكن الضحية ضد المقاتل. أيضًا، إذا صدر حكم بالإعدام على شخص ما وقام الجلاد بتنفيذ هذا الحكم، فلن يُعتبر الشخص الذي نفذ هذا الحكم إرهابيًا، حتى لو كان هذا العمل عنيفًا. وبناءً على ذلك، استُخدمت عبارة "الأبرياء" في بعض الوثائق الدولية. تعني هذه العبارة الشخص غير المقاتل أو المحكوم عليه بالإعدام. في إيران، تُترجم هذه العبارة إلى "الأشخاص ذوي الحصانة القانونية". مع ذلك، فإن الشخص الذي يتمتع بالحصانة القانونية هو من يتمتع بالحصانة الدبلوماسية أو البرلمانية، وهذه الترجمة غير صحيحة. حاليًا، يُفسر هذا الجزء من المادة (١) من القانون بأنه إذا قتل شخص سفير دولة أجنبية في إيران بقصد التأثير على السياسة الإيرانية، فقد ارتكب عملاً إرهابيًا، ولكن إذا قتل مئات الإيرانيين الذين لا يتمتعون بالحصانة، فلا يمكن اعتباره إرهابيًا. هذا النهج لا يتوافق مع المعايير الدولية ولا مع المنطق السليم، ويبدو أنه ينبغي تعديل هذا الجزء من القانون في أقرب وقت ممكن وإزالة هذا العيب.

ثانيا: قانون جرائم الحاسوب تُعدّ مواد قانون جرائم الحاسوب، مثل المواد ١ و٣ و٤ و٩٨ و١٠ و١١، حاليًا، خطوةً رائدةً إلى حدٍ ما في تكييف بعض حالات الإرهاب في الفضاء الافتراضيمع هذه المواد القانونية.

وبذلت إيران، باعتبارها إحدى الدول الرائدة في المنطقة، جهودًا كبيرة لتنظيم وصياغة القوانين المتعلقة بالجرائم الإلكترونية. ويُعرف قانون جرائم الحاسوب الإيراني، الذي صدر عام ٢٠٠٩، بأنه الإطار الرئيسي لمكافحة الجرائم الإلكترونية. ويغطي هذا القانون قضايا مثل الوصول غير المصرح به، وتزوير بيانات الحاسوب، والاحتيال الإلكتروني. ومع ذلك، تُظهر الدراسات أن هذا القانون يعاني من أوجه قصور في مجالات أحدث مثل حماية البيانات الشخصية والأمن السيبراني من التهديدات العابرة للحدود الوطنية.[٤٦]

الخاتمة

في ضوء ما تقدم، يتضح أن الجرائم الإرهابية في الفضاء الافتراضي أصبحت تشكل تحدياً متزايداً للأمن القانوني والرقمي في الدول المعاصرة. وقد أظهرت الدراسة أن التشريعات في كل من العراق وإيران سعت إلى مواكبة هذه الظاهرة، إلا أن هناك تفاوتاً في مستوى التطور والمرونة التشريعية بينهما. كما تبين أن الطبيعة المتغيرة للتكنولوجيا تفرض ضرورة تحديث مستمر للأطر القانونية. ويؤكد ذلك أهمية التكامل بين التشريع الوطني والتعاون الدولي لمكافحة هذه الجرائم. وعليه، فإن تطوير سياسات قانونية حديثة يمثل ضرورة ملحة لتعزيز فاعلية المواجهة القانونية للإرهاب الإلكتروني.

أولاً: **النتائج**

١.وجود تنوع في صور الجرائم الإرهابية في الفضاء الافتراضي، مثل التجنيد الإلكتروني والتحريض والتمويل الرقمي .

٢.قصور نسبي في بعض النصوص القانونية العراقية والإيرانية في مواكبة التطورات التقنية المتسارعة .

٣.تفوق نسبي لبعض التشريعات في معالجة الجوانب الأمنية مقارنة بالجوانب الوقائية .

٤.ضعف التنسيق الدولي والإقليمي في مكافحة الإرهاب الإلكتروني يؤثر على فعالية المواجهة .

٥.اعتماد الجماعات الإرهابية بشكل متزايد على التكنولوجيا الحديثة في تنفيذ أنشطتها .

