Journal Of the Iraqia University (73-10) August (2025)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

الإجراءات القانونية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي

البروفيسور في القانون الجنائي و علم الاجرام اب والفتح خالقي
جامعه قم الحكومية /كلية القانون/قسم الجنائي و علم الاجرام المؤلف المسؤول
طالب الدكتوراه حيدر احمد خضير
جامعه قم الحكومية /كلية القانون/قسم الجنائي و علم الاجرام

Legal measures to combat terrorist crimes in cyberspace

Professor of Criminal Law and Criminology Abolfath Khaleghi
Qom University / Faculty of Law / Department of Criminal law and Criminology
Responsible Author
ab-khaleghi@qom.ac.ir
PhD student Haider Ahmed Khadir
Qom University / Faculty of Law / Department of Criminal law and Criminology
haider811111@gmail.com

المستخلص:

الإجراءات القانونية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي تتطلب مزيجاً من التشريعات القانونية، التعاون الدولي، واستخدام التكنولوجيا الحديثة. تركز هذه الإجراءات على تطوير قوانين لمكافحة التطرف والتحريض على الإرهاب عبر الإنترنت، وكذلك التعاون بين الدول لمشاركة المعلومات حول الأنشطة الإرهابية. تتضمن هذه الإجراءات أيضاً إنشاء هيئات مختصة لمراقبة المحتوى المتطرف على منصات التواصل الاجتماعي واستخدام الذكاء الاصطناعي والتحليل البياني لتحديد الأنشطة المشبوهة.**الكلمات المفتاحية** :الفضاء الافتراضي، الجرائم الإرهابية، التعاون الدولي، التطرف الإلكتروني، التحريض على الإرهاب، مكافحة الإرهاب، الأمن السيبراني.

Abstract:

Legal measures to combat terrorist crimes in cyberspace require a combination of legislation, international cooperation, and the use of modern technology. These measures focus on developing laws to combat extremism and incitement to terrorism online, as well as cooperation between countries to share information about terrorist activities. These measures also include the establishment of specialized bodies to monitor extremist content on social media platforms and the use of artificial intelligence and data analysis to identify suspicious activities.Keywords: cyberspace, terrorist crimes, international cooperation, online extremism, incitement to terrorism, counterterrorism, cybersecurity.

المقدمة

لقد أصبح الفضاء الافتراضي جزءاً أساسياً من حياتنا اليومية، حيث يشهد تطوراً سريعاً في مختلف المجالات التقنية والاجتماعية. ومع هذا التقدم الكبير، ظهرت العديد من التحديات المتعلقة بالأمن السيبراني، وأصبحت الجرائم الإرهابية الإلكترونية من أبرز القضايا التي تهدد الاستقرار العالمي. فالإرهاب اليوم لم يعد مقتصرًا على الهجمات التقليدية، بل انتقل إلى الفضاء الإلكتروني حيث يتم استخدام الإنترنت في نشر الفكر المتطرف، تحريض الأفراد على ارتكاب الأعمال الإرهابية، وتمويل الأنشطة غير القانونية.وقد أصبحت الجرائم الإرهابية في الفضاء الافتراضي

تمثل تهديداً غير محدود من حيث المكان والزمان، مما يتطلب استجابة قانونية فعّالة تتسم بالمرونة والسرعة. ولذلك، تطلب الأمر تحديث وتطوير التشريعات القانونية على مستوى الدول وتوسيع نطاق التعاون الدولي لمواجهة هذا التحدي بشكل جماعي.تهدف الإجراءات القانونية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي إلى منع انتشار الفكر المتطرف، وتعقب الأنشطة الإرهابية على الإنترنت، وملاحقة الأشخاص الذين يستغلون الفضاء الرقمي في ارتكاب الجرائم. يشمل ذلك أيضاً تنسيق الجهود بين الدول والمنظمات الدولية، وتبادل المعلومات، بالإضافة إلى استخدام التقنيات الحديثة مثل الذكاء الاصطناعي والتحليل البياني في ملاحقة النشاطات المشبوهة والكشف عنها في الوقت المناسب. علاوة على ذلك، تتضمن هذه الإجراءات تدريب وتثقيف المجتمع حول مخاطر الإنترنت والسبل الأمثل لاستخدامه بشكل آمن.في هذه السياق، تمثل القوانين الوطنية والتشريعات الدولية والتقنيات الحديثة أدوات أساسية في مكافحة الجرائم الإرهابية في الفضاء الافتراضي، حيث تساهم في تعزيز الأمن السيبراني، وتقليل التهديدات التي تشكلها هذه الجرائم على المجتمعات، وتؤمن حماية الأفراد من مخاطر التطرف والإرهاب الرقمي.

أهمية البحث:

تتمثل أهمية هذا البحث في دراسة الإجراءات القانونية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي، حيث يعد هذا الموضوع من أكثر القضايا إلحاحًا في العصر الرقمي الذي نعيشه. مع تطور وسائل الاتصال الحديثة واستخدام الإنترنت بشكل موسع، أصبح الفضاء الإلكتروني بيئة خصبة للجماعات الإرهابية للتخطيط، التحريض، وتمويل الأنشطة الإرهابية. لذلك، فإن هذا البحث يسلط الضوء على أهمية تحديث وتطوير التشريعات الوطنية والدولية لمواكبة التحديات التي تطرأ بسبب الاستخدام غير المشروع للإنترنت في العمليات الإرهابية.

مشكلة البحث:

تكمن مشكلة البحث في التحديات القانونية والتنظيمية التي تواجه الدول في مكافحة الجرائم الإرهابية عبر الإنترنت. حيث لا تزال بعض التشريعات الوطنية لا تتواكب مع سرعة التطور التكنولوجي، مما يجعل من الصعب ملاحقة الأنشطة الإرهابية التي تتم عبر الإنترنت بشكل فعال. فضلاً عن ذلك، فإن الفضاء الافتراضي عابر للحدود، وهو ما يعقد التنسيق بين الدول لمكافحة هذه الجرائم.

منهج البحث:

يعتمد هذا البحث على المنهج التحليلي الوصفي، حيث سيتم دراسة التشريعات والقوانين الوطنية والدولية المتعلقة بمكافحة الإرهاب في الفضاء الافتراضي، وتحليل مدى فعاليتها في التصدي لهذه الجرائم. سيتم تحليل مختلف القوانين التي تعتمدها الدول في مواجهة الجرائم الإرهابية الإلكترونية، وتحديد جوانب القوة والضعف فيها.

كما سيتم استخدام المنهج المقارن لمقارنة التشريعات القانونية في دول مختلفة وتحديد أساليب وأساليب التعاون الدولي في مكافحة الجرائم الإرهابية عبر الإنترنت. سيشمل البحث أيضاً دراسة الأدوات والتقنيات الحديثة مثل الذكاء الاصطناعي والتحليل البياني التي تساهم في مراقبة الأنشطة الإرهابية.

هيكلية البحث:

لمعالجة موضوع البحث قمنا بتقسيمه الى مبحثين تناولنا ماهية الجرائم الإرهابية في الفضاء الافتراضي في المبحث الأول ومن ثم انتقلنا للحديث عن الاجراءات الجنائية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانونين العراقي والايراني في المبحث الثاني.

المبحث الأول ماهية الجرائم الإرهابية في الفضاء الافتراضي

في ظل التطور التكنولوجي السريع وانتشار الإنترنت في جميع أنحاء العالم، أصبح الفضاء الافتراضي يشكل بيئة خصبة للأعمال الإرهابية، حيث يُستخدم من قبل الجماعات الإرهابية لعدة أغراض مثل التحريض، التخطيط، والتواصل، فضلاً عن تجنيد الأفراد، وتمويل العمليات الإرهابية. في هذا السياق، أصبح من الضروري فهم ماهية الجرائم الإرهابية التي ترتكب في الفضاء الإلكتروني، وكذلك التعرف على الأركان القانونية لهذه الجرائم.الفضاء الافتراضي، الذي يضم منصات التواصل الاجتماعي، المنتديات الإلكترونية، ومحركات البحث، قد تحوّل إلى أداة رئيسية بالنسبة للإرهابيين في تنفيذ أنشطتهم التخريبية. من خلال الإنترنت، يستطيع الإرهابيون نشر أفكارهم المتطرفة، وتحريض الأفراد على الانضمام إلى مجموعات متطرفة، وتبادل المعلومات حول كيفية تصنيع الأسلحة، أو حتى تنسيق الهجمات.الجرائم الإرهابية في الفضاء الافتراضي تشمل مجموعة من الأنشطة غير القانونية التي تُرتكب باستخدام الإنترنت والتكنولوجيا الحديثة. وتشمل هذه الأنشطة التحريض على العنف والإرهاب، نشر المحتوى المتطرف، تجنيد الأشخاص لصالح الجماعات الإرهابية، وتسهيل العمليات الإرهابية من خلال الأنظمة الرقمية.

المطلب الأول مفهوم الجرائم الإرهابية

تُعد الجرائم الإرهابية من أخطر الظواهر التي تواجه المجتمعات الحديثة، لما لها من تأثيرات سلبية عميقة على الأمن والاستقرار والسلام الاجتماعي. وتختلف التعريفات القانونية والفقهية لهذه الجرائم بحسب السياقات الوطنية والدولية، لكنها تتفق على أن الإرهاب يشمل استخدام العنف أو التهديد به لتحقيق أهداف سياسية أو دينية أو أيديولوجية عبر إلحاق الضرر بالأفراد أو المنشآت العامة. ومن هنا تأتي أهمية فهم مفهوم الجرائم الإرهابية بدقة، لا سيما في ظل التطور التكنولوجي وانتشار الفضاء الافتراضي الذي أصبح ملاذاً جديداً لتنفيذ هذه الجرائم، مما يستدعي دراسة متعمقة لمضامينها وأبعادها القانونية.وعلى هذا فإن هذا المطلب ينقسم إلى عدة فروع، وسنتناولها حسب التقسيم التالي:

الفرع الأول: تعريف الجرائم الإرهابية لغة

لم تتناول معاجم اللغة العربية القديمة كلمة الإرهاب لأنها كلمة حديثة الاستعمال ولكنها عرفت كلمة الإرهاب كونها مشتقة من الفعل رهب ويقال رهب فلاناً أَي خَوَفَهُ وفَزَّعَه، ورهَب رهبه ورهباً – خافه، والرهبة الخوف[١].والرهباء اسم من الرهب نقول: الرهباء من الله والرغباء اليه، وفي حديث الدعاء: رغبة ورهبة اليك[٢]. والراهب المتعبد مصدره الرهبه والترهب تعنى التعبد، ويقال ترهب فلان اي تعبد في صومعته.[٣]ومن المجاز ارهب الابل عن الحوض ذادها، وارهب عنه الناس بأسه ونجدته[٤]، والرهب هو الناقة المهزوله، والرهاب هو عظم في الصدر مشرف على البطن مثل اللسان[٥].والارهاب بالفتح ما لا يصيد من الطير كالبغاث، ومن المجاز قولهم لم أرهب اي لم أستر[٦]، اما الفعل المزيد بالتاء وهو ترهب حيث يستعمل الفعل أيضاً بمعنى توعد اذا كان متعديا فيقال: ترهب فلان أي توعده[٧].وتجدر الاشارة أن معاجم اللغة العربية كان القاسم المشترك فيما يتعلق بالفعل (رهب) هو الخوف والرعب والفزع، وأن الإرهاب رعب تحدثه أعمال العنف[٨]، مثل القاء المتفجرات أو القتل أو التخريب بفرض اقامة سلطة او تقويض سلطة أخرى، والإرهابيون وصف يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق اهدافهم السياسية.[٩]اما كلمة الإرهاب في القرآن الكريم فقد استعملت بصيغ مختلفة وفي أكثر من معنى لبعض سور القرآن الكريم فمنها معنى الخشية وتقوى الله كما في قوله تعالى (يابني إِسْرَائِيلَ اذْكُرُوا نِعْمَتِيَ الَّتِي أَنْعَمْتُ عَلَيْكُمْ وَأَوْفُوا بِعَهْدِي أُوفِ بِعَهْدِكُمْ وَإِيَّايَ فَارْهَبُونَ)[١٠].

