جرائم الإرهاب الإلكتروني وسبل التصدي لها

The Cyberterrorism Crimes and Ways to Confront Them

سيروان شكر سمين
مدرس المساعد
جامعة كرميان– قسم القانون

sirwan shukr samin
Assistant Lecturer
Garmian University-
Department of Law

sirwan.shukr@garmian.edu.krd

الكلمات المفتاحية: الإرهاب الإلكتروني، الحاسب الآلي، مكافحة الجريمة.
Keywords: cyber terrorism, computer, crime control.

الملخص

إن أكثر الجرائم الارهابية اليوم ترتكب بواسطة الإنترنيت إذ أضحى الفضاء المجازي المسرح المفضل للإرهابيين لتنفيذ مآربهم الإجرامية، وبما أن الإنترنيت تلغي الحدود بين الدول لذلك إن جرائم الإرهاب الإلكتروني تحظى بإهتمام واسع لدى المجاميع الإرهابية وبإمكانهم الوصول عن طريق زر الكومبيوتر إلى بلدان تبعد عنهم آلاف الكيلومترات والتدخل في أنظمة الاتصالات والماء والكهرباء وباقي مجالات الحياة الأخرى وخلق حالة من الفوضى.

ومن ناحية أخرى فإن التصدي لهذه الجرائم ليس بالسهل وذلك لخصوصيتها وتمتع مرتكبها بخبرة فائقة، يجعل من الصعب على الأجهزة التنفيذية كشفها بالوسائل التقليدية، وصعوبة جمع الأدلة والإثبات في هذا المجال لأن الجريمة ذات صبغة غير مادية، وهو ما يتطلب إعداد الكادر اللازم والمتسلح بخبرة علمية خارقة، وخاصة إذا ما علمنا قصور نصوص التجريم التقليدية على مسايرة جرائم الإرهاب الإلكتروني، مما يستوجب تعديل القوانين النافذة لمسايرة التطور الهائل في مجال البرمجيات.

تهدف هذه الدراسة إلى التعرف على جرائم الإرهاب الإلكتروني باعتبارها الخطر الحقيقي التي تستهدف المجتمع، وسنحاول أن نبين ماهيتها وخصائصها والاسباب الدافعة لإرتكابها وصورها وكذلك بيان كيفية التصدي لها والصعوبات التي تواجهها، وتوضيح الطرق القانونية والفنية للإجهزة الامنية لمكافحتها، مع بيان الدور الهام الذي تقوم بها الجامعات في رفد الأجهزة الأمنية بخبرات عن طريق الدورات العلمية، ودورها في توعية المجتمع بخطورة هذه الجرائم على السلم المجتمعي برمته، ونبذ التطرف بجميع أشكاله.

Abstract

Since the Internet removes international borders, it has become the preferred venue for terrorists to carry out their criminal objectives. As a result, the majority of terrorist crimes are now committed online, and terrorist groups are very interested in cyber terrorism crimes because they allow them to enter countries thousands of kilometers away and interfere with water, electricity, and other critical infrastructure.

On the other hand, dealing with these crimes is challenging because of their specificity and the perpetrator's superior experience, making it challenging for executive agencies to detect them using conventional methods. Additionally, because the crime is of a non-material nature, gathering evidence and proof in this area is challenging and necessitates the preparation of the necessary staff with extraordinary scientific experience. This is particularly true if we are aware of how inadequate the techniques employed to gather information and proof in this area are.

This study aims to identify cyber-terrorism crimes as the real threat targeting society. We will try to explain what they are, their characteristics, the reasons they are committed, and their images, as well as a statement of how to address them and the challenges they face, and to clarify the legal and technical methods of the security services to combat them. We also highlight the significant role that universities play in providing the security services with experienced personnel.