ثانياً: المقترحات

١.تحديث التشريعات الوطنية بشكل دوري بما يتلاءم مع التطور التكنولوجي المستمر .

٢.سن قوانين متخصصة في الجرائم الإرهابية الإلكترونية بدلاً من الاكتفاء بالنصوص العامة .

٣.تعزيز التعاون الدولي وتبادل المعلومات بين الدول لمكافحة هذه الجرائم .

٤.تطوير قدرات الأجهزة الأمنية والقضائية في مجال الجرائم السيبرانية .

٥.نشر الوعي المجتمعي حول مخاطر الفضاء الافتراضي وسبل الوقاية من الاستقطاب والتطرف الإلكتروني .

قائمة المصادر والمراجع:

أولا: الكتب والمؤلفات

١. إبراهيم، ماجد موريس .الإرهاب الظاهرة وأبعادها النفسية .دار الفارابي، لبنان، ٢٠٠٥.

٢. الأشقر، جبور منى .السيبرانية هاجس العصر .المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٦.

٣. بسيوني، محمود شريف .الجرائم ضد الانسانية في القانون الجنائي الدولي .القاهرة، ١٩٩٩.

٤. بسيوني، محمود شريف .الجريمة المنظمة عبر الوطنية وماهيتها ووسائل مكافحتها دوليا وعربيا .دار الشروق، القاهرة.

٥. بوادي، حسنين المحمدي .الإرهاب الإلكتروني بين التجريم والمكافحة .دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.

٦. الجبوري، سليم عبد الله .الحماية القانونية لمعلومات شبكة الإنترنت .منشورات الحلبي الحقوقية، بيروت، ٢٠١١.

٧. جعفر، علي عبود، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ٢٠١٣.

٨. سلامة، محمد عبد الله أبو بكر .جرائم الكمبيوتر والإنترنت .منشأة المعارف، الإسكندرية، ٢٠٠٦.

٩. سليمان، احمد ابراهيم مصطفى .الارهاب والجريمة المنظمة التجريم وسبل المواجهه.2007 .

١٠. شوقي، حسام .حماية وأمن المعلومات على الإنترنت .دار الكتب العلمية، القاهرة، ٢٠٠٣.

١١. عبد التواب، معوض .السرقة واغتصاب السندات والتهديد .دار المشرق العربي، القاهرة، ١٩٨٨.

١٢. عبد الصادق، عادل، الإرهاب الإلكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الاهرام للدراسات السياسية و الاستراتيجية، القاهرة ، ٢٠١٣.

١٣. عبد الملك بك، جندي .الموسوعة الجنائية .دار الكتب المصرية، القاهرة، ١٩٣٢.

١٤. عبيد، رؤوف .جرائم الاعتداء على الأشخاص والأموال في القانون المصري .مطبعة نهضة مصر، ١٩٦٥.

١٥. العريمي، مشهور بخيت الشرعية الدولية لمكافحة الإرهاب .دار الثقافة، عمان، ٢٠٠٩.

١٦. غارو، رنيه .موسوعة قانون العقوبات العام والخاص .منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣.

١٧. فاضل، محمد .التعاون الدولي في مكافحة الجريمة .منشورات جامعة دمشق، دمشق، ١٩٩٧.

١٨. الفقي، عمر عيسى .الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية .المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٦.

١٩. الفيل، علي عدنان .الجرائم الإلكترونية، دراسة مقارنة .منشورات زين الحقوقية، بيروت، ٢٠١١.

٢٠. مطر، عصام عبد الفتاح عبد السميع .الجريمة الإرهابية .دار الجامعة الجديدة، الإسكندرية، ٢٠٠٥.

٢١. المقاطع، محمد عبد المحسن .حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي .ذات السلاسل، الكويت، ١٩٩٢.
٢٢. المناعسة، أسامة أحمد وآخرون .جرائم الحاسوب الآلي والإنترنت .دار وائل للنشر، الأردن، ٢٠٠١.
٢٣. منشاوي، محمد عبد الله .جرائم الإنترنت من منظور شرعي وقانوني .مطبعة جامعة الملك فهد، الرياض، ٢٠١١.
٢٤. نيك، كلارك ريتشارد وروبرت .حرب الفضاء الإلكتروني .مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠١٢.
٢٥. ونس، عمر محمد أبو بكر .الجرائم الناشئة عن استخدام الإنترنت .دار النهضة العربية، القاهرة، ٢٠٠٤.
٢٦. يوسف، أمير فرج .الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت .مكتبة الوفاء القانونية، مصر، ٢٠١١.