الفرع الثاني: تعريف الجرائم الإرهابية اصطلاحا

لقد تعددت تعاريف الإرهاب واختلفت في وضع تعريف محدد وواضح له؛ وذلك لاختلاف الايديولوجيات والفلسفات الفكرية في دول العالم وذلك لاختلاف العقائد الدينية بين المجتمعات البشرية فكل فلسفة وفكر معين يضع تعريفاً خاصاً للإرهاب؛ وذلك حسب ما يخدم مصالحه من جميع الجوانب والاتجاهات سواء أكانت سياسية أم اجتماعية أم اقتصادية أم فكرية وحتى الدينية منها، فهناك من يصنف بعض الأعمال التي تمارس على المستوى الفردي، أو الاجتماعي إرهاباً وهناك من ينظر اليها على أنها أعمال مشروعة من حق الفرد، أو المجتمع أن يقوم بها ولا يصنفها إرهاباً، وأن دول العالم مهددة بخطر الإرهاب وبخاصة الفكري لذلك حاول الكثير من الفقهاء وأساتذة القانون والعلوم السياسية والأمنية وكذلك المنظمون على الاتفاقيات الدولية ان يضعوا تعريفا محدداً للإهاب فضلاً عن محاولة بعض المنظمات الدولية والاقليمية لكن هذه الجهود لم تنجح في وضع تعريف موحد له.[١١]هذا وقد عرف جانب الفقه الإرهاب بأنه (بث الرعب الذي يثير الخوف والفزع، أي الطريقة التي تحاول بها جماعة منظمة أو حزب أن يحقق اهدافه عن طريق استخدام العنف، وتوجه الأعمال الإرهابية ضد الأشخاص، سواء أكانوا أفراد أم ممثلين للسلطة، ممن يعارضون أهداف هذه الجماعة).[١٢]ويعرف بأنه الاستخدام غير المشروع للعنف، أو التهديد به بواسطة مجموعة أو دولة ضد فرد أو جماعة أو دولة ينتج عنه رعب يعرض للخطر أرواحا بشرية أو يهدر حريات أساسية، ويكون الغرض منه الضغط على جماعة أو دولة تغير سلوكها تجاه موضوع معين.[١٣]وعرف ايضا بأنه استراتيجية عنف محرم دولياً، تحفزها بواعث عقائدية ايديولوجيا ترمي الى احداث الرعب داخل شريحة خاصة من مجتمع معين من أجل الوصول الى سلطه أو مصلحة، بغض النظر عما اذا كان مقترفو العنف يعملون لمصلحتهم الشخصي أو لمصلحة أحدى الدول.[١٤]وعرف الإرهاب كذلك بأنه نتاج العنف المتطرف الذي يرتكب من أجل الوصول إلى أهداف سياسية معينة، يضحي من أجلها بكافة المعتقدات الانسانية والأخلاقية.[١٥]أما في المعاهدات والمواثيق والتقارير الدولية فقد عرف الإرهاب في المادة الرابعة والعشرون /الفقرة الثانية في التقرير الثالث عشر للجنة القانون الدولي الصادر عام ١٩٩٥ بما يأتي: (أن الأعمال ادناه تعد من الإرهاب الدولي: ممارسة أعمال العنف، أو تنظيمها، أو توجيهها أو تسهيلها، أو توفير الدعم المالي لها، أو الحث عليها، أو أدارة تلك الموجهة ضد دولة أخرى، بحيث يستهدف منها الاشخاص أو الأموال، وتتصف بإثارة الرعب والخوف في الأفكار أو التنظيمات أو الفئات أو الرأي العام بغية أجبار الدولة المذكورة على منح بعض الامتيازات أو القيام بعمل ما).[١٦]وفي ضوء التعريفات الاصطلاحية المتعددة، فإن الإرهاب هو ممارسة مجرمة قانوناً على الصعيد الداخلي،

أو الدولي كونها تحفز بواعث ايديولوجيا وعقائدية لدى بعض الافراد في مجتمع معين لتستهدف شخص أو جماعة أو طائفة أو قومية والتي من شأنها أن تمس أمن المجتمعات البشرية بمختلف أعراقها، معتقداتها وديانتها عن طريق نشر الخوف والرعب فيها لتحقيق أهداف وغايات غير مشروعة فتعريف الإرهاب هو ارتكاب أعمال محددة بقصد التأثير على سياسة جمهورية إيران الإسلامية أو المنظمات الدولية الممثلة على أراضيها، مثل أعمال تخريب الممتلكات والمرافق العامة وغير الحكومية، وإلحاق أضرار جسيمة بالبيئة، كتسميم المياه وإشعال الحرائق في الغابات؛ والإنتاج غير المشروع للسموم والعناصر والمواد النووية والمواد الكيميائية والميكروبية والبيولوجية، وحيازتها ونقلها وتخزينها وتطويرها أو تكديسها، وسرقتها، وحيازتها بالاحتيال والاتجار بها؛ والإنتاج غير المشروع للمتفجرات والأسلحة والذخائر من هذا النوع، وشرائها وبيعها واستخدامها والاتجار بها. وفيما يتعلق بهذا التعريف، تجدر الإشارة إلى أن الأعمال المذكورة فيه تُعتبر أعمالًا إرهابية إذا نُفذت بقصد التأثير على سياسة جمهورية إيران الإسلامية أو المنظمات الدولية الممثلة على أراضيها، وإذا لم تكن هناك نية لذلك، فلا تُعتبر أعمالًا إرهابية. ويشمل التعريف الثالث الأعمال التي تُعتبر أعمالًا إرهابية بغض النظر عن نية الجاني والنتيجة المترتبة عليها. وتشمل هذه الأفعال الأفعال التي تشكل خطرًا على سلامة الطائرات أو الطيران، والاستيلاء على طائرة أثناء طيرانها وممارسة السيطرة غير القانونية عليها، وارتكاب أعمال عنف ضد راكب أو ركاب وطاقم طائرة، والأفعال التي تشكل خطرًا على الممتلكات على متن طائرة أثناء طيرانها، والإنتاج غير المشروع أو الإنتاج أو الحيازة أو الاستحواذ أو النقل أو التخزين أو التطوير أو التراكم أو السرقة أو الاستحواذ الاحتيالي والاتجار بالسموم والعناصر والمواد النووية بكميات غير مبررة للأغراض الطبية والعلمية والسلمية، وغيرها من الحالات المشار إليها في المادة (١). لذلك، فإن الفرق بين الأفعال المذكورة في التعريف الثاني والأفعال المذكورة في التعريف الثالث هو أن الأفعال المذكورة في التعريف الثاني تعتبر إرهابية إذا كان مرتكبها ينوي التأثير على سياسة جمهورية إيران الإسلامية أو المنظمات الدولية الممثلة في أراضيها، والأفعال التي يشملها التعريف الثالث هي أفعال تعتبر أعمالًا إرهابية بغض النظر عن نية مرتكبها والنتيجة المترتبة عليها.[١٧]وقد عرف بعض الفقه الإرهاب في الفضاء الافتراضيبأنه ارتباط الأعمال الإرهابية بالتطورات الحديثة التي صاحبت ظهور الحاسوب والإنترنت، إذ لم تعد أفعال الإرهاب مقتصرة على جانبها التقليدي في التفجير والتفخيخ والإتلاف والقتل إنما أصبح من الأفعال التي ترتكب عن طريق أجهزة الحاسوب وشبكة الإنترنت حتى بات الإرهابي يجلس في قارة من الكرة الأرضية خلف حاسوب وبضغطة زر واحدة يقوم بعمل إرهابي ينفذه في بقارة أخرى.[١٨] وقد عرفه بعض الفقهاء بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادرة عن الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني أو ان يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له[١٩]. وقد عرفته منظمة الأمم المتحدة في تشرين الأول/ أكتوبر (٢٠١٢) بأنه استخدام الإنترنت لنشر أعمال إرهابية.[٢٠]ويتضمن التعريف الرابع للتعريف السابق الأفعال التي تُعتبر جرائم إرهابية بموجب القوانين والاتفاقيات المحلية، والتي انضمت إليها جمهورية إيران الإسلامية أيضًا. وكما ذُكر، لا يوجد حاليًا أي قانون محلي آخر يُعرّف الفعل بأنه جريمة إرهابية، وفيما يتعلق بالمعاهدات الدولية، تجدر الإشارة إلى أن معظم الأفعال المدرجة في التعريفين الثاني والثالث هي أفعال تُعتبر جرائم إرهابية بموجب الاتفاقيات الدولية، والتي انضمت إليها جمهورية إيران الإسلامية أيضًا. لذلك، تُعتبر الأفعال المذكورة أعلاه إرهابية بناءً على كل من التعريفين الثاني والثالث والتعريف الرابع.[٢١]لم يتطرق قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، إلى تعريف الإرهاب بوصفه جريمة مستقلة، ولم يحدده بتعريف مانع جامع، مما يؤثر في التشريع، إلى أن عالج المشرع العراقي بإصداره قانون مكافحة الإرهاب ذي العدد ١٣ لسنة ٢٠٠٥، المعالجة الأعمال الإرهابية وإخضاعها للقانون، إذ عرف الجريمة الإرهابية في المادة (الأولى) بأنها " كل فعل إجرامي يقوم به فرد أو جماعة منظمة، استهدف فردا أو مجموعة أفراد أو جماعات أو مؤسسات رسمية أو غير رسمية ، أو أوقع الاضرار بالممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو إدخال الرعب والخوف والفزع بين الناس أو إثارة الفوضى تحقيقا لغايات إرهابية".ويُذكر في متابعة هذا التعريف نقطة مهمة تُميز قانون مكافحة تمويل الإرهاب في إيران عن القانون الدولي والقوانين الأخرى في هذا المجال. تنص الملاحظة ٢ من المادة (١) من القانون على أن الأفعال التي يقوم بها الأفراد أو الدول أو الجماعات أو منظمات التحرير لمواجهة أمور مثل الهيمنة الأجنبية والاحتلال والاستعمار والعنصرية ليست أمثلة على الأعمال الإرهابية التي هي موضوع هذا القانون. تقع مسؤولية تحديد الأمثلة والمجموعات التي تغطيها هذه المذكرة على عاتق المجلس الأعلى للأمن القومي. وبناءً على ذلك، فإن الدافع وثيق الصلة بمفهوم الإرهاب وتمويله، وإذا نُفذ عمل يندرج تحت تعريف الإرهاب ولكن تم تنفيذه بالدوافع المذكورة في هذه المذكرة، فلن يُعتبر عملاً إرهابيًا، ولن يُعتبر تمويله تمويلًا للإرهاب. ومن النقاط المثيرة للاهتمام التي تلفت الانتباه هنا أن المجلس الأعلى للأمن القومي ملزم بإدراج وإعلان المنظمات والجماعات التي تعزز الحرية. هذا بينما يحدث الاتجاه المعاكس عادةً في دول أخرى، حيث لا تحدد المؤسسات المختصة المنظمات والمؤسسات الإرهابية وتعلن عنها، ويبدو هذا النهج أصح؛ لأن المبدأ هو أنها ليست إرهابية، وإذا اعتُبرت منظمة أو جماعة