المقدمة

أصبحت إشكالية الجريمة الإرهابية الإلكترونية واحدة من القضايا الأكثر تعقيداً في السنوات الاخيرة في العقدين الماضيين، ولم تعد هذه الجرائم يقتصر إرتكابها على دولة أو أقليم بعينها بل أمتدت لتشمل جميع الدول وفي مختلف بقاع العالم، ومن ما لاشك فيه أن المجاميع الإرهابية أستطاعت توظيف التقدم الحاصل في مجال التكنولوجيا لتحقيق مآربهم الإجرامية على نطاق واسع في مختلف بقاع المعمورة، وتعد الجريمة الارهابية الإلكترونية من أخطر الجرائم قياساً على الجرائم التقليدية لأنه يتم إرتكابها عن طريق زر الكومبيوتر وهو ما جعل تنفيذ الجريمة أمراً سهلاً ارتكابه وجعل من الصعب رصد الجاني فيها وتتبعه وإلقاء القبض عليه وذلك لسهولة التمويه والتخفي وتغير الهوية وبسرعة قياسية، ويتضح خطورتها أيضاً من خلال فداحة وجسامة الخسائر التي يمكن أن تسببها عملية واحدة، ولذلك اصبح الفضاء المجازي في عالم الرقميات والبرمجيات المسرح المفضل للإرهابيين لتنفيذ جرائمهم والحاق ضرر كبير بالدول، فمن الممكن تهديد الاقتصاد عن طريق اقتحام البورصة الاقتصادية وكذلك يمكن تهكير واختراق أنظمة الاتصالات، الماء، الكهرباء، قطاع النقل وباقي القطاعات الضرورية للحياة، وبذلك بإمكانهم تهديد بلد برمته، وهذا لاشك فيه الفرصة والمكان المناسب لهم للتحكم في المنظومات المتصلة بحياة المواطنين عن طريق إغلاقها والسيطرة التامة عليها.

وبما أن العراق من الدول التي كانت الضحية الأولى لهذا النوع من الجرائم الإرهابية في الماضي والحاضر وربما في المستقبل، ولذا تناولت بالدراسة جريمة الإرهاب الإلكترونية، وبيان طرق مكافحتها من الناحية الفنية وكذلك من الناحية القانونية سواء باصدار التشريعات اللازمة لمواجهتها أو بتشكيل هيئة تنفيذية مدربة ومسلحة بأحدث الاجهزة والتقنيات الضرورية لممارسة عملهم، وكذلك بيان الدور الفعال للجامعات بالمشاركة في مكافحة هذه الجريمة الخطرة سواء برفد الاجهزة الامنية بخبرة كوادرها من خلال إقامة دورات تأهيلية لهم أو عن طريق نشر التوعية اللازمة لنبذ العنف والارهاب ونشر فكر التسامح.

أهمية الدراسة:

تأتي أهمية هذه الدراسة من أن جريمة الإرهاب الإلكتروني أشد أنواع الجرائم التي ترتكب عبر شبكة الإنترنيت خطورة، ويتضح هذا واضحاً من خلال النظر إلى فداحة الخسائر التي يمكن أن تسببها عملية واحدة. وتعتبر جريمة الارهاب بأستخدام الوسائل التقنية والبرمجية من الجرائم الخطيرة وذات تكلفة باهظة، كونها تهدف إلى الإخلال بالامن والنظام العام في المجتمع، ولا يشترط في هذا النوع من الجرائم تحقيق النتيجة الجرمية لهذه الجريمة كونها من جرائم الخطر.

وتأتي أهمية دراسة جرائم الإرهاب الإلكتروني في توعية الافراد والمجتمع في الوسائل والطرق التي تلجأ إليها التنظيمات لهكذا جرائم، وللدور الذي يجب أن تضطلع به الدول والجماعات والأفراد للتصدي لهذه الآفة ومكافحتها.

مشكلة الدراسة:

تتمحور مشكلة الدراسة في التطورات العلمية الكبيرة في مجال تقنيات المعلومات والبرمجيات ولتطور الهائل لأنواع الجرائم المرتبطة بتطور تكنولوجيا المعلومات، ولسرعة تنفيذ هذا النوع من الجرائم وتعقيدها وصعوبة ضبط مرتكبها واثباتها، ولقدرة الجناة على التخفي ومسح جميع الأدلة في مسرح الجريمة، ولتجاوز هذه الجريمة الحدود العابرة للدول بل عابرة للقارات ولخطورتها ولحجم الخسائر التي تلحقها بالمجتمعات، ومن ثم كان من الضروري دراسة هذا النوع من الجرائم وبيان مدى كفاية الطرق المتبعة من قبل الأجهزة الأمنية لمكافحتها، وبيان النصوص القانونية التي تعالج الموضوع. وعليه تتجسد إشكالية هذه الدراسة، في تساؤل رئيس تتركز في الاجابة على التساؤل الآتي: **كيف واجه المشرع العراقي الجريمة الإرهابية المرتكبة عن طريق الوسائل الإلكترونية؟**