ثانيا:المجلات والدوريات

١.جلالی فراهانی امیر حسین .تروریسم سایبری .نشریه حقوق اسلامی، سال سوم، شماره ١٠، ١٣٨٥.
٢.روح الله خیرانی آرانی، شهرام زرنشان، محمدهادی سلیمانیان .ارزیابی وضعیت ایران در ارتباط با مقررات بین المللی مرتبط با پول شویی .مجله پژوهشهای حقوقی، دوره ٢١ شماره ٤٩، ١٣٠١.
٣.فیرحی، داود و ظهیری صمد .رهیافتهای موجود در تحلیل پدیده تروریسم .فصلنامه سیاست مجله دانشکده حقوق و علوم سیاسی، شماره ٣، ١٣٨٧.
٤.لیلا میرید، صادق سلیمی صابر نیاورانی، سید قاسم زمانی .تروریسم سایبری نقض حقوق بشر و آزادیهای بنیادین .فصلنامه حقوق پزشکی ویژه نامه حقوق بشر و حقوق شهروندی، ١٣٩٨.
٥.نیازپور، امیر حسن .پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم .مجله حقوقی دادگستری شماره ٤٥، ١٣٨٤.

ثالثا:الرسائل والأطروحات

١. الأسدي، لينا محمد متعب .مدى فاعلية أحكام القانون الجنائي في مكافحة جريمة المعلوماتية – دراسة مقارنة .رسالة ماجستير، جامعة النهرين، العراق، ٢٠١٢.
٢. عبد الله، أحمد كيلان .حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي .أطروحة دكتوراه، جامعة بغداد، ٢٠٠٧.

رابعا: المؤتمرات والأوراق البحثية

١. پرویزی، رضا. جرم های رایانه ای .مجموعه مقاله های همایش بررسی جنبه های حقوقی فن آوری اطلاعات قوه قضائیه، ١٣٩٢.
٢. رضوی فرد، بهزاد .سخن دبیر علمی همایش چکیده مقالت همایش بین المللی ابعاد حقوقي – جرم شناختي تروریسم .انتشارات دانشگاه علامه طباطبائي، ١٣٩٦.
٣. عرب پور امیر حمزه شادمان فر محمد رضا .سیاست جنایی اجرایی جمهوری اسلامی ایران در مقابلة باتروریسم سایبری .(١١)(٤٥)،١٣٩٩.

٤. مريم شيريان نسل، زهرا نورى زاده خامنه .تروريسم سايبرى و نقش گروه تروريستى داعش في فضاء مجازي .جامعة آزاد الإسلامية وحدة مراغة، ١٤٠٢.

٥. موسسه توسعه حقوق فناورى اطلاعات برهان مشاوره حقوقى .مفهوم شناسى جرايم رايانه اى جرايم اينترنتى و جرايم سايبرى.1394 .

خامسا: القوانين والتشريعات

١.قانون اصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل

٢.قانون مكافحة الارهاب رقم ١٣ لسنة ٢٠٠٥.

٣.قانون جهاز مكافحة الارهاب رقم ٣١ لسنة ٢٠١٦.

الهوامش

[١]. ونس، عمر محمد أبو بكر، ٢٠٠٤، الجرائم الناشئة عن استخدام الإنترنت دار النهضة العربية، القاهرة، ص ٣٣٦.

[٢]. بوادي، حسنين المحمدي، ٢٠٠٥، الإرهاب الإلكتروني بين التجريم والمكافحة، دار الفكر الجامعي، الإسكندرية، ص ٣٤.

[٣]. يوسف، أمير فرج، ٢٠١١، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الطبعة الأولى، مصر، ص ١٠١.