منظمة إرهابية، فيجب الإعلان عن اسمها، بدلاً من أسماء الجماعات والمنظمات غير الإرهابية. مادة نادرة أخرى في قانون إيران لمكافحة تمويل الإرهاب هي المادة (٣)[٢٢]. وفقًا لهذه المادة، إذا كان شخصٌ على علمٍ بالجرائم المشمولة بها ولم يُبلغ السلطات الإدارية أو سلطات إنفاذ القانون أو السلطات الأمنية أو القضائية المختصة بها في أسرع وقت ممكن، فإنه يُعدّ مذنبًا ويُحكم عليه بعقوبة تعزير من الدرجة السابعة. تُعد هذه المادة نادرة، وربما غير مسبوقة، لأنها تُعتبر عامة الناس، وليس فقط موظفي القضاء، مسؤولين عن الإبلاغ عن الجرائم التي ينوي آخرون ارتكابها. من حيث المبدأ، تقع مسؤولية الكشف عن الجرائم على عاتق الموظفين والنظام القضائي، وليس على عامة الناس، ومجرد الصمت عن جريمة ارتكبها شخصٌ آخر أو على وشك ارتكابها لا يُعدّ جريمة.لذلك تعد جريمة الإرهاب باستخدام الوسائل الإلكترونية من الجرائم الخطيرة كونها تهدف إلى الإخلال بالأمن والنظام العام في المجتمع، ولضمان تفادي النتائج السلبية التي تتركها هذه الجريمة أفردت العديد من التشريعات في الدول والقوانين الخاصة بمعالجتها ومن ثم استقلت هذه القوانين استقلالا تاما في القواعد العامة غير أن هذا الاستقلال لا يغني عن الرجوع إلى القواعد العامة كلما اقتضت الحاجة لسد النقص وإزالة الغموض والعمل كنظام قانوني متكامل.[٢٣]لقد أصبح الإرهاب ظاهرة إجرامية خطيرة ومدمرة لأنه يهدف إلى مهاجمة المجتمعات البشرية وينعكس هذا الخطر بشكل واضح في تفكير الإرهابين اللافت للنظر لأنهم يعتقدون أن تفكيرهم صحيح بينما باقي أفكار الإنسانية خاطئة، لذلك يبذلون قصارى جهدهم لنشر أيديولوجيتهم ومعتقداتهم، حتى لو تطلب الأمر ارتكاب أعمال إجرامية قاسية، لذا فإن أهم شيء هو نشر المعتقدات، لأنهم غالبا كما يزعمون يمتلكون مشروع دولة متكامل سياسيا واقتصاديا واجتماعيا وثقافيا[٢٤]، بما أن الجريمة لها نفس الخصائص وقد ارتكبها الإنسان الأول، فلا شك أن وسائل تنفيذها وارتكابها تختلف وتتطور بمرور الوقت، ومع ظهور تكنولوجيا المعلومات بجميع أنواعها وبفضل الخدمات الواضحة والرائعة التي تقدمها هذه التقنية الحديثة، حاول الإرهابيون استغلالها، لكنهم أضروا بالمجتمع، وبذلك أصبح الإنترنت أفضل وسيلة لنشر أفكارهم ومعتقداتهم والترويج لها، واستقطاب عناصر جديدة إلى صفوفهم وجمع التبرعات لهم، وحتى التخطيط لجرائمهم الإرهابية، ثم ظهر مصطلح "الإرهاب في الفضاء الافتراضي" أو "الإرهاب المعلوماتي"[٢٥] وبدأت هذه الجريمة تهدد الدول والأفراد. في الواقع أن هذه التقسيمات لجرائم الإرهاب لا تخرج عن كونها تقسيمات لفظية فهي من حيث التقسيم لا تختلف عن جرائم القانون العام، فالجرائم الإرهابية هي جرائم قانون عام يضفي عليها وصف الإرهاب بسبب جسامة الإخلال بالمصالح القانونية المحمية بموجب القانون، لذلك كان لزاما على المجتمع الدولي أن يشرع أنظمة عقابية وإجرائية مشددة لمواجهتها.إن تحديد طبيعة جريمة تقنية المعلومات الحديثة يعني التمييز بين جريمة التكنولوجيا الحديثة عن الجريمة، والجريمة بشكل عام هي فعل غير مشروع يرتكب كعقوبة يعاقب عليها القانون او تدبير احترازي، فهذا يعتبر سلوكا محظورا بالنسبة للمجتمع، لأنه يهدد القدرة على صيانة نظامها، ولا يمكن أن يوجد نظام بدون قواعد ضد الأنشطة الخبيثة والمؤذية والأجهزة لفرض تلك القواعد، وتشكل هذه القواعد القانون الجنائي[٢٦]، ومع انتشار التقنيات الحديثة وانتشار أجهزة الكمبيوتر والإنترنت واعتماد العالم التزايد عليها، لم يعد الإرهابي بحاجة إلى جهاز كمبيوتر لتأمين اتصاله بالإنترنت لارتكاب أعمال إرهابية فأصبحت جريمة الإرهاب في الفضاء الافتراضي تهديدا للعالم أجمع والخطر يكمن في سهولة استخدامه إذ يستخدمها في المنزل أو في المكتب أو في غرفته بالفندق بعيدا عن أنظار السلطات والمجتمع.الإرهاب في الفضاء الافتراضي ليس نتيجة لحظة أو حادث ولكنه نشأ مع ظهور التكنولوجيا وخاصة تكنولوجيا الإنترنت، وقد نشأ مع ظهور الفضاء السيبراني ويحتوي على معلومات وبيانات حول البلدان والأفراد والمنظمات في شكل رقمي، فأصبح الفضاء السيبراني أرضا خصبة للعمليات الإرهابية الحديثة ولا شك في أن التقدم التكنولوجي يفوق محاولات الاستخدام القانوني[٢٧]، فإن ما يميز الإرهاب في الفضاء الافتراضي عن الإرهاب التقليدي هي الطريقة العصرية المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي هيئتها تقنية عصر المعلومات إذ تستخدم هذه الجماعات في الإرهاب التقليدي الوسائل التقليدية كالضرب والاغتيال، أما في الإرهاب في الفضاء الافتراضي فتستخدم الوسائل العلمية والتقنية المتطورة إذ تقوم باستغلال وسائل الاتصالات وشبكة المعلومات. كما تواجه بعض الدول صعوبات بالمراقبة على الإنترنت في حالات ارتكاب الأعمال الإرهابية وما ينشر فيه، وهذا ما جعل الإنترنت مقرا للإرهابيين، حيث أن الهدف من القيام بهذه العمليات هو زعزعة الأمن والإخلال بالنظام العام والاستيلاء على الأموال العامة والخاصة وإلحاق الضرر بالمرافق العامة والاتصالات والمواصلات[٢٨]، إن الأنظمة الإلكترونية والبنية التحتية المعلوماتية تعد هي هدف الإرهابيين، إذ يشير الإرهاب في الفضاء الافتراضي عنصرين أساسيين هما (الفضاء الافتراضي، والعالم الافتراضي)، وهو المكان الذي تعمل به أجهزة وبرامج الحاسوب كما تنتقل فيه المعلومات في الفضاء الافتراضي والإرهاب، وأصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية.[٢٩]

المطلب الثاني مفهوم الفضاء الافتراضي

يُعتبر الفضاء الافتراضي من أبرز الظواهر التكنولوجية الحديثة التي غيّرت مجرى الحياة الاجتماعية والاقتصادية والسياسية في العالم، حيث يشير إلى البيئة الرقمية التي تتشكل عبر شبكات الإنترنت والتقنيات في الفضاء الافتراضي، والتي تتيح تفاعل الأفراد والمؤسسات بشكل مباشر وفوري دون الحاجة إلى التواجد الجسدي. ويتميز هذا الفضاء بمرونته وسرعته وانتشاره الواسع، مما جعله منصة مركزية للأعمال والتواصل والترفيه، لكنه في الوقت ذاته أصبح ساحة لتحديات قانونية وأمنية متعددة، خصوصاً فيما يتعلق بانتشار الجرائم في الفضاء الافتراضي والإرهابية التي تستغل هذه البيئة لتحقيق أهدافها. لذا، فإن فهم مفهوم الفضاء الافتراضي يمثل خطوة أساسية لدراسة الجرائم الإرهابية التي تنشأ أو تستهدف هذا المجال.الفرع الأول: تعريف الفضاء الافتراضي لغة ورد في "لسان العرب" في مادة (فضا) أن الفضاء هو الموضع الواسع من الأرض، ويُقال: فَضَا يَفْضُو فُضُوًّا، فهو فاضٍ، أي اتّسع المكان. ويُقال: فَضِيَ المكان وأَفْضَى، أي اتّسع وانبسط، ويُطلق الفضاء على الساحة أو الموضع الخالي المتسع من الأرض. وجاء في حديث معاذ في عذاب القبر: "ضربه بمرضافة وسط رأسه حتى يفضي كل شيء منه"، أي حتى يصير جسده كأنّه فضاء مفتوح. ويقال "أفضيت" بمعنى خرجت إلى الأرض الواسعة أو المكان الفسيح.[٣٠]الافتراض في اللغة مشتق من مادة "الفرض"، التي تدل على القطع أو الشق في الشيء[٣١]، كما تُستخدم أيضًا للدلالة على الإلزام والتحديد. فيُقال: "فرضت الشيء" أي قطعته أو ألزمته، و"فرضته لكثير" أي أوجبته عليه[٣٢]. وقد يُستعمل الفرض كذلك بمعنى العطاء غير المرتبط بشرط، كما في قولهم: "ما أعطيت من غير فرض"، أي من غير إلزام سابق. أما في الاستخدام الشرعي، فإن الفرض يُطلق على ما أوجبه الله تعالى على عباده، وسُمي فرضًا لما يتسم به من تحديد دقيق ومعالم واضحة وحدود ثابتة، ويُقال: "فرضه عليه" أي ألزمه به وفقًا لأوامر الله ونواهيه. [٣٣]يُستخدم مصطلح "الفرض" في اللغة بعدة معانٍ، منها التقدير والتحديد، فيُقال: "فُرض له في العطاء" أي خُصص له نصيب معين. كما يُستعمل بمعنى الإلزام، كأن يُقال: "القاضي فريضة" أي أوجب الحكم وقدّره. وفي وصف الحيوان، يُقال: "فَرَضَ الحيوان" أي بلغ سنًّا متقدمة وأصبح كبيرًا، ويُطلق عليه "فارض" في حال كونه مذكرًا، و"فارضة" إذا كان مؤنثًا. ومن الناحية اللغوية، يُشتق الفرض من أفعال مثل "جلس" و"ظرف"، أما اسمه فهو "الفريضة". وقد أُطلق اسم "علم الفرائض" على علم تقسيم الميراث؛ لأنه يُعنى بتحديد أنصبة الورثة بدقة ووضوح، وفق ما نصت عليه الشريعة الإسلامية. ومن أبرز هذه الأنصبة التي وردت في القرآن الكريم: النصف، الربع، الثمن، الثلثان، الثلث، والسدس.[٣٤]الفرع الثاني: تعريف الفضاء الافتراضي اصطلاحا قبل تعريف الفضاء الإلكتروني، لا بد من التطرق بإيجاز إلى منصة الاتصالات. هذه المنصة عبارة عن مجموعة ضخمة من الأصفار والواحدات التي تُشكل بيانات إلكترونية، كما أنها تعكس المفاهيم إلكترونيًا بصيغ مختلفة. الفضاء الإلكتروني هو في الواقع المنصة نفسها التي تُخزن فيها البيانات الإلكترونية وتُعالج بطرق مختلفة، ثم تُعكس في النهاية بالطريقة المطلوبة. [٣٥]عرّف بعض المؤلفين الفضاء الإلكتروني بأنه "مجموعة من الاتصالات الداخلية بين البشر عبر أجهزة الكمبيوتر وأجهزة الاتصالات دون مراعاة الجغرافيا الطبيعية"[٣٦]. وعرّفه آخرون بأنه "بيئة إلكترونية حقيقية تُجرى فيها الاتصالات البشرية بسرعة تتجاوز الحدود الجغرافية وبمساعدة أدوات إلكترونية. ويحدث ذلك بشكل مباشر وحي بطريقته الخاصة.[٣٧]الفضاء الافتراضي أو ما يُطلق عليه شبكة الإنترنت، واسم "إنترنت" في اللغة الإنجليزية **Internet**هو اسم مركب من جزأين: الجزء الأول **Inter**ويعني "بيني"، أما الجزء الثاني **Net**فيعني "شبكة"، وهو اختصار لعبارة **Interconnected Network**، أي "الشبكة المترابطة" أو "الشبكة البيئية". أما من حيث مدلولها، فهي تشير إلى الترابط بين الشبكات، كونها تضم عددًا هائلًا من الشبكات المترابطة فيما بينها، كما تُعرف أيضًا باسم "شبكة الشبكات المعلوماتية"، لأنها توفّر لمستخدميها أفضل الطرق للاستفادة من خدماتها المختلفة والتواصل مع الآخرين.وتُعدّ البيئة الافتراضية شبكة حاسوبية ضخمة تتكوّن من عدد كبير من الشبكات الأصغر، والتي تتيح لأي شخص متصل بها الدخول والتجوال داخلها، والحصول على المعلومات المسموح بها، والتحدث مع أي شخص في أي مكان حول العالم[٣٨]. فهي، باختصار، وسيلة تؤمن التواصل بين الشبكات المعلوماتية المختلفة دون التقيد بزمان أو مكان، ومن غير أي اعتبار للحدود الدولية بين الدول المختلفة[٣٩]. كما تملك هذه الشبكة القدرة على توفير الاتصال بأي نقطة في العالم من خلال بيئة افتراضية تعتمد على وسائل نقل متعددة مثل خطوط الهاتف، أو التقنيات البصرية المختلفة[٤٠]، وغيرها من وسائل وتقنيات الاتصال الحديثة. ويمكن اعتبارها "أم الشبكات"، لأنها تتيح الربط بين مختلف أجهزة الحاسوب وشبكاتها بعضها ببعض بشكل متكامل وفعّال. [٤١]بهذا القول، تُجنّب عبارة "الواقعي" الاعتقاد بأن افتراضية هذا الفضاء تعني أنه غير حقيقي؛ إذ توجد فيه نفس خصائص التفاعلات البشرية في العالم الخارجي، كالمسؤولية. إضافةً إلى ذلك، يُعدّ الفضاء الإلكتروني في الواقع بيئةً تُجرى فيها الاتصالات؛ أي مجرد مجموعة من الاتصالات، ووفقًا للتعريف المذكور، يتميز الفضاء الإلكتروني بالخصائص التالية: أ. هذا الفضاء عالمي وعابر للحدود. بمعنى آخر، يُمكن لأي شخص في أي مكان في العالم الوصول بسهولة إلى أحدث المعلومات من خلاله. لا يُمكن للحدود الجغرافية أن تمنع هذه الاتصالات، أو على الأقل يجب القول إنها لم تتمكن من منعها حتى الآن، حتى أن بعض الحكومات التي تحاول تصفية جزء من هذا الفضاء تواجه صعوبات. سهولة الوصول

إلى أحدث المعلومات. لقد أتاح الفضاء الإلكتروني أو الفضاء الإلكتروني وصولاً سهلاً وسريعًا إلى أحدث المعلومات في العالم. ج. جاذبية وتنوع وسائل الإعلام التي تستخدم الأفلام والصور والنصوص أو أي فن آخر لإضفاء الجاذبية. د. حرية المعلومات والاتصال: لقد تحقّق المعنى الحقيقي لحرية المعلومات في الفضاء الإلكتروني.[٤٢] للأسف، عند وصف الركن القانوني لجريمة الإرهاب السيبراني، تجدر الإشارة إلى أنه على الرغم من إقرار مجلس الشورى الإسلامي في السنوات الأخيرة لقانون جرائم الحاسوب بتاريخ ٢٠٠٩/٠٥/٠٣، والذي سد بعض الثغرات القانونية في مجال الجرائم المرتكبة ضد الحواسيب، إلا أنه ليس قانونًا شاملاً لمكافحة مختلف الأعمال من هذا النوع. ومن الأمثلة على ذلك جريمة الإرهاب السيبراني، والتي قد تكون بعض مواد هذا القانون فعالة في هذا المجال حتمًا، مع قليل من التساهل. ولكن بالنظر إلى أهم اتفاقية لمكافحة الإرهاب الإلكتروني، والمعروفة باتفاقية بودابست، يُمكن تعريف الإرهاب في الفضاء الافتراضي بأنه: أعمال مُخطط لها ومُستهدفة لأغراض سياسية وغير شخصية، تُنفذ ضد أجهزة الكمبيوتر والمرافق والبرامج المُخزنة فيها عبر الشبكة العالمية، بهدف تدميرها أو إلحاق أضرار جسيمة بها. ووفقًا للتعريفات المذكورة، فإن الإرهاب في الفضاء الافتراضيله دوافع سياسية؛ إذ يُنفذ باستخدام أجهزة الكمبيوتر كأسلحة وأدوات أو كأهداف ومُستهدفات؛ وتُنفذه جماعات دولية أو عناصر سرية بقصد العنف للتأثير على الشهود والمراقبين من خلال تغيير سياسات الحكومة المعنية. ومع ذلك، يجب إضافة الدوافع المالية والاقتصادية إلى هذه الفقرات لإكمال تعريف الإرهاب الإلكتروني.