وتتفرع عن هذا السؤال أسئلة أخرى فرعية ومنها:

١. ماهي العقوبات المقررة للجريمة الإرهابية الإلكترونية في التشريع العراقي ؟
٢. وما هي الطرق القانونية لمكافحة هذه الجريمة؟
٣. وما هي الطرق الفنية لمكافحة هذه الجريمة؟
٤. وهل بإمكان جامعاتنا القيام بدورها في مكافحة هذه الجريمة؟

فرضية الدراسة: في ظل تساؤلات المشكلة تنطلق الدراسة من فرضيتين هما:

١. عدم وجود نصوص تشريعية واضحة وكافية لتغطية جرائم الإرهاب الإلكتروني، وعدم وجود قانون واضح المعالم يتعلق بهذه الطائفة من الجرائم.

٢. إبراز العلاقة الطردية بين التصدي لجرائم الإرهاب الإلكتروني وبين تحقيق أعلى مستويات للأمن على مستوى الوطني والدولي.

منهج الدراسة:

إتبعنا في دراسة بحثنا (مكافحة جريمة الإرهاب الإلكتروني) المنهج التأصيلي التحليلي، ومن خلال هذا المنهج قمنا بشرح وتحليل عناصر ومقومات ودوافع وصور جريمة الإرهب الإلكتروني والاحكام الخاصة بها، وبيان الطرق القانونية والفنية لمكافحة هذه الجريمة.

هيكلية البحث:

سيتم تقسيم البحث الى مبحثين إضافة الى المقدمة والخاتمة، في المبحث الاول سنتناول ماهية جريمة الارهاب الإلكتروني من خلال ثلاثة مطالب، في المطلب الاول سنتوقف لبيان مفهوم جرائم الإرهاب الإلكتروني، وفي المطلب الثاني سنبين أهم خصائص جرائم الإرهاب الإلكتروني وأهدافها، وفي المطلب الثالث سنتناول بالدراسة أهم أسباب جرائم الإرهاب الإلكتروني وصورها، وفي المبحث الثاني سنتوقف لدراسة سبل التصدي لجرائم الإرهاب الإلكتروني في ثلاثة مطالب، ففي المطلب الاول سيرتكز على دراسة السبل الفنية للتصدي لجرائم الإرهاب الإلكترونية، بينما يعالج المطلب الثاني السبل القانونية للتصدي لجرائم الإرهاب الإلكترونية، والمطلب الثالث والأخير سيخصص لدراسة دور الجامعات في التصدي لجرائم الإرهاب الإلكتروني، وفي الخاتمة بينا اهم استنتاجاتنا وتوصياتنا.

المبحث الأول

ماهية جرائم الإرهاب الإلكتروني

إن دراسة جريمة الإرهاب الإلكتروني تتطلب منا أولاً بيان ماهية هذه الجريمة من خلال تعريفها وتوضيح خصائص هذه الجريمة التي تميّزها عن الجرائم الاخرى مع تحديد أهدافها وكذلك التوقف عند أهم الاسباب التي تدفع بالجناة إلى إرتكابها ونقل أهم صور لهذه الجريمة الخطرة، وذلك من خلال ثلاث مطالب وفق الاتي:

المطلب الأول: مفهوم جرائم الإرهاب الإلكتروني

لتوضيح مفهوم جريمة الإرهاب الإلكتروني لا بد من تعريف الإرهاب ومن ثم تعريف جريمة الارهاب الإلكتروني وكذلك بيان عناصرها، وذلك كالأتي:

الفرع الاول: تعريف الإرهاب: الإرهاب في اللغة: وأصله مأخوذ من الفعل الثلاثي رَهِبَ بالكسر، يَرْهَبُ رَهْبَةً ورُهْباً، بالضم، ورَهَباً، بالتحريك، أي خاف. واسْتَرْهَبَه: استدعى رَهْبَتَه حتى رَهِبَه الناسُ[١]، وبذلك فسر قوله عز وجل (واسترهبوهم وجاؤوا بسحر عظيم)[٢] أي أرهبوهم.