[٤]. إبراهيم، ماجد موريس، ٢٠٠٥، الإرهاب الظاهرة وأبعادها النفسية، الطبعة الأولى، دار الفارابي، لبنان، ص ٢٣.

[٥]. مطر، عصام عبد الفتاح عبد السميع، ٢٠٠٥، الجريمة الإرهابية، دار الجامعة الجديدة، الإسكندرية، ص ١٨٣.

[٦]. عبد الصادق، عادل، الإرهاب الإلكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مصدر سابق، ص ١٣٧.

[٧]. بوادي، حسنين المحمدي، الإرهاب الإلكتروني بين التجريم والمكافحة، مصدر سابق، ص ٤٢.

[٨]. الفقي، عمر عيسى، ٢٠٠٦، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، ص ٨٤.

[٩]. منشاوي، محمد عبد الله، ١٤٣٢، جرائم الإنترنت من منظور شرعي وقانوني، مطبعة جامعة الملك فهد، الرياض، ص ٣٨.

[١٠]. شوقي، حسام، ٢٠٠٣، حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية، القاهرة، ص ٨٥

[١١]. الأشقر، جبور منى، ٢٠١٦، السيبرانية هاجس العصر: جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت، ص ٢٧

[١٢]. إبراهيم، ماجد موريس، الإرهاب الظاهرة وأبعادها النفسية، مصدر السابق، ص ٣٦.

[١٣]. فاضل، محمد، ١٩٩٧، التعاون الدولي في مكافحة الجريمة، منشورات جامعة دمشق، دمشق، الطبعة السابعة، ص ٩٦.

[١٤]. بسيوني، محمود شريف، الجريمة المنظمة عبر الوطنية وماهيتها ووسائل مكافحتها دوليا وعربيا، الطبعة الأولى، دار الشروق، القاهرة، ص ٥٧.

[١٥]. العريمي، مشهور بخيت، ٢٠٠٩، الشرعية الدولية لمكافحة الإرهاب، الطبعة الأولي، دار الثقافة، عمان، ص ١٦١.

[١٦]. المقاطع، محمد عبد المحسن، ١٩٩٢، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، ذات السلاسل، الكويت، ص ٩٦ وما بعدها.

[١٧]. عبد التواب، معوض، ١٩٨٨، السرقة واغتصاب السندات والتهديد، دار المشرق العربي، القاهرة، ص٣٧٥ -٣٧٦.

[١٨]. غارو، رنيه، ٢٠٠٣، موسوعة قانون العقوبات العام والخاص، ترجمة لين صلاح مطر، المجلد السادس، منشورات الحلبي الحقوقية، بيروت، ص ٣١٥-٣١٦.

[١٩]. عبد الملك بك، جندي، ١٩٣٢، الموسوعة الجنائية، ج٢، ط١، دار الكتب المصرية، القاهرة، ص٧٥٥.

[٢٠]. عبيد، رؤوف، ١٩٦٥، جرائم الاعتداء على الأشخاص والأموال في القانون المصري، ط٥، مطبعة نهضة مصر، ص٣٧٤.

[٢١]. عبد الله، أحمد كيلان، ٢٠٠٧، حجية المحررات المستخرجة من الحاسوب في الإثبات الجنائي: أطروحة دكتوراه، جامعة بغداد، كلية القانون، ص ٧٣.

[٢٢]. المناعسة، أسامة أحمد وآخرون، ٢٠٠١، جرائم الحاسوب الآلي والإنترنت، الطبعة الأولى، دار وائل للنشر، الأردن، ص ١٠٥.

[٢٣]. العنف المعنوي: هو كل فعل لا يترك أي أثر مادي على جسد الضحية لأن قوام الفعل المعنوي هو العنف، التهديد، الخوف، الرعب وغيرها من صور العبث بعاطفة الإنسان التي تؤدي إلى حدوث موت مفاجئ أو سكتة قلبية تؤدي بحياة المجني عليه.

[٢٤]. الفيل، علي عدنان، ٢٠١١، الجرائم الإلكترونية، دراسة مقارنة، منشورات زين الحقوقية، بيروت، لبنان، ص ٧٩.

[٢٥]. الجبوري، سليم عبد الله، ٢٠١١، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، ص ٣٥٩.