المبحث الثاني الإجراءات الجنائية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانونين العراقي والإيراني

تتسم الإجراءات الجنائية لمكافحة الجرائم الإرهابية في هذا المجال بطابع فني وتقني عالٍ، حيث تتطلب استيعاباً واسعاً للتقنيات الحديثة وطرق جمع الأدلة الرقمية وتحليلها، إضافة إلى التعاون الدولي بين الدول لتتبع مرتكبي الجرائم الذين غالباً ما يكونون في مواقع مختلفة حول العالم. ويُعتبر ضمان سرعة اتخاذ الإجراءات القانونية دون المساس بحقوق المتهمين من أهم التحديات التي تواجه الجهات القضائية، إذ يجب تحقيق التوازن بين فعالية المكافحة وضمان احترام القوانين وحقوق الإنسان.علاوة على ذلك، يتطلب التعامل مع الجرائم الإرهابية في الفضاء الافتراضي تكامل وتنسيق بين مختلف الأجهزة الأمنية والقضائية، وكذلك بين التشريعات الوطنية والدولية، لتمكين عملية التحقيق والملاحقة القضائية بشكل فعال. ويشمل ذلك استخدام تقنيات متطورة مثل التتبع الرقمي، وحفظ الأدلة الإلكترونية، وتحديد هوية الجناة، وهو ما يستوجب وجود أطر قانونية واضحة تدعم هذه العمليات وتضمن شرعيتها.في هذا السياق، تكتسب دراسة الإجراءات الجنائية في القانونين العراقي والإيراني أهمية بالغة، حيث تعكس هذه الدراسة مدى تطور التشريعات والإجراءات القضائية في كل بلد لمواجهة هذا النوع من الجرائم، ومدى قدرتها على مواكبة التحديات التقنية والأمنية المعاصرة. كما تسلط الضوء على الفجوات القانونية والميدانية التي قد تعوق عملية مكافحة الإرهاب الرقمي، مما يفتح المجال لمزيد من التطوير والتحسين في إطار سيادة القانون وحماية الأمن الوطني

لذلك تم تقسيم هذا المبحث إلى مطلبين هما:

- المطلب الأول: الاجراءات الجنائية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون العراقي
- المطلب الثاني: الاجراءات الجنائية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون الايراني

المطلب الأول: الاجراءات الجنائية لمكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون العراقي

تُعد الإجراءات الجنائية من الأدوات الأساسية التي يعتمد عليها النظام القانوني في التصدي للجرائم الإرهابية في الفضاء الافتراضي، حيث يسعى المشرّع العراقي من خلالها إلى تنظيم آليات الكشف عن هذه الجرائم وتعقب مرتكبيها وتقديمهم إلى العدالة. ونظرًا لما تتميز به الجرائم الإرهابية الإلكترونية من طابع خفي وعابر للحدود وصعوبة الإثبات، فقد واجهت المنظومة القانونية العراقية تحديات كبيرة في تطوير إجراءات فعالة تضمن تحقيق الردع دون المساس بالحقوق الدستورية والحريات الأساسية. وقد تضمنت التشريعات العراقية ذات الصلة مجموعة من الأحكام التي تُنظِّم وسائل التحري، وضبط الأدلة الرقمية، والتعاون القضائي، إلا أن الحاجة لا تزال قائمة إلى المزيد من التحديثات التشريعية والإجرائية لمواكبة التقدم التقني وتنامي استخدام الفضاء الرقمي في الأعمال الإرهابية.

الفرع الأول: مرحلة التحقيق

إن مرحلة التحقيق تعد مرحلة مهمة من مراحل مكافحة الأجهزة الأمنية لجريمة الإرهاب الإلكتروني، فكما هو ثابت بأن الدعاوي الجزائية تمر بمرحلة التحقيق ومن ثم المحاكمة وكذلك هو الحال على هذه الطريقة فإن التحقيق الجنائي يمر بمرحلتين، مرحلة التحقيق الأولى الذي يقوم الجهاز الأمني (أعضاء الضبطية القضائية) أولا للكشف عن الجريمة أول مرة وأما بالنسبة للمرحلة الثانية فهي مرحلة التحقيق الابتدائي والتي تتمثل بدور قاضي التحقيق والمحقق وعضو الادعاء العام، وتشمل أو تبنى إجراءات التحقيق في هذه المرحلة على إجراءات التحقيق الأولى التي قام بها أول

مرة أعضاء الضبط القضائي٤٣.كما هو معروف إن التحقيق الجنائي بمفهومه العام هو كيفية البحث والتحري عن جريمة معينة منذ لحظة معرفة ارتكابها أو تلقي البلاغ عن وقوعها وإلى مراحل جمع الأدلة الكاملة عن هذه الجريمة في سبيل كشف الغموض عنها وتحديد الفاعلين فيها ويتم ذلك من خلال:التفتيش الإلكتروني: ويمكن تعريفه بأنه إجراء من إجراءات الأجهزة الأمنية تقوم بها طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى متهم٤٤، وإن التفتيش دور لابد منه في الجرائم التقليدية فهو أسلوب لابد منه في التحقيق فيها، أما في التفتيش عن جريمة الإرهاب الإلكتروني فهذا من خلال: تفتيش مكونات الكمبيوتر المادية٤٥. لقد أجازت المادة (٧٤) من قانون أصول المحاكمات الجزائية العراقي لقاضي التحقيق تفتيش مكونات الحاسوب المادية حيث نصت "إذا تراءى له وجود أشياء أو أوراق تفيد التحقيق لدى شخص، فيما أن مشروع جرائم المعلوماتية في العراق لسنة ٢٠١١ قد أقر تتبع المعلومات إلى أنظمة الكمبيوتر والشبكات الأخرى محل الاشتباه فقد نصت المادة (٢٦/أولا/ج) على أنه "الدخول إلى أجهزة الحاسوب والشبكات أو أي جزء منها وإلى البيانات المخزنة فيها وإلى أي واسطة أو وسيلة يمكن أن تخزن فيها بيانات الحاسوب الموجودة داخل العراق وله اعتراض البيانات ورصدها ومراقبتها بقرار مسبب ولمدة وغرض محددين".المعاينة الإلكترونية:تعد المعاينة على غرار التفتيش من المراحل الأولى للاستدلال في التحقيق في ملابسات أي جريمة بل ومن أهم المراحل فيها على الإطلاق، وذلك نظرا لما يمكن أن توفره هذه المعاينة من أدلة إثبات جريمة الإرهاب الإلكتروني، وتزداد أهمية المعاينة في جريمة الإرهاب الإلكتروني، نتيجة طبيعتها الخاصة في السلوك الإجرامي وبالإضافة إلى اعتبارها من الجرائم المستحدثة مما يستوجب ابتكار إجراءات خاصة في المعاينة عليها على عكس الجرائم التقليدية الأخرى٤٦، وتعنى المعاينة رؤية أماكن ارتكاب الوقائع الجنائية كما وينصرف مفهوم المعاينة الجنائية إلى فحص جسم المجني عليه والمتهم وإثبات ما يتخلف عندهما من آثار٤٧، وقد عرفت من جانب الفقه بأنها مناظرة وفحص المكان الذي ارتكبت فيه الجريمة بما يحوي من أشياء وأشخاص بهدف التعرف على كل أو بعض الحقائق الجوهرية التي يستهدفها التحقيق الجنائي، واكتشاف ورفع ما يخلفه الجناة من آثار جنائية٤٨.الاستعانة بالخبراء التقنيين:إذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم المعلوماتية حيث تتعلق بمسائل فنية غاية في التعقيد، يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها وبالوسائل الأخرى للإثبات، ويلاحظ أن نجاح التحريات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء٤٩، فإجرام الذكاء والفن لا يكشفه ولا يحله إلا ذكاء وفن مماثلين.وتبرز أهمية الاستعانة بالخبير في مجال جريمة الإرهاب الإلكتروني عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه، ونشير هنا إلى أن هناك دول أعدت أجهزة متخصصة للخبرة الغرض منها مكافحة تصاعد جرائم الإرهاب الإلكتروني كالولايات المتحدة الأمريكية.٥٠ ونظرا لتطور جريمة الإرهاب الإلكتروني وأن الدليل الذي يقوم على إثبات هذا النوع من الإجرام لابد أن يكون من ذات الطبيعة التقنية وهو الأمر الذي لا تكون فيه النصوص الكلاسيكية للتحقيق واستخراج الدليل قادرة على القيام به، مما يؤدي إلى إفلات الكثير من المجرمين من العقوبة، لذلك أصبح للخبير التقني أدورا مختلفة في مكافحة جريمة الإرهاب الإلكتروني٥١ وهي كالتالي:تسريب العملاء:يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول أحد موظفي الضابطة العدلية إلى العالم المعلوماتي، عن طريق اختراقه لمواقع معينة وفتح ثغرات رقمية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية ارتكابهم للجرائم والدور الذي يقوم به كل منهم واعتماده كدليل للقبض عليه متلبسين في الجريمة، وهذا الإجراء لا يسمح باللجوء إليه إلا في حالات محددة وخطيرة كجرائم الإرهاب الإلكتروني٥٢.اعتراض المراسلات:ذلك الإجراء السري الذي يقوم به المراقب للتتبع المراسلات الخاصة بالمشتبه به ودون عمله، باعتباره إجراء تحقيقي يباشر خلسة وتنتهك فيه سرية المراسلات الخاصة، تسمح به السلطات العدلية في الشكل المحدد قانونا، بهدف الحصول على دليل مادي للجريمة لاستخدامه في مواجهة جريمة الإرهاب الإلكتروني عبر وسائل الاتصال السلكية واللاسلكية.٥٣المراهقة الإلكترونية للشبكات المعلوماتية:إجراء من إجراءات التحقيق يباشر في جناية أو جنحة وقعت، للبحث عن أدلتها ضد شخص قامت تحريات جدية على أنه ضالع في ارتكاب جريمة الإرهاب الإلكتروني أو لديه أدلة تتعلق بها وأن في مراقبة أحاديثه٥٤ التليفونية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية، وكانت الجريمة على درجة من الجسامة تستوجب اتخاذ هذا الإجراء الاستثنائي، بأن كانت جناية أو جنحة يعاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، فالمشتبه به الإلكتروني يمكن أن يكون شخصا أو موقعا أو بريدا إلكترونيا مخالف للقانون وتشمل المراقبة الإلكترونية جميع تحركات المشتبه به عبر الإنترنت بما في ذلك بريده الإلكتروني.٥٥استيفاء

المعلومات من مصادرها:يلزم مقدم الخدمات التقنية بتسليم البيانات التي في حوزته أو الموضوعة تحت رقابته، تنفيذا لموجبي الحفظ المنصوص عليه في القانون وذلك في حدود مقتضيات التحقيق والمحاكمة وأن يخوله الوصول إلى التعليمات المذكورة وفقا للوقت الحقيقي، لأي عملية اتصال عابرة عبر شبكته، ويتم ذلك عن طريق التعاون بين الحكومة والجهات المشغلة للخدمة ومن أجل تسهل هذا الأمر قد تذهب الجهات الأمنية في الحكومة إلى عقد اتفاقات، تجبر الشركات المقدمة لخدمة الإنترنت على الاستجابة لهذه القرارات القضائية٥٦، وكذلك أشار مشروع جرائم المعلوماتية في العراق في المادة (٢٦/أولا/ب) منه على (أن للقاضي المختص إصدار الأوامر لجهات تزويد خدمات شبكة المعلومات أو الخدمات التقنية بأنواعها لتقديم بيانات الاشتراك والمرور لجهة التحقيق إذا كان من شأنها أن تساهم في الكشف عن الجريمة).