الإرهاب في الاصطلاح: لقد تباينت تعاريف الإرهاب وتبعاً لذلك تباينت الاجتهادات في شأنه ولا يوجد إلى الآن تعريفاً جامعاً مانعاً يحدد الإرهاب وذلك لتنوع أشكاله ومظاهره، وتعدد أساليب تنفيذه، واختلاف وجهات النظر السياسية والقانونية لكل بلد إلى الإرهاب. إذ عرفته منظمة التعاون الإسلامي بأنه كل فعل من أفعال العنف والتهديد به أياً كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي يهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم وأمنهم واعراضهم أو حقوقهم للخطر[٣]، وعرفته الاتفاقية العربية لمكافحة الارهاب لعام ١٩٨٨ " كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه وأغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو أمنهم أو حريتهم للخطر، أو إلحاق ضرر بالبيئة أو

---

(١) إبن منظور العربي. (٢٠٠٥). لسان العرب، المجلد الأول، منشورات مؤسسة الأعلمي للمطبوعات، بيروت، ٢٠٠٥، ص١٥٩٥.

(٢) سورة الاعراف، الاية ١١٦.

(٣) د.حسن تركي عمير وسلام جاسم عبدالله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم والسياسية، جامعة ديالى، عدد خاص المؤتمر العلمي الدولي الثاني للكلية – إشكالية التداخل بين مفهومي الإرهاب وحقوق الإنسان، ٢٠١٣، ص٣٢٣.

بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[١].

بينما عرّف قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥ في المادة الاولى منها الإرهاب بأنه كل فعل إجرامي يقوم به فرد أو جماعة منظمة فرداً أو مجموعة أفراد أو جماعات أو مؤسسات رسمية أو غير رسمية أوقع أضراراً بالممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو إدخال الرعب أو الخوف والفزع بين الناس أو إثارة الفوضى تحقيقاً لغايات إرهابية.

وفيما يخص الإرهاب الإلكتروني حيث تعددت أيضاً التعاريف التي تناولتها، ومنهم من عرفه بإنه " نشاط أو هجوم متعمد، يملك دوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام العالمي، ويستخدم الفضاء الإلكتروني بوصفه عاملاً مساعداً ووسيطاً في عملية التنفيذ الإرهابي أو الحربي. كما ويسعى لإحداث تأثير معنوي ونفسي عبر التحريض على بث الكراهية الدينية وحروب الافكار. ويأتي هذا العمل في صورة رقميّة عبر إستخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور في الفضاء الإلكتروني، وقد يقتصر تأثيرها على بعدها الرقمي، أو تتعداه لتصل إلى الإضرار بأهداف مادية تتعلق بالبنية التحتية الحيوية."[٢]، وعرف أيضاً بأنه "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادرة عن الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو في نفسه، أو في عرضه، أو في ماله، بغير حق بشتى صنوف وصور الإفساد في الأرض الذي نهت عنه الشريعة الإسلامية[٣]"، وذهب البعض الأخر منهم إلى تعريفه : بأنه الاستخدام غير الأمثل للشبكة العالمية بما يؤدي إلى ترويع المواطنين بشكل خطر، أو يسعى إلى زعزعة الأمن والاستقرار، أو تقويض المؤسسات السياسية، أو الدستورية، أو الاقتصادية، أو الاجتماعية، لإحدى الدول، أو المنظمات الدولية، عن طريق استعمال لغة التهديد

---

(١) خالد دليل محمد العازمي، جريمة الإرهاب في التشريع الكويتي، رسالة ماجستير غير منشورة، كلية الدراسات القانونية العليا، جامعة عمان العربية، سنة ٢٠٠٧، ص٢٠.

(٢) د. غادة نصار، الإرهاب والجريمة الإلكترونية، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص٧٦.

(٣) د. بن يحيى الطاهر ناعوس، مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية، بحث منشور على شبكة الألوكة، ص٦، الرابط الالكتروني: FwieUr٣http://bit.ly/، تاريخ الزيارة: ٢٠٢٣/٣/١٧.

والعدوان[١]. وعليه يمكننا تعريف الإرهاب الإلكتروني بأنه : العمل العدواني أو التهديد المادي او المعنوي الصادر من الدول أو المنظمات أو الأفراد بوسائل إلكترونية بهدف ترويع الافراد أو إجبار الحكومة على القيام بعمل أو الامتناع عن القيام بعمل ما، أو تدمير وتخريب المؤسسات الاساسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو منظمة دولية، أو زعزعة استقرارها.