[٢٦]. سليمان، احمد ابراهيم مصطفى، ٢٠٠٧، الارهاب والجريمة المنظمة... التجريم وسبل المواجهه، ط، ١، ص ٨٥

[٢٧]. جعفر، علي عبود، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، مصدر سابق، ص ٥٦٩.

[٢٨]. سلامة، محمد عبد الله أبو بكر، ٢٠٠٦، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ص ١٤٥.

[٢٩]. نيك، كلارك ريتشارد وروبرت ٢٠١٢، حرب الفضاء الإلكتروني، ط ١ مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ص ٤٩

[٣٠]. قانون مكافحة الارهاب رقم ١٣ لسنة ٢٠٠٥، المصدر الوقائع العراقية، العدد ٤٠٠٩ لسنة ٢٠٠٥

[٣١]. ينظر قانون جهاز مكافحة الارهاب رقم ٣١ لسنة ٢٠١٦، المصدر الوقائع العراقية، العدد ٤٤٢٠ لسنة ٢٠١٦.

[٣٢]. قانون اصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل، المصدر الوقائع العراقية، العدد ٢٠٤، لسنة ١٩٧١

[٣٣]. جدير بالذكر ان العراق تراجع للمرتبة ١٢٩ عالميا و ١٧ عربيا عام ٢٠٢١ ضمن التصنيف العالمي للأمن السيبراني، والذي يطلقه مؤشر الأمن السيبراني العالمي (GCI) بصورة دورية، اذ كان في المركز ١٠٧ عالميا عام ٢٠١٨، وذلك ضمن مجموع ١٩٣ مرتبة عالمية، وهذا الانحدار مؤشر خطير يجب التنبه اليه

[34]. AbdulAmeer, S. A., Saleh, W. R., & Hussam, R. 2022, Cyber Security Readiness in Iraq: Role of the Human Rights Activists. Journal of Cybercrime, Vol 16 Issue 2, p3

[٣٥]. بسيوني، محمود شريف، ١٩٩٩، الجرائم ضد الانسانية في القانون الجنائي الدولي، ط ٢، القاهرة، ص ٨٩

[٣٦]. الأسدي، لينا محمد متعب، ٢٠١٢، مدى فاعلية أحكام القانون الجنائي في مكافحة جريمة المعلوماتية – دراسة مقارنة، رسالة ماجستير، كلية الحقوق – جامعة النهرين، العراق، ص ٤٠

[٣٧]. فيرحی، داود و ظهيری صمد، رهيافتهای موجود در تحليل پديده تروريسم، ١٣٨٧، فصلنامه سياست مجله دانشكده حقوق و علوم سياسی دور ٣٨٠، شماره ٣ ص ١٥۶

[٣٨]. موسسه توسعه حقوق فناوری اطلاعات برهان مشاوره حقوقی، ١٣٩۴، مفهوم شناسی جرايم رايانه ای جرايم اينترنتی و جرايم سايبری

[٣٩]. نيازپور، امير حسن، ١٣٨۴، پيشگيری از بزهكاری در قانون اساسی و لايحه پيشگيری از وقوع جرم، مجله حقوقی دادگستری شماره ۴۵، ص٨٩

[٤٠]. جلالی فراهانی امير حسين، ١٣٨٥، تروريسم سايبری نشريه حقوق اسلامی ١٣٨٥ سال سوم، شماره ١٠ زمستان، ص٤٥.

[٤١]. پرويزی، رضا، ١٣٩٢، جرمهای رايانه ای مجموعه مقاله های همايش بررسی جنبه های حقوقی فن آوری اطلاعات قوه قضائيه معاونت حقوقی و توسعه قضائی سلسبيل، ص٦٦.

[٤٢]. ليلا ميربد، صادق سليمی صابر نياورانی، سيد قاسم زمانی، ١٣٩٨، تروريسم سايبری نقض حقوق بشر و آزاديهای بنيادين، فصلنامه حقوق پزشكی ويژه نامه حقوق بشر و حقوق شهروندی، ص ٢٣٠.

[٤٣]. مريم شيريان نسل، زهرا نوری زاده خامنه، ١٤٠٢، تروريسم سايبری و نقش گروه تروريستی داعش در فضای مجازی، دانشگاه آزاد اسلامی واحد مراغه، ص٧١.