الفرع الثاني: مرحلة الإثبات

إن الشهادة كوسيلة من وسائل الإثبات هي المعلومات التي يدلي بها الشاهد أمام سلطات التحقيق وهي الطريق العادي للإثبات الجزائي، في حين تعد الكتابة هي الطريق العادي للإثبات المدني، وفي ظل التطور الحاصل في المجتمعات وظهور أنماط حديثة في السلك الإجرامي والتي ترافقت مع ظهور تكنولوجيا المعلومات المتمثلة في جرائم الإرهاب الإلكتروني، فقد غدت وسائل الإثبات التقليدية قاصرة على مساعدة الأجهزة الأمنية.فتعرف الشهادة بشكل عام على أنها تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه بإحدى حواسه الأخرى، فهي التعبير عن مضمونها والإدراك الحي للشاهد بالنسبة للواقعة التي شاهدها أو سمعها أو أدركها بحاسة من حواسه بطريقة مباشرة والمطابقة لحقيقة الواقعة التي يشهد عليها في مجلس القضاء ممن تقبل شهادتهم بعد أداء اليمين.٥٧أما بالنسبة للشهادة في جرائم المعلوماتية فهي لا تختلف من حيث ماهيتها عنها في الجرائم التقليدية من حيث المبدأ العام، وإن تقدير حضور الشهود في هذه الجرائم يكون متروكا لفطنة وذكاء المحقق ومرتبط بظروف التحقيق في جرائم المعلوماتية، أي أن تقدير مدى كفاية شهادة الشاهد المعلوماتي يرجع إلى جهات التحقيق المختصة في هذه الجرائم.٥٨وعلى أساس ما تقدم فإنه يمكن تعريف الشاهد في جريمة الإرهاب الإلكترونية على أنه الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات في دخل هذا النظام، ولذلك يطلق عليه اسم الشاهد الإلكتروني تمييزا له عن الشاهد التقليدي.٥٩مضمون الشهادة في جريمة الإرهاب الإلكتروني:على الشاهد في جريمة الإرهاب الإلكتروني إعلام سلطات التحقيق بمعلومات جوهرية عن جريمة الإرهاب الإلكتروني وهذه المعلومات هي:طباعة ملفات البيانات الموجودة في ذاكرة الحاسب الآلي:يقضي هذا العنصر أن يعلم الشاهد المعلوماتي سلطات التحقيق والتحري جرائم المعلوماتية بملفات البيانات المخزنة في ذكارة الحاسب أو الذاكرات المتنقلة وأن يقوم بطبع هذه الملفات أو المعلومات وتسليمها لهم طالما اقتضت مصلحة التحقيق ذلك.٦٠الإفصاح عن كلمات المرور السرية:يستلزم هذا العنصر أن يعلم الشاهد المعلوماتي سلطات التحري والتحقيق بجرائم المعلوماتية بكلمات المرور السرية للأنظمة المعلوماتية وأن كلمة المرور ما هي إلا وسيلة لتأمين نظام الحاسب ضد الاستخدام بواسطة شخص غير مسؤول قد يتسبب في فقد بيانات مهمة، فيتم استخدام كلمة مرور وجعل معرفتها مقصورة على الأشخاص المسئولين فقط، وفي نظم المعلومات الكبيرة يتم تصميم كلمات المرور لمستويات الإدارة المختلفة تمكن المدراء من التعامل مع بعض البيانات دون سواهم وكذلك بالنسبة لباقي المستويات٦١.الكشف عن الشفرات المدونة بها الأوامر الخاصة تنفيذ البرامج المختلفة:بمقتضى هذا العنصر يجب على الشاهد المعلوماتي في جريمة الإرهاب الإلكتروني أن يبين مفاتيح الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة للأنظمة المعلوماتية، ذلك أن الأوامر أو الرسائل المكتوبة بالشفرة تحتاج إلى ترجمة لحل هذه الشفرة حتى يمكن فهمها، وجدير بالذكر أن البيانات أو البرامج المسجلة على أقراص أو شرائح تسجيل هي شفرات ثنائية وهذه الشفرة قد تكون مكتوبة بلغة عالية المستوى وتسمى في هذه الحالة شفرة المصدر أو أن تكون مكتوبة بلغة الآلة وتسمى في هذه الحالة شفرة الهدف أو الموضوع٦٢.شروط أداء الشهادة في جريمة الإرهاب الإلكتروني:ومن المنطلق السابق ولتحديد المقصود بشروط الشهادة في جريمة الإرهاب الإلكتروني فإنه يمكن إيجازها في هذه الشروط من خلال ما يأتي:يجب أن تكون بصدد جريمة إلكترونية وقعت بالفعل وسواء أكانت جنحة أو جناية:أي بمعنى أن يكون هناك جريمة إلكترونية قد وقعت حتلا يتحقق التزام الشاهد المعلوماتي بالإخبار عنها، فالتزام هذا الشاهد لا يمكن أن يتحقق لضبط جريمة مستقبلية حتى ولو كانت هنالك تحقيقات جدية تؤكد بأن هنالك جريمة ستقع، كما أن وقوع جريمة معلوماتية بشكل فعلي لا يحقق التزام الشاهد المعلوماتي بالإعلام عنها أيضا، ما لم تكن هذه الجريمة الواقعة فعلا هي من نوع جنحة أو جناية، فالمخالفات هنا تستبعد من أداء هذه الشهادة وإن مرد ذلك يعود إلى أن الآثار الناجمة عنها لا تشكل خطورة كبيرة على المجتمع.٦٣أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل جريمة المعلوماتية:إن معرفة الشاهد المعلوماتي الجوهرية المتصلة بالنظام المعلوماتي محل جريمة المعلوماتية تمثل شرطا جوهريا ليكون هذا الشاهد ملتزما بالإعلام عن جريمة

الإرهاب الإلكتروني، وأن عناصر هذه المعلومات هي الكشف عن مفاتيح الشفرات، الإفصاح عن كلمات السر، طباعة الملفات الخاصة بالبيانات٦٤.أن تكون هنالك مصلحة لسلطات التحقيق في الحصول على المعلومات الجوهرية المتصلة بالنظام المعلوماتي محل جريمة الإرهاب الإلكتروني:إن الشهادة المعلوماتية حتى تحقق أثرها أثناء التحقيق فإنه لابد من أن تكون المعلومات الجوهرية المتعلقة بالأنظمة المعلوماتية محل البحث والتحقيق لازمة ومهمة لاختراق هذه الأنظمة وذلك من أجل البحث عن الأدلة التي تنتج عن جريمة المعلوماتية والتي تكون بداخل هذه الأنظمة.٦٥.عدم خبرة الأجهزة الأمنية بالمجتمع الرقمي:إن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان فبعد ظهور الإنترنت لم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات وبسبب هذه الطبيعة العالمية للجريمة المعلوماتية برزت العديد من المشاكل والصعوبات أمام السلطات الأمنية ويشترط لقبول الدليل الجنائي كدليل إثبات أن يتم الحصول عليه، بطريقة مشروعة، كما إن هناك صعوبات تتعلق بالجانب الخاص بتطبيق القانون الواجب التطبيق من حيث مبادئ إقليمية تطبيق القانون الجنائي، ومبدأ العينية والشخصية والصعوبات الخاصة بالإنابة القضائية الدولية، ليس هذا فحسب، وإنما يمتد هذا الغموض والإبهام إلى القضاء الذي ينظر في الجريمة التي وقعت باعتبارها من الجرائم الجديدة والحديثة وعدم امتلاك القاضي المعرفة والإحاطة الكاملة بالموضوع الذي ينظر فيه وخاصة موضوع الدليل الذي تم الحصول عليه من الفراغ.٦٦إن نقص المهارة الفنية في استخدام الكمبيوتر والإنترنت وقلة توافر المعرفة بأساليب ارتكاب جرائم الإرهاب الإلكتروني وقلة الخبرة في مجال التحقيق والتحري عن جرائم العالم الافتراضي، هي عوامل من شأنها أن تضعف من دور الأجهزة المختصة بالتحقيق في هذه الجرائم وكشف النقاب عنها، كما أن مسألة كيفية التعامل والحفاظ على الأدلة الرقمية من قبل الأجهزة الأمنية من أهم العقبات التي تحول أمام مهمة الأجهزة الأمنية في مواجهة جريمة الإرهاب الإلكتروني.٦٧

المطلب الثاني: الاجراءات الجنائية لـ مكافحة الجرائم الإرهابية في الفضاء الافتراضي في القانون الايراني

إن التطور التكنولوجيا أوجب على الأجهزة الأمنية إعادة النظر في قواعد الإثبات الجنائي فإن جريمة الإرهاب في الفضاء الافتراضي قد أوجب التقصي عنها تغييرا في الأساليب المعتمدة في الكشف على المسرح المعلوماتي لهذه الجريمة ومعاينة الأشياء غير المادية فيها وآليات البحث عن الأدلة الرقمية والتفتيش عن كل ما يسهم في كشف كيفية ارتكاب هذه الجرائم وتحديد المساهمين فيها، ذلك على أساس أن هذه الجرائم يصعب الكشف عن هوية مرتكبيها كونهم يلجون عالمها الافتراضي الرقمي[٦٨].

الفرع الأول: مرحلة التحقيق

يكتسب تطور التقنيات الحديثة أبعادًا جديدة كل يوم، ويتداخل وينشط في جميع مجالات ومجالات البشرية. وقد أدى تطوره الواسع والشامل إلى اختفاء العديد من أبعاده، وجعله مكانًا مناسبًا للمجرمين لتنفيذ عملياتهم الإجرامية. وأصبح الفضاء الإلكتروني، إلى جانب فوائده وآثاره الإيجابية العديدة، مصدر تهديدات خطيرة لجميع الأفراد والمنظمات ودول العالم، المتقدمة منها والمتخلفة. وقد دفع انتشار جرائم الحاسوب في الدول الأكثر استخدامًا للحاسوب والإنترنت الحكومات إلى التفكير في إنشاء آلية قانونية وشرعية للتحقيق في هذه الجرائم ومكافحتها. كما وُضعت اتفاقيات دولية للتعاون في عملية تحديد الجرائم والمجرمين، والتعاون في التحقيق مع المجرمين وملاحقتهم من قبل الشرطة، وتبادل المعارف والمعلومات الشرطية في مجال التعرف العلمي على الجرائم الإلكترونية واكتشافها[٦٩]. وتتدخل عدة عوامل في عملية التحقيق في الجرائم ورفع الدعاوى القضائية، من أهمها النظام القضائي الشرطي والمحضرون، وخاصة الخبراء القضائيون. إن فهم دور هذه المؤسسات وتنظيمها في تشكيل الدعوى القضائية، وخاصةً في مراحلها الأولى والتحقيقات الأولية، له دورٌ بالغ الأهمية في توضيح آلية ومنهجية التحقيق في الجرائم. ومن المهام الرئيسية للنظام الإسلامي على مستوى المجتمع إرساء الأمن، ولذلك تُشكل أدواتٌ ومنظماتٌ ومؤسساتٌ لتحقيق الأمن وممارسة السيادة، ومن أبرزها جهاز الشرطة[٧٠]. إن قوة شرطة جمهورية إيران الإسلامية، وفقًا لواجبها القانوني والإلزامي (المادة ٤ من قانون إنشاء قوة الشرطة (١٣٦٩/٤/٢٧))، مسؤولة عن أمور مثل منع ارتكاب الجرائم، واعتقال المجرمين، ومنع إزالة آثار الجريمة، وتقديم الدعم الأولي للضحايا. إن أنشطة هذه المنظمة مادية وملموسة في الغالب، ولكن في العقود الأخيرة، خضع نوعها وطريقة عملها لتغييرات كبيرة.[٧١]فالتحقيق في القانون الإيراني يعني حرفيًا التحقيق والبحث للوصول إلى الحقيقة، والتحقيقات الأولية هي مجموعة من التدابير والتحقيقات التي يقوم بها الموظفون القضائيون مباشرة أو بأمر وإحالة من السلطات القضائية أو من قبل قضاة التحقيق والسلطات القضائية المختصة الأخرى من أجل تسهيل وإعداد الأدلة، بما في ذلك الأدلة لإثبات الجريمة والأدلة المفيدة للمتهم، مع مراعاة مبدأ البراءة. والهدف الرئيسي منها هو إعداد القضية وتسهيل وتسريع المحاكمة في المحكمة،[٧٢]

ويستند التحقيق في الجرائم الإلكترونية وملاحقتها في البلاد إلى قانون جرائم الكمبيوتر في الجزء الثاني من قانون جرائم الكمبيوتر الذي أقره مجلس الشورى الإسلامي بتاريخ ٢٠٠٩/٠٣/٢٥، مع الإشارة إلى القواعد الإجرائية لمراحل التحقيق الأولي وملاحقة الجرائم الإلكترونية، بما في

ذلك مسائل الاختصاص القضائي وجمع أدلة الجريمة والاعتماد عليها وما إلى ذلك.[٧٣]فقبل وقوع الحادث، تتخذ البعثة إجراءاتها من خلال رصد وتحديد التهديدات والأضرار والجرائم المحتملة. يُعدّ منع الجريمة نوعًا من التحقيق والمواجهة. عند وقوع الحادث، لا يكتمل أثر الجريمة، فتتخذ الشرطة إجراءات لمواجهة النشاط الإجرامي ومنع استمراره. فبعد وقوع الحادث، تعمل الشرطة والنظام القضائي على التحقيق والمساءلة، ولإكمال التحقيق والملف، تدخل مرحلة ملاحقة المجرمين بناءً على الخطوات التالية:١) الحصول على إذن قضائي؛ ٢) تشكيل فريق تحقيق؛ ٣) التحقيق في الجرائم الإلكترونية؛ معاينة مسرح الجريمة؛ تحديد الهويات في الفضاء الإلكتروني؛ الأدلة الإلكترونية؛ استجواب المشتبه بهم؛ ٤) الاستعانة بخبراء تقنيين حاسوبيين كمستشارين؛ ٥) إعادة بناء مسرح الجريمة.يمكن تعريف التفتيش في ايران على أنه إجراء من اجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى متهم، إن التفتيش المعلوماتي الذي يستلزم عبور الحدود الدولية لا بد أن يتم في إطار اتفاقيات ثنائية أو دولية في ما بين الدول تجيز وتسهل هذا الامتداد ما بين الدول للحد من جريمة المعلوماتية، وبالمحصلة فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الاتفاقيات أو على الأقل الحصول على إذن الدولة المراد التفتيش فيها، وإن هذا ما يؤكد على أهمية وفعالية التعاون بين الدول في مجال مكافحة جرائم المعلوماتية أو الجرائم الإلكترونية المرتكبة عبر الإنترنت.[٧٤]