[٤٤]. عرب پور امير حمزه شادمان فر محمد رضا، ١٣٩٩، سياست جنايی اجرايی جمهوری اسلامی ايران در مقابله باتروريسم سايبری ١١(۴۵)، ص ٣۶۶.

[٤٥]. رضوی فرد، بهزاد، ١٣٩۶، سخن دبير علمی همايش چكيده مقالت همايش بين المللی ابعاد حقوقی – جرم شناختی تروريسم، تهران: انتشارات دانشگاه عالمه طباطبايی، چاپ اول صفحه ۵

[٤٦]. روح الله خيرانی آرانی، شهرام زرنشان، محمدهادی سلیمانیان، ۱۳۰۱، ارزیابی وضعیت ایران در ارتباط با مقررات بین المللی مرتبط با پول شویی، مجله پژوهشهای حقوقی دوره ۲۱ شماره ۴۹ بهار، ص ۵۰.

المصادر الأجنبية:

1.AbdulAmeer, S A, Saleh, W R, & Hussam, R. Cyber Security Readiness in Iraq: Role of the Human Rights Activists. Journal of Cybercrime, Vol 16 Issue 2, 2022.

Sources and references

First: Books and Publications

1.Ibrahim, Majid Morris. *Al-Irhab al-Zahira wa Ab'aduhu al-Nafsiyya* [Terrorism: The Phenomenon and Its Psychological Dimensions]. Dar Al-Farabi, Lebanon, 2005.
2.Al-Ashqar, Jbour Mona. *Al-Saybiraneya Hajis al-Asr* [Cybersecurity: The Obsession of the Age]. The Arab Center for Legal and Judicial Research, Beirut, 2016.
3.Bassiouni, M. Cherif. *Al-Jara'im Did al-Insaniyya fi al-Qanun al-Jina'i al-Dawli* [Crimes Against Humanity in International Criminal Law]. Cairo, 1999.
4.Bassiouni, M. Cherif. *Al-Jarima al-Munathama Abr al-Wataniyya wa Mahiyatuha wa Wasail Mukafahatiha Dawliyya wa Arabiyya* [Transnational Organized Crime: Its Nature and Means of International and Arab Combating]. Dar Al-Shorouk, Cairo.
5.Bawadi, Hassanein Al-Mohammadi. *Al-Irhab al-Iliktroni bayn al-Tajrim wa al-Mukafaha* [Cyber Terrorism Between Criminalization and Combating]. Dar Al-Fikr Al-Jame'i, Alexandria, 2005.
6.Al-Jubouri, Salim Abdullah. *Al-Himaya al-Qanuniyya li Ma'lumat Shabakat al-Internet* [Legal Protection of Internet Network Information]. Al-Halabi Legal Publications, Beirut, 2011.
7.Jaafar, Ali Abboud. *Jara'im Tiknulujiya al-Ma'lumat al-Haditha al-Waqi'a ala al-Ashkhas wa al-Hukuma* [Modern Information Technology Crimes Against Individuals and Government]. Zain Legal Publications, Beirut, 2013.
8.Salama, Mohamed Abdullah Abu Bakr. *Jara'im al-Computer wa al-Internet* [Computer and Internet Crimes]. Mua'ssat Al-Maaref, Alexandria, 2006.
9.Suleiman, Ahmed Ibrahim Mustafa. *Al-Irhab wa al-Jarima al-Munathama al-Tajrim wa Sabil al-Muwajaha* [Terrorism and Organized Crime: Criminalization and Means of Confrontation]. 2007.
10.Shawqi, Hesham. *Himaya wa Amn al-Ma'lumat ala al-Internet* [Protection and Security of Information on the Internet]. Dar Al-Kutub Al-Ilmiyya, Cairo, 2003.
11.Abdel Tawab, Moawad. *Al-Sariqa wa Ightisab al-Sanadat wa al-Tahdid* [Theft, Forgery of Documents and Threat]. Dar Al-Mashreq Al-Arabi, Cairo, 1988.
12.Abdel Sadeq, Adel. *Al-Irhab al-Iliktroni: Al-Quwa fi al-Alaqat al-Dawliyya, Namat Jadeed wa Tahadiyat Mukhtalifa* [Cyber Terrorism: Power in International Relations, A New Pattern and Different Challenges]. Al-Ahram Center for Political and Strategic Studies, Cairo, 2013.
13.Abdel Malik Bek, Gundi. *Al-Mawsu'ah al-Jina'iyya* [The Criminal Encyclopedia]. Egyptian Books House, Cairo, 1932.
14.Obeid, Raouf. *Jara'im al-I'tida' ala al-Ashkhas wa al-Amwal fi al-Qanun al-Masri* [Crimes of Assault Against Persons and Property in Egyptian Law]. Nahdet Misr Press, 1965.

15.Al-Ariymi, Mashhur Khait. *Al-Shar'iyya al-Dawliyya li Mukafahat al-Irhab* [The International Legitimacy of Combating Terrorism]. Dar Al-Thaqafa, Amman, 2009.
16.Garraud, René. *Mawsu'at Qanun al-Uqubat al-Aam wa al-Khas* [Encyclopedia of General and Special Criminal Law]. Al-Halabi Legal Publications, Beirut, 2003.
17.Fadel, Mohamed. *Al-Ta'awun al-Dawli fi Mukafahat al-Jarima* [International Cooperation in Combating Crime]. Damascus University Publications, Damascus, 1997.
18.El-Feki, Omar Eissa. *Al-Jara'im al-Ma'lumatiyya, Jara'im al-Hasib al-Ali wa al-Internet fi Misr wa al-Duwal al-Arabiyya* [Information Crimes, Computer and Internet Crimes in Egypt and Arab Countries]. Al-Maktab Al-Jame'i Al-Hadith, Alexandria, 2006.
19.Al-Feil, Ali Adnan. *Al-Jara'im al-Iliktroniyya, Dirasah Muqarana* [Electronic Crimes, A Comparative Study]. Zain Legal Publications, Beirut, 2011.
20.Matar, Essam Abdel Fattah Abdel Samie. *Al-Jarima al-Irhabiyya* [The Terrorist Crime]. New University House, Alexandria, 2005.
21.Al-Muqata', Mohamed Abdel Mohsen. *Himayat al-Hayat al-Khassa lil Afrad wa Damanatiha fi Muwajahat al-Hasib al-Ali* [Protection of Individuals' Private Life and its Guarantees in the Face of Computers]. That Al-Salasil, Kuwait, 1992.
22.Al-Mana'seh, Osama Ahmed, et al. *Jara'im al-Hasib al-Ali wa al-Internet* [Computer and Internet Crimes]. Wael Publishing House, Jordan, 2001.
23.Manshawy, Mohamed Abdullah. *Jara'im al-Internet min Manthur Shar'i wa Qanuni* [Internet Crimes from a Legal and Jurisprudential Perspective]. King Fahd University Press, Riyadh, 2011.
24.Clarke, Richard A., and Robert K. Knake. *Harb al-Fada' al-Iliktroni* [Cyber War: The Next Threat to National Security and What to Do About It]. Emirates Center for Strategic Studies and Research, Abu Dhabi, 2012.
25.Wanes, Omar Mohamed Abu Bakr. *Al-Jara'im al-Nashi'a an Istikhdam al-Internet* [Crimes Arising from the Use of the Internet]. Dar Al-Nahda Al-Arabiya, Cairo, 2004.
26.Youssef, Amir Farag. *Al-Jarima al-Iliktroniyya wa al-Ma'lumatiyya wa al-Juhud al-Dawliyya wa al-Mahalliyya li Mukafahat Jara'im al-Computer wa al-Internet* [Electronic and Information Crime and International and Local Efforts to Combat Computer and Internet Crimes]. Al-Wafa Legal Library, Egypt, 2011.