الفرع الثاني: مرحلة الإثبات

يحتل الإثبات الالكتروني الأهمية البالغة، في تأكيد وجود الحق المتنازع عليه، بوصفه من المواضيع الجديدة التي أصبحت من أكثر المواضيع القانونية التي أثارت اهتمام جانب كبير من الفقه القانوني، إذ فرض هذا الإثبات نفسه في عالمنا المعاصر بسبب تطور وسائل الاتصال الناجمة عن اتحاد تقنيتي المعلومات والاتصالات، وهو ما أدى إلى الربط بين شعوب العالم، فأصبحت عملية تبادل المعلومات سهلة وميسرة، بفضل التقنية المعلوماتية المتمثلة في اختراع وتطوير الحاسب الآلي القادر على الاحتفاظ واسترجاع ومعالجة المعلومات بسرعة فائقة، وهو ما انعكس بدوره على الثقة والأمان التي تعطى لأدلة الإثبات الالكتروني.[٧٥]إن أهم صعوبة في الخبرة المعلوماتية هي جلب الخبير المناسب للاستعانة به؛ باعتبار أن الخبرة في مجال المعلوماتية لا تنطبق على نفس الشروط التقليدية الخاصة بتعيين الخبير، فيتطلب بالخبير المعلوماتي أن يكون ملما بالجوانب التقنية والفنية المعلوماتية والتي منها كحد أدنى ما يلي[٧٦]:

- المعرفة بمكونات أجزاء الكومبيوتر وصناعته وطرازه ونوع نظام التشغيل فيه والأجهزة الطرفية الملحقة به وكلمات المرور ورموز التشفير ... والخ.
- البيانات الرقمية المحتمل تواجد أدلة الاثبات والصور أو الاشكال التي تتخذها.
- الطريقة التي يمكن بواسطتها فصل النظام المعلوماتي دون إتلاف أو إفساد أو تغيير الأجهزة
- الطريقة التي تتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب على ذلك إتلافها.
- استطاعة تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة
- نسخ أو مطبوعات بشكل أو طريقة يمكن للقاضي أن يفهمها ويستوعبها.

يمكن القول بشكل عام بأن هنالك أسلوبان لعمل الخبير المعلوماتي في مكافحة جرائم المعلوماتية، يمكن التطرق إليهما بشيء من الإيجاز:[٧٧]

أ. جمع مجموعة المواقع التي تشكل جريمة في ذاتها مثل جرائم النصب والتهديد والنسخ وسرقة المعلومات ... وإلخ، ومن ثم يقوم الخبير المعلوماتي بعملية تحليل رقمي لهذه المواقع في إطار معرفة الكيفية التي تم من خلالها الاعداد البرمجي لها ونسبتها إلى المسار الذي أعدت فيه وتحديد عناصر حركتها وكيف تم التوصل إلى معرفتها، وأخيرا التوصل لمعرفة "بروتكول **IP** والذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع.

ب القيام بتجميع وضبط مجموعة المواقع التي لا تشكل في ذاتها جريمة ولكن هنالك جرائم معلوماتية تقع جراء تتبع موضوعات هذه المواقع الأخيرة، كما هو الحال في المواقع التي تساعد الغير على معرفة المؤثرات العقلية وجرعات المخدرات حسب وزن الإنسان، بإيهام أنه إذا تم تتبع التعليمات الواردة فيها لن يصل الشخص إلى حالة الإيمان، وكذلك الحال بالنسبة لكيفية اعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية ... إلخ.

وبالإضافة إلى ما تقدم فإن العناصر المكلفة بالتحقيق في جرائم المعلوماتية لا تكون ضمن المستوى المطلوب في التحقيق في هذه الجرائم؛ فإذا كانت السلطات القائمة بالتحقيق من أفراد الضبطية القضائية وقضاة بما لها من خلفية قانونية تؤدي دوراً كبيرا في التحري عن الجرائم والبحث

عن مرتكبيها في إطار الجرائم التقليدية، فإن وظيفتها في مكافحة جرائم المعلوماتية لا ترق إلى نفس الدرجة وإن ذلك يمكن أن يعزى إلى أن الطبيعة الخاصة للبيئة الإلكترونية التي تتعامل معها هذه الجهات وفضلاً عن خصوصية الدليل الرقمي الذي ينعكس ويؤثر على عمل الجهات المكلفة بالتحقيق عن هذه الجرائم، فيتطلب الكشف عن جرائم المعلوماتية اكتساب جهات التحقيق فيها مهارات خاصة على نحو يساعدهم في مواجهة التقنيات المعلوماتية. ويرى المتخصصين في مكافحة جرائم المعلوماتية أن الأنظمة المعلوماتية وما يمكن أن يقع عليها من جرائم تعد تحديا كبيرا أمام أجهزة العدالة الجنائية؛ ذلك أن أفراد الأمن غير المتخصصين معلوماتيا ولديهم معرفة بسيطة بالمعلوماتية والذين انحصرت معلوماتهم في جرائم قانون العقوبات بصورته المألوفة، من قتل وضرب وسرقة لن يكونوا قادرين على التعامل مع مفهوم جريمة المعلوماتية والتي تقع بطريقة تقنية عالية[٧٨]

إن الشهادة كوسيلة من وسائل الإثبات هي المعلومات التي يدلي بها الشاهد أمام سلطات التحقيق وهي الطريق العادي للإثبات الجزائي، في حين تعد الكتابة هي الطريق العادي للإثبات المدني، وفي ظل التطور الحاصل في المجتمعات وظهور أنماط حديثة من السلوك الإجرامي والتي ترافقت مع ظهور تكنلوجيا المعلومات متمثلة بجرائم المعلوماتية أو الإلكترونية، فقد غدت وسائل الإثبات التقليدية قاصرة عن أن تساعد أفراد التحقيق في هذه الجرائم في التحقيق فيها وكشف مرتكبيها؛ فالشهادة مثلاً موضوع البحث هذا لا يمكن للوهلة الأولى تصور توافرها في جرائم المعلوماتية والتي كما اتضح في مواضيع سابقة بأن محل الجريمة فيها هو البيانات والمعلومات والبرامج التي تكون غير مرئية وغير قابلة للمشاهدة من جانب الغير، ولكن على الرغم من ذلك وباعتبار أن الشهادة هي الطريق العادي للإثبات الجزائي فإن الشهادة المعلوماتية من قبل أفراد معينين ومختصين بجرائم المعلوماتية يكون لها دور مهم في مساعدة أفراد التحقيق في هذه الجرائم في كشفها وحل لغزها وتقديم مرتكبيها إلى المحاكم المختصة؛ ذلك أن المعلومات التي يقدمها الشاهد المعلوماتي لأفراد التحقيق في جرائم المعلوماتية هي معلومات هامة وجوهرية للدخول إلى النظام الإلكتروني ومعاينة الأدلة الناجمة عن هذه الجرائم. وكما سبق وأن بين الباحث بأن موضوع الشهادة في جرائم المعلوماتية يبدو غير مألوف بالنسبة للقضاء وللجهات المكلفة بالتحقيق في هذه الجرائم للوهلة الأولى بما يتصف به محل هذه الجرائم من طبيعة إلكترونية تصعب الشهادة فيه، ولكن على أساس أن الشهادة هي من الطرق المهمة في الإثبات الجنائي ضد مرتكبي أي جريمة وبما فيها جريمة المعلوماتية فإنه لا بد من توضيح كيفية انطباق هذه الشهادة على هذا النمط من الإجرام.[٧٩]

أولا: تنوع الأنماط:

قد تفنن مرتكبو هذه الجرائم في تنوع الأساليب المبتكرة في تنفيذ جرائمهم مستغلين في هذا معرفتهم وقدراتهم في هذا المجال من أجل القيام بأنشطتهم غير المشروعة وتتسم جريمة الإرهاب الإلكتروني بخصائص تجعلها مختلفة عن الجرائم التقليدية، وهذا ما يجعل المجرم يستغلها في ارتكاب جريمة العابرة للحدود، من خلال إتلاف أنظمة المعلومات وصناعة ونشر الفيروسات وجرائم الاختراقات وجرائم السطو والتحويل الإلكتروني، وذلك نظرا لدخول شبكة الإنترنت إلى مختلف ميادين الحياة أصبحت المعلومات المتعلقة بالأفراد متداولة عبرها بكثرة مما يجعلها عرضة للانتهاك والاستعمال من قبل المجرمين وقد نتج عن ذلك التهديد والمضايقة والملاحقة وجرائم القذف والسب وتشويه السمعة وانتحال الصفة والتغرير والاستدراج ونشر الإباحية وغيرها.[٨٠]

ثانيا: عدم ترك المجرم أثر ملموس:

إن كان هناك دليل يستطيع تدميره في ثوان معدودة وفرض الجناة لتدابير أمنية تحيط بالسلوكيات الإجرامية هذه تحول دون إمكانية الوصول إليها عن طريق استخدام كلمة السر المتداولة في المجتمع الإلكتروني إن صح التعبير فهؤلاء المجرمون غالبا ما يكونوا من الأذكياء فلهذا يلجئون إلى هذه التدابير حتى لا تنالهم يد العقاب، وحتى لا تمكن غيرهم من الوصول إلى بياناتهم المخزنة إلكترونيا أو المنقولة عبر شبكات الأتصالات أو قد يقوم المجرم الإلكتروني بإخفاء هويته أو انتحال شخصية أو تحت اسم وهمي مما يجعل الكشف عن تلك المرسلات أو المعلومات بالغة الصعوبة ويؤدي بالنتيجة إلى صعوبة اكتشاف النشاطات الإجرامية المرتكبة في نطاق العالم الافتراضي، ومعاقبة مرتكبيها[٨١]، وإن ما يزيد صعوبة الكشف عن جريمة الإرهاب الإلكتروني هو أن المجني عليه وخصوصا في جرائم الابتزاز ما يتم التكتم عن الجرائم ولا تبلغ السلطات المختصة عنها، أن يكون المجني عليه مصرفا أو مؤسسة مالية أو مشروعا صناعيا أو تجاريا ضخما ولا يتم الإبلاغ عن تلك الجريمة والسبب في ذلك يرجع في اعتبارها أن الإبلاغ عن تلك الجرائم ربما يؤدي إلى إحاطة المجرمين عمدا بنقاط الضعف في أنظمتها ورغبة منها في توخي الخسائر التي قد تلحق بها من جراء هذا البلاغ وتأثير ذلك على ثقة العملاء بها وإن الجريمة الإرهابية الإلكترونية ترتكب في مسرح افتراضي.[٨٢]

الخاتمة

في ختام هذا البحث، يمكننا أن نؤكد على أن الجرائم الإرهابية في الفضاء الافتراضي أصبحت تهديداً كبيراً للأمن الدولي، حيث يتم استغلال الإنترنت بشكل متزايد من قبل الجماعات الإرهابية لتحقيق أهدافهم العنيفة. ومع الانتشار الواسع للتكنولوجيا الرقمية، أصبح من الضروري أن تتطور التشريعات القانونية على الصعيدين الوطني والدولي لمواكبة هذا التحدي المستمر. يُعد التنسيق بين الدول والمنظمات الدولية في هذا المجال أمراً بالغ الأهمية، نظراً للطابع العابر للحدود الذي يتميز به الفضاء الافتراضي.

إن التصدي للجرائم الإرهابية عبر الإنترنت يتطلب تطوير آليات فعالة لمراقبة المحتوى المتطرف ومكافحة نشر الفكر المتطرف، بالإضافة إلى تعزيز التعاون بين الحكومات ومقدمي خدمات الإنترنت. تكنولوجيا الذكاء الاصطناعي والتحليل البياني أصبحت من الأدوات الأساسية في الكشف عن هذه الأنشطة الإرهابية والحد منها.

النتائج:

١. زايد استخدام الجماعات الإرهابية للفضاء السيبراني في تنفيذ مخططاتها، بما في ذلك التجنيد ونشر الفكر المتطرف والتحريض على العنف.
٢. قصور بعض التشريعات الوطنية في مواكبة الجرائم الإرهابية الإلكترونية الحديثة، ما يخلق فجوة قانونية يستغلها الجناة.
٣. ضعف التعاون الدولي في تبادل المعلومات بين الدول وجهات إنفاذ القانون، مما يحد من فعالية ملاحقة الجريمة الإرهابية العابرة للحدود.
٤. تحديات تقنية تواجه سلطات التحقيق، منها صعوبة الوصول إلى الأدلة الرقمية المشفرة وتحديد مواقع الجناة.
٥. أهمية التوازن بين الأمن وحرية التعبير، خاصة في ظل الاتهامات الموجهة إلى بعض الحكومات باستخدام مكافحة الإرهاب كذريعة للرقابة.