Second: Journals and Periodicals

1.Jalali Farahani, Amir Hossein. "Terrorism-e Sayberi" [Cyber Terrorism]. *Journal of Islamic Law*, Year 3, No. 10, 2006.
2.Ruhollah Khairani Arani, Shahram Zarneshan, Mohammad Hadi Soleimaniyan. "Arzyabi Vaz'iat Iran Dar Ertebat Ba Mogharrat-e Beyn Almelali Mortabet Ba Pool Shoyee" [Assessment of Iran's Situation Concerning International Regulations Related to Money Laundering]. *Journal of Legal Research*, Vol. 21, No. 49, 1922.
3.Firahi, Davood and Zahiri, Samad. "Rahyafthaye Mojoud Dar Tahlil-e Padideh Terrorism" [Existing Approaches in Analyzing the Phenomenon of Terrorism]. *Quarterly Politics, Journal of the Faculty of Law and Political Science*, No. 3, 2008.
4.Leila Mirbad, Sadegh Soleimi Saber Niavarani, Seyed Ghasem Zamani. "Terrorism-e Sayberi: Naghz-e Hoquq-e Bashar va Azadiha-ye Bonyadin" [Cyber Terrorism:

Violation of Human Rights and Fundamental Freedoms]. *Medical Law Quarterly, Special Issue on Human Rights and Citizenship Rights*, 2019.
5.Niazpour, Amir Hassan. "Pishgiri Az Bazhkari Dar Ghanun-e Asasi va Layeheh Pishgiri Az Voghu-e Jorm" [Crime Prevention in the Constitution and the Crime Prevention Bill]. *Judiciary Law Journal*, No. 45, 2005.

Third: Theses and Dissertations

1.Al-Asadi, Lina Mohammed Muteb. *Mada Fa'aliyat Ahkam al-Qanun al-Jina'i fi Mukafahat Jarimat al-Ma'lumatiyya - Dirasah Muqaranah* [The Effectiveness of Criminal Law Provisions in Combating Cybercrime - A Comparative Study]. Master's Thesis, Al-Nahrain University, Iraq, 2012.
2.Abdullah, Ahmed Kailan. *Hujiyat al-Muharrarat al-Mustakhraja min al-Hasib fi al-Ithbat al-Jina'i* [The Admissibility of Computer-Generated Documents in Criminal Evidence]. Doctoral Dissertation, University of Baghdad, 2007.

Fourth: Conferences and Research Papers

1.Parvizi, Reza. "Jorm-haye Rayane-i" [Computer Crimes]. *Proceedings of the Conference on Legal Aspects of Information Technology, Judiciary*, 2013.
2.Razavi Fard, Behzad. "Sokhan-e Dabir-e Elmi Hamayesh; Chekideh Maqalat Hamayesh-e Beyn Almelali Ab'ad-e Hoquqi - Jorm Shenakhti Terrorisim" [Speech of the Scientific Secretary of the Conference; Abstracts of the International Conference on Legal-Criminological Dimensions of Terrorism]. Allameh Tabataba'i University Publications, 2017.
3.Arab Pour, Amir Hamzeh; Shadman Far, Mohammad Reza. "Siyasat-e Jaza-i Ejra-i Jomhouri-e Islami Iran Dar Moqabeleh Ba Terrorism-e Sayberi" [The Executive Criminal Policy of the Islamic Republic of Iran in Confronting Cyber Terrorism]. (11)(45), 2020.
4.Maryam Shiriyan Nasel, Zahra Nouri Zadeh Khameneh. "Terrorism-e Sayberi va Naghsh-e Goruh-e Terroristi Daesh Dar Fazaye Majazi" [Cyber Terrorism and the Role of the ISIS Terrorist Group in Cyberspace]. Islamic Azad University, Maragheh Branch, 2023.
5.Borhan Institute for Development of Information Technology Law & Legal Consultancy. "Mafhum Shenasi Jara'im-e Rayane-i, Jara'im-e Interneti va Jara'im-e Sayberi" [Conceptology of Computer Crimes, Internet Crimes and Cybercrimes]. 2015.

Fifth: Laws and Legislation

1.Code of Criminal Procedure No. 23 of 1971, as amended.
2.Anti-Terrorism Law No. 13 of 2005.
3.Counter-Terrorism Agency Law No. 31 of 2016.

Foreign Sources:

1.AbdulAmeer, S A, Saleh, W R, & Hussam, R. Cyber Security Readiness in Iraq: Role of the Human Rights Activists. *Journal of Cybercrime*, Vol 16 Issue 2, 2022.