المقترحات:

١. حديث التشريعات الوطنية لتشمل تعريفًا دقيقًا وشاملًا للجرائم الإرهابية الإلكترونية، مع إدراج عقوبات تتناسب مع خطورتها.
٢. إنشاء وحدات متخصصة في مكافحة الإرهاب السيبراني ضمن أجهزة الأمن، تضم خبراء في القانون والتقنية والتحليل الرقمي.
٣. تعزيز التعاون الإقليمي والدولي لتبادل المعلومات والخبرات، وتوقيع اتفاقيات مشتركة لمكافحة الجريمة الإلكترونية ذات الطابع الإرهابي.
٤. رفع مستوى الوعي المجتمعي حول مخاطر التطرف عبر الإنترنت، من خلال برامج تربوية وإعلامية تشارك فيها المؤسسات التعليمية والدينية.
٥. الاستثمار في تطوير تقنيات التحليل الجنائي الرقمي، والتدريب المستمر للقضاة والمحققين على استخدام الأدلة الإلكترونية.

المصادر والمراجع

الكتب والمؤلفات

١. ابن منظور، محمد بن مكرم .لسان العرب .الجزء الثاني، مؤسسة الأعلمي للمطبوعات، بيروت، ٢٠٠٥.
٢. أردبيلى، محمد على .حقوق جزاى عمومى .جلد اول، انتشارات ميزان، تهران، ١٣٨٠.
٣. بدوي، أحمد زكي .معجم مصطلحات العلوم الاجتماعية .مكتبة لبنان، بيروت.
٤. البركتي، محمد عميم المجددي، ٢٠٠٩، التعريفات الفقهية معجم يشرح الالفاظ المصطلح عليها بين الفقهاء والأصوليين وغيرهم من علماء الدين، دار الكتب العلمية، بيروت.
٥. البقمي، ناصر بن محمد، ٢٠٠٨، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، دبي.
٦. بن زكريا، ابن الحسين أحمد بن فارس .معجم مقاييس اللغة .الدار الإسلامية، لبنان، ١٩٩٠.
٧. بن يونس، عمر محمد ابو بكر، ٢٠٠٤، الجرائم الناشئة عن استخدام الانترنت الاحكام الموضوعية والجوانب الاجرائية، ط١، القاهرة، دار النهضة العربية.
٨. بوگانسكى ميتكو؛ پترسكى دريژ .تروريسم سايبرى تهديد عليه امنيت جهانى .ترجمة ندا نيازمند، انتشارات نگاه بينه، تهران، ١٣٩٤.
٩. الجابري، إسراء طارق جواد كاظم .الإرهاب الإلكتروني .مطبعة العاني، بغداد، ٢٠١٧.
١٠. جعفر، علي عبود .جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة .منشورات زين الحقوقية، بيروت، ٢٠١٣.
١١. حجازي، عبد الفتاح بيومي، ٢٠٠٧، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر.
١٢. حسن، سعيد عبد اللطيف، ٢٠٠١، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر.

١٣. الحنفي، محب الدين أبي فيض السيد محمد مرتضى الزبيدي .تاج العروس من جواهر القاموس .دار الفكر، بيروت، ١٩٩٤.
١٤. الرازي، أبو بكر .مختار الصحاح .دار الكتب العلمية، بيروت، ١٩٩٤.
١٥. ربايعة، عبد اللطيف محمود، ٢٠١٦، الجرائم الإلكترونية التجريم والملاحقة والإثبات، مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية، نابلس.
١٦. الزمخشري، جار الله .اساس البلاغة .دار صادر، بيروت، ١٩٧٩.
١٧. الزيات، أحمد وآخرون .المعجم الوسيط .مؤسسة الصادق للطباعة والنشر، طهران، ٢٠٠٧.
١٨. عبد الرحمن، سامي جاد واصل .إرهاب الدولة في إطار القانون الدولي العام .منشأة المعارف، الإسكندرية، ٢٠٠٣.
١٩. عبد الملك، عماد مجدي .جرائم الكمبيوتر والإنترنت .دار المطبوعات الجامعية، مصر، ٢٠١١.
٢٠. عز الدين، أحمد جلال .الإرهاب والعنف السياسي .دار الحرية، القاهرة، ١٩٩٨.
٢١. عمر، سامان فوزي، ٢٠٠٧، المسؤولية المدنية للصحفي دراسة مقارنة، ط١، عمان، دار وائل للتوزيع والنشر.
٢٢. عميد، حسن .فرهنگ لغت عميد .انتشارات أشجع، ١٣٨٩.
٢٣. غياض، وسام، ٢٠٠٥، سلطات التحقيق، مركز الأبحاث والدراسات في المعلوماتية القانونية.
٢٤. الفرحان، محمد أحمد محمد .الجرائم الإلكترونية .دار وائل للنشر والتوزيع، ٢٠١٧.
٢٥. فضل، سليمان أحمد .المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام الإنترنت .دار النهضة العربية، القاهرة، ٢٠١٣.
٢٦. فضل، سليمان أحمد، ٢٠٠٧، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت، دار النهضة العربية، القاهرة
٢٧. القاسم، شادي محمود حسن، ٢٠٠٧، دور النشر الالكتروني في المكتبات ومراكز المعلومات الانترنت – المعلومات، د ط، عمان، دار الضياء للنشر والتوزيع.
٢٨. القدسي، بارعة، ٢٠١٠، أصول المحاكمات الجزائية، الجزء الثاني، منشورات جامعة دمشق، سورية.
٢٩. كافي، مصطفى يوسف .جرائم الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني .مكتبة المجتمع العربي، الأردن، ٢٠١٤.
٣٠. الكواري، محمد علي أحمد، ٢٠٠٧، مسرح الجريمة ودوره في كشف غموض الجريمة، مكتبة جامعة نايف العربية للعلوم الأمنية الرياض، السعودية.
٣١. گركى، ماركو .جرايم سايبرى راهنمايى براى كشورهاى در حال توسعه .ترجمة مرتضى اكبرى، نيروى انتظامى ايران، ١٣٨٩.
٣٢. مسعود، جبران .معجم الرائد .دار العلم للملايين، بيروت، ١٩٩٠.
٣٣. المصري، عبد الصبور عبد القوي علي، ٢٠١٢، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض.
٣٤. مصيلحي، محمد الحسيني .الإرهاب مظاهره وأشكاله وفقاً للاتفاقية العربية لمكافحة الإرهاب.
٣٥. المهدي، السيد، ١٩٩٣، مسرح الجريمة ودلالته في تحديد شخصية الجاني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
٣٦. ميلر لورا، ١٣٩٤، فضاى سايبرى ترجمه فاطمه قره باقى، تهران: انتشارات سبزان.
٣٧. هاشمي، حسين .الإرهاب بين الفقه الاسلامي والقانون الدولي .ترجمة رعد الحجاح، مركز الحضارة، بيروت، ٢٠١٤.
٣٨. اليماني، محمد بن محمد بن عبد الجبار السماوي .الموسوعة العربية .دار الأدب، بيروت، ١٩٨٩.

ثانيا: المجلات والدوريات

٣٩. البشري، محمد أمين، ٢٠٠٠، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة.
٤٠. توسلى نائينى، منوچهر؛ محسن پور، سميرا .بررسى سير تحول توسل به زور عليه تروريسم بين المللى .مجلة مطالعات حقوقى دانشگاه شيراز، ١٣٩٣.

٤١. حسینی، سید حسین؛ شایگان فرد، مجید؛ عرفانی، عطا .فرآیند تحقیقات جنایی و کشف جرم .فصلنامه دانش انتظامی خراسان رضوی، ١٣٩٢.

٤٢. رضوی، محمد .جرایم سایبری و نقش پلیس .فصلنامه دانش انتظامی، ١٣٨٦.

٤٣. الشكري، عادل يوسف عبد النبي، ٢٠٠٨، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العراق، جامعة الكوفة، كلية القانون، مجلة جامعة الكوفة، العدد٧.

٤٤. شلبي، كريم مزعل .مفهوم الإرهاب دراسة في القانون الدولي والداخلي .مجلة أهل البيت، جامعة الكربلاء، ٢٠١٦.

٤٥. صبح خیز، رضا .چالش های حقوقی جرایم سایبری .فصلنامه پژوهش های اطلاعاتی و جنایی، ١٣٩٤.

٤٦. طارمی، محمد حسین، ١٣٨٧، فضای سایبر آسیبها ومخاطرات مجله راه آورد نور، بهار ١٣٨٧، شماره ٢٢.

٤٧. گلستانی، محمود؛ پهلوانی، محمدتقی؛ عبدالله پور، مهدي .چالش ها و فرصتهای جرم شناسی سایبری. فصلنامه دانش انتظامی سمنان، ١٣٩١.

٤٨. وطنی، امیر؛ اسدی، حمید .سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری .پژوهشنامه حقوق اسلامی، ١٣٩٥.

٤٩. وهيب، مشتاق طالب .مفهوم الجريمة المعلوماتية .مجلة العلوم القانونية والسياسية، جامعة ديالي، ٢٠١٤.

ثالثا: الرسائل والأطروحات

٥٠. آمال، قارة .الجريمة المعلوماتية .رسالة ماجستير، جامعة الجزائر، ٢٠٠١.

٥١. جمال، براهيمي .التحقيق الجنائي في الجرائم الإلكترونية .رسالة دكتوراه، جامعة مولود معمري، الجزائر، ٢٠١٨.

٥٢. صبح خیز، رضا .بررسی تطبیقی جرایم سایبری .رسالة ماجستير، جامعة آزاد اسلامی، مراغه، ١٣٩١.

٥٣. علي، هدى طلب، ٢٠١٢، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية الحقوق، العراق.

٥٤. فيصل، بدري، ٢٠١٨، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه، جامعة الجزائر، بن يوسف بن خدة.

٥٥. محمود، ضيف، ٢٠١٤، المساس بحقوق المؤلف في القانون الدولي الخاص، إطروحة دكتوراه في الحقوق الجزائر، جامعة الجزائر ط١.

٥٦. يحي، فاطمة الزهراء، ٢٠١٤، إجراءات التحقيق في الجريمة الإلكترونية، شهادة ماستر، جامعة المسيلة الجزائر.

رابعا: المواقع الإلكترونية

٥٧. مطر، علي .الإرهاب الإلكتروني في القانون الدولي .مقال منشور، ٠١٣ https://www.inbaa.com

٥٨. صدیق بنای هلن؛ سایبر اسپیس پایگاه اینترنتی آفتاب www.aftab.ir مورخ ١٣٩١/١٢/٢٣.

خامسا: المصادر الاجنبية

59. **Bassiouni, M. Cherif.** A Policy-Oriented Inquiry into the Different Forms and Manifestations of International Terrorism. 1988.

هوامش البحث

[١] . أبن منظور، محمد بن مكرم، ٢٠٠٥، لسان العرب الجزء الثاني، ط ١، مؤسسة الاعلمي للمطبوعات، بيروت، ص ١٥٩٥ – ١٥٩٦.

[٢] . الرازي، ابو بكر، ١٩٩٤، مختار الصحاح، ط١، دار الكتب العلمية، بيروت، ص ١٦٩.

[٣] . الزمخشري، جار الله، ١٩٧٩، اساس البلاغة، ط ١، دار صادر، بيروت، ص ٣٦١

[٤] . اليماني، محمد بن محمد بن عبد الجبار السماوي، ١٩٨٩، الموسوعة العربية، ط١، الجزء الثاني، دار الادب، بيروت، ص ١٩٠.

[٥] . بن زكريا، ابن الحسين احمد بن فارس، ١٩٩٠، معجم مقاييس اللغة، د. ط، الجزء الثاني، الدار الاسلامية، لبنان، ص ٤٤٧

[٦] . الحنفي، محب الدين أبي فيض السيد محمد مرتضى الواسطي الزبيدي، ١٩٩٤، تاج العروس من جواهر القاموس، د. ط، الجزء الثاني، دار الفكر، بيروت، ص ٤٣.

[٧] . عز الدين، أحمد جلال، ١٩٩٨، الإرهاب والعنف السياسي، دار الحرية القاهرة، ص ٢١.

[٨] . مسعود، جبران، معجم الرائد، ط١، دار العلم للملايين، بيروت، ١٩٩٠، ص ٨٨

[٩] . الزيات، أحمد واخرون، ٢٠٠٧، المعجم الوسيط، ط٦، مجمع اللغة العربية الجزء الثاني، مؤسسة الصادق للطباعة والنشر، طهران، ص ٣٧٦

[١٠] . سورة البقرة، الآية: ٤٠

[١١] . مصيلحي، محمد الحسيني، الإرهاب مظاهره واشكاله وفقاً للاتفاقية العربية لمكافحة الإرهاب، بدون ناشر وتاريخ، ص ٩.

[١٢] . بدوي، أحمد زكي، معجم مصطلحات العلوم الاجتماعية، مكتبة لبنان بيروت، د.ط، وتاريخ، ص ١٨٢

[١٣] . الرواشدة، محمد سلامة، ٢٠١٠، أثر قوانين الإرهاب على الحرية الشخصية، د. ط دار الثقافة للنشر والتوزيع، عمان، الأردن، ص ٥١.

[14] . Bassiouni Mch, 1988, a policy Oriented inquiry into the Defferent Froms and Maninfestation inter ational Terrorism. P 16.

[١٥] . عبد الرحمن، سامي جاد واصل، ٢٠٠٣، إرهاب الدولة في إطار القانون الدولي العام د.ط، منشأة المعارف، الإسكندرية، ص ٥٠.

[١٦] . هاشمي، حسين، ٢٠١٤، الإرهاب بين الفقه الاسلامي والقانون الدولي، ط١، ترجمة رعد الحجاح مركز الحضارة للتنمية والفكر الاسلامي، سلسلة الدراسات الحضارية، بيروت، ص ٤٥

[١٧] . توسلى نائينى، منوچهر محسن پور سميرا، ١٣٩٣، بررسى سير تحول توسل به زور عليه تروريسم بين المللى از ديدگاه حقوق بين الملل و رويه قضايى بين المللى، مجله مطالعات حقوقى دانشگاه شيراز دوره ششم شماره ٣، ص ٣١١

[١٨] . الربيعي، نبأ نزار، مخاطر الإرهاب الإلكتروني وسبل مكافحته، مقال منشور http://law.uobabylon.eduliq ، ٢٠١٧.

[١٩] . عبد الصادق، عادل، ٢٠١٣، الإرهاب الإلكتروني نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، مصر، ص ٢.

[٢٠] . مطر، علي، الإرهاب الإلكتروني في القانون الدولي، نوع جديد لم يتم التعامل معه بعد، مقال منشورة في مواقع أنباء الإخبارية، http://www.inbaa.com ، ٢٠١٣.

[٢١] . بوگانسكى ميتكو؛ پترسكى دريژ، ١٣٩٤، تروريسم سايبرى تهديد عليه امنيت جهانى» ترجمه ندا نيازمند مجموعه مقالات تروريسم شناسى (رويكرد حقوقى فلسفى، چاپ اول تهران انتشارات نگاه بينه، ص ٢٥٠.

[٢٢] . المادة ٣: على كل من يعلم بالجرائم المنصوص عليها في هذا القانون إبلاغ الجهات الإدارية والأمنية والقضائية المختصة في أسرع وقت ممكن، وإلا حُكم عليه بالعقوبة التعزيرية من الدرجة السابعة.

[٢٣] . الفرجان، محمد أحمد محمد، ٢٠١٧، الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، ص ١٧٣.

[٢٤] . شلبي، كريم مزعل، ٢٠١٦، مفهوم الإرهاب دراسة في القانون الدولي والداخلي، مجلة أهل البيت، جامعة الكربلاء، بغداد، العراق، العدد ٤، ص ٥٤.

[٢٥] . وهيب، مشتاق طالب، ٢٠١٤، مفهوم الجريمة المعلوماتية ودور الحاسب الآلي بارتكابها، مجلة العلوم القانونية والسياسية، جامعة ديالي، بغداد، العراق، العدد ١، ص ٣٣٢.

[٢٦] . جعفر، علي عبود، ٢٠١٣، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، لبنان، ص ٧٣.

[٢٧] . الجابري، إسراء طارق جواد كاظم، ٢٠١٧، الإرهاب الإلكتروني، مطبعة العاني، بغداد، العراق، ص ٢٤.

[٢٨] . عبد الملك، عماد مجدي، ٢٠١١، جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار المطبوعات الجامعية، مصر، ص ٢٧.

[٢٩] . كافي، مصطفى يوسف، ٢٠١٤، جرائم (الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية، الطبعة الأولى، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ص ١٤٣.

[٣٠] . ابن منظور، أبي الفضل جمال الدين محمد بن مكرم، لسان العرب، المجلد الثالث، مدر سابق، ص ١٥٧.

[٣١] . الرازي، محمد بن أبي بكر بن عبد القادر، مختار الصحاح، مصدر سابق، ص ٤٩٨.

[٣٢] . الفراهيدي، الخليل بن أحمد، كتاب العين، ط ١، مكتبة لبنان ناشرون، بيروت، ٢٠٠٤، ص ٦٢٩.

[٣٣] . ابن منظور، محمد بن مكرم بن علي أبو الفضل جمال الدين، لسان العرب، باب الفاء، ج ١٠، مصدر سابق، ص ٢٣٢

[٣٤] . البركتي، محمد عميم المجددي، ٢٠٠٩، التعريفات الفقهية معجم يشرح الالفاظ المصطلح عليها بين الفقهاء والأصوليين وغيرهم من علماء الدين، دار الكتب العلمية، بيروت، ص ١٦٣.

[٣٥] . عمر، سامان فوزي، ٢٠٠٧، المسؤولية المدنية للصحفي دراسة مقارنة، ط١، عمان، دار وائل للتوزيع والنشر، ص ٢٢٤

[٣٦] . صديق بناى هلن؛ سايبر اسپيس پايگاه اينترنتى آفتاب www.aftab.ir مورخ ١٣٩١/١٢/٢٣.

[٣٧] . طارمى، محمد حسين، ١٣٨٧، فضاى سايبر آسيبها ومخاطرات مجله راه آورد نور، بهار ١٣٨٧، شماره ٢٢، ص ٢٣.

[٣٨] . القاسم، شادي محمود حسن، ٢٠٠٧، دور النشر الالكتروني في المكتبات ومراكز المعلومات الانترنت – المعلومات، د ط، عمان، دار الضياء للنشر والتوزيع، ص ١٩٩

[٣٩] . بن يونس، عمر محمد ابو بكر، ٢٠٠٤، الجرائم الناشئة عن استخدام الانترنت الاحكام الموضوعية والجوانب الاجرائية، ط١، القاهرة، دار النهضة العربية، ص ٣٨.

[٤٠] . القاسم، شادي محمود حسن، دور النشر الالكتروني في المكتبات، مصدر سابق، ص ١٩٩

[٤١] . محمود، ضيف، ٢٠١٤، المساس بحقوق المؤلف في القانون الدولي الخاص، إطروحة دكتوراه في الحقوق الجزائر، جامعة الجزائر ط١، ص ٨١

[٤٢] . ميلر لورا، ١٣٩٤، فضاى سايبرى ترجمه فاطمه قره باقى، تهران: انتشارات سبزان، ص ٧٨.

[٤٣] . علي، هدى طلب، ٢٠١٢، الإثبات الجنائي في جرائم الإنترنت والاختصاص القضائي دراسة مقارنة، رسالة ماجستير، جامعة النهرين، كلية الحقوق، العراق، ص ٦٩.

[٤٤] . حجازي، عبد الفتاح بيومي، ٢٠٠٧، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، ص ١٩٢.

[٤٥] . المصري، عبد الصبور عبد القوي علي، ٢٠١٢، المحكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، ص ٢٧٣.

[٤٦] . فضل، سليمان أحمد، ٢٠٠٧، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت، دار النهضة العربية، القاهرة، ص ٩٠

[٤٧] . المهدي، السيد، ١٩٩٣، مسرح الجريمة ودلالته في تحديد شخصية الجاني، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ص ٦٦.

[٤٨] . الكواري، محمد علي أحمد، ٢٠٠٧، مسرح الجريمة ودوره في كشف غموض الجريمة، مكتبة جامعة نايف العربية للعلوم الأمنية الرياض، السعودية، ص ٤٤.

[٤٩] . ونذكر هنا إلى أن مشروع الجرائم المعلوماتية في العراق ٢٠١١ أجاز للقاضي المختص الاستعانة بالخبير الفني، حيث نصت المادة ٢٦/ ثالثا (أنه للخبير أن يقدم مستخرجات النسخ الإلكترونية بصورة ورقية ويرفق معها تقرير تفصيلي بتاريخ إجراء عملية الاسترجاع الورقي)، ونصت المادة ٢٥/ رابعا (إنه للقاضي المختص في مرحلتي التحقيق والمحاكمة الاستعانة بالخبرة الفنية من داخل العراق وخارجه).

[٥٠] . السرحاني، محمد بن نصير، مهارات التحقيق الجنائي والفني في جرائم الحاسوب والإنترنت، دراسة مسحية على ضباط الشرطة في المنطقة الشرقية، مصدر سابق، ص ٨١.

[٥١] . فضل، سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت، مصدر سابق، ص ١١١.

[٥٢] . حسن، سعيد عبد اللطيف، ٢٠٠١، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، ص ١٢٩.

[٥٣] . السرحاني، محمد بن نصير، مهارات التحقيق الجنائي والفني في جرائم الحاسوب والإنترنت، دراسة مسحية على ضباط الشرطة في المنطقة الشرقية، مصدر سابق، ص ٨٤.

[٥٤] . المصري، عبد الصبور عبد القوي علي، المحكمة الرقمية والجريمة المعلوماتية، مصدر سابق، ص ٣٤٥.

[٥٥] . فيصل، بدري، ٢٠١٨، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، رسالة دكتوراه بن يوسف بن خدة، ص ١٢.

[٥٦] . المصري، عبد الصبور عبد القوي علي، المحكمة الرقمية والجريمة المعلوماتية، مصدر سابق، ص ٣٤٦.

[٥٧] . القدسي، بارعة، ٢٠١٠، أصول المحاكمات الجزائية، الجزء الثاني، منشورات جامعة دمشق، سورية، ص ١٣٠.

[٥٨] . العفيفي، يوسف خليل يوسف، الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة، مصدر سابق، ص ١٠٢.

[٥٩] . غياض، وسام، ٢٠٠٥، سلطات التحقيق، مركز الأبحاث والدراسات في المعلوماتية القانونية، ص ٥٤.

[٦٠] . مشموشي، عادل، جرائم المعلوماتية وتحدياتها، مصدر سابق، ص ٣٠٠.

[٦١] . فيصل، بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، مصدر سابق، ص ٢٣.

[٦٢] . مشموشي، عادل، جرائم المعلوماتية وتحدياتها، مصدر سابق، ص ٣٠٣.

[٦٣] . الشكري، عادل يوسف عبد النبي، ٢٠٠٨، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العراق، جامعة الكوفة، كلية القانون، مجلة جامعة الكوفة، العدد٧، ص ١٢٢.

[٦٤] . ربايعة، عبد اللطيف محمود، ٢٠١٦، الجرائم الإلكترونية التجريم والملاحقة والإثبات، مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية، نابلس، ص ٢٧.

[٦٥] . يحي، فاطمة الزهراء، ٢٠١٤، إجراءات التحقيق في الجريمة الإلكترونية، شهادة ماستر، جامعة المسيلة الجزائر، ص ٦٥.

[٦٦] . البقمي، ناصر بن محمد، ٢٠٠٨، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، دبي، ص ٢٣.

[٦٧] . البشري، محمد أمين، ٢٠٠٠، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، ، ص ١٠٧

[٦٨] . جمال، براهيمي، ٢٠١٨، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، جامعة مولود معمري، تيزي وزو، الجزائر، ص ٢٢٣.

[٦٩] . آشوری، محمد، ١٣٨۶ مقدمه ای بر کتاب جرایم رایانه ای و اینترنتی جلوه ای نوین از بزهکاری چاپ دوم تهران: انتشارات بهنام، ص٦٦.

[٧٠] . اردبیلی، محمد علی، ١٣٨٠ حقوق جزای عمومی جلد اول، چاپ دوم تهران انتشارات میزان، ص٨٨.

[٧١] . جلالی، علی اکبر، ١٣٩١، رفتارشناسی مجرمان در فضای سایبر، فصلنامة کاراگاه، سال ششم شماره ٢١، صص ١١.

[٧٢] . حسینی سید حسین شایگان فرد مجید و عرفانی عطا، ١٣٩٢، فرآیند تحقیقات جنایی و کشف جرم توسط پلیس ایران با نگاهی به حقوق انگلستان و آمریکا، فصلنامه دانش انتظامی خراسان رضوی سال پنجم شماره ٢١، صص ١١٩.

[٧٣] . عمید، حسن، ١٣٨٩، فرهنگ لغت عمید سرپرست ویرایش فرهاد قربان زاده انتشارات أشجع، ص٨١.

[٧٤] . باقری اصل، رضا، ١٣٨۴، کنوانسیون جرایم سایبر و گزارش توجیهی آن گروه ارتباطات و فناوری های نوین گروه کارشناسان کمیسیون حقوقی و قضایی مجلس شماره ٧۶۴۶، ص ٧.

[٧٥] . گلستانی محمود پهلوانی محمدتقی و عبدالله پور مهدی (١٣٩١) چالش ها و فرصتهای پیش روی جرم شناسی سایبری فصل نامه دانش انتظامی سمنان سال دوم شماره ششم، ص ١٠۶.

[٧٦] . صبح خیز، رضا، ١٣٩٤، چالش های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران، فصلنامه پژوهش های اطلاعاتی و جنایی ، سال ١٠، شماره ٣، ص١٢.

[٧٧] . وطنی، امیر و اسدی، حمید، ١٣٩٥، سیاست جنایی جمهوری اسالمی ایران در جرائم سایبری با تأکید بر ویژگ یهای خاص این جرائم، پژوهشنامه حقوق اسالمی ، سال ١٧، شماره ١، ص٥٥.

[٧٨] . گرکی مارکو ، ١٣٨٩، جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری تهران نیروی انتظامی جمهوری اسلامی ایران، ص٧٧

[٧٩] . زیبر اولریش،١٣٩٠، جرایم رایانه ای ترجمه محمد علی نوری رضا نخجوانی و مصطفی بختیاروند و احمد رحیمی تهران انتشارات گنج دانش، ص٧١.

[٨٠] . فضل، سليمان أحمد، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، الإنترنت، 2013، ص ١٢١.

[٨١] . صفاء كاظم غازي الجياشي، جريمة قرصنة البريد دراسة مقارنة، مرجع سابق، ص ٨٨.

[٨٢] . آمال، قارة، ٢٠٠١، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، كلية الحقوق، الجزائر، ص ٣٣.