الفرع الثاني: عناصر جرائم الإرهاب الإلكتروني: لا يمكن الحديث عن جريمة الإرهاب الإلكتروني إذا لم تحتوِ على الأفعال المحرّمة فيه على عناصر الإرهاب، ولكي يتحقق الإرهاب لابد من توافر العناصر التالية:

١. استخدام العنف أو التهديد باستخدام الوسائل الإلكترونية، إذ يراد بالعنف هو العدوان على الأشخاص والحكومة باستخدام الوسائل الإلكترونية، فالإرهابيون يعتمدون على استخدام وسائل الإتصالات وشبكة المعلومات من أجل تخويف الناس وإلحاق الضرر بهم وتهديدهم[٢].

٢. أن يقع العنف أو التهديد تنفيذاً لعمل فردي أو جماعي، والمقصود بالعمل الفردي أو الجماعي النية المبيتة التي يتم وضعها موضع التنفيذ، بخطة مدبرة تتم ترجمتها من خلال جهود منسقة بقصد تحقيق الهدف المنشود عبر الوسائل الإلكترونية[٣].

٣. أن يكون من شأن العنف المخطط له أو التهديد به إيقاع الرعب بين الناس وترويعهم أو تعريض أمنهم للخطر أو إلحاق الضرر بالبيئة أو المرافق العامة والأملاك العامة أو الأملاك الخاصة أو المرافق الدولية أو باحتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر.

٤. أن يكون الهدف من استعمال العنف عبر الوسائل الإلكترونية والمخطط له أو التهديد باستخدامه، هو الإخلال بالنظام العام أو تعريض سلامة المجتمع للخطر، فاستخدام

---

(١) محمد الامين البشري، التحقيق في جرائم الحاسب الألي والانترنيت، المجلة العربية للدراسات الامنية والتدريب، الرياض، ١٤٢٢هجرية، ص٢٢.

(٢) عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير مقدمة إلى كلية الحقوق جامعة تكريت، ٢٠١٩، ص١١.

(٣) محمد العفيفي، جرائم الإرهاب في التشريع المقارن، المكتبة الوطنية، الأردن، ٢٠٠٧، ص١٠٤.

العنف أو التهديد باستخدامه بتعطيل مظاهر الحياة العادية في الدولة أو زعزعة السكينة لدى الأفراد سواءً إنصب على الأفراد أو الأموال(١).

المطلب الثاني: خصائص جرائم الإرهاب الإلكتروني وأهدافها

إن لجريمة الإرهاب الإلكتروني خصائص معينة يختص بها دون غيرها من الجرائم كما وأنها تسعى إلى تحقيق جملة من الاهداف والغايات غير المشروعة، والتي سنبينها وفق الآتي:

الفرع الأول: خصائص جرائم الإرهاب الإلكتروني: للإرهاب الإلكتروني سمات وخصائص معينة مما يجعلها مختلفة تماماً عن الإرهاب التقليدي، ومن أهم هذه الخصائص:

١. عدم الحاجة في جريمة الإرهاب الإلكتروني عند إرتكابه إلى ممارسة القوة والعنف فقط يحتاج إلى توافر حاسب آلي متصل بالشبكة المعلوماتية ومجهز ببعض البرامج اللازمة.
٢. جريمة الإرهاب الإلكتروني جريمة إرهابية عابرة للحدود بل عابرة للقارات وغير خاضعة لنطاق إقليمي محدد، وترتكب في أغلب الأحوال دون الحاجة إلى الحركة والتنقل ما بين الدول.
٣. صعوبة اكتشاف جريمة الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الاجهزة الأمنية والقضائية في التعامل مع هذا النوع من الجرائم.
٤. صعوبة الإثبات في جرائم الإرهاب الإلكتروني، وذلك لإن مسرح الجريمة هي الفضاء المجازي في العالم الرقمي ولإنها تقع في بيئة إلكترونية وإن الإدلة التي تخلفها في الغالب أدلة إلكترونية مما يترتب عليه تنظيف مسرح الجريمة من قبل الجناة بسهولة وسرعة، وكل هذا بدوره يترتب عليه جملة من المشاكل والصعوبات التي تعوق إكتشاف هذه الجرائم وبالتالي التحقيق فيها.
٥. تتميز جريمة الإرهاب الإلكتروني بأنها سهلة الإرتكاب، إذ يرتكبها الجاني في كثير من الاحيان لوحده دون الحاجة للإستعانة بشخص آخر، إذ أنه قادر على تنفيذ مخططه الإجرامي لوحده وهو جالس أمام الكومبيوتر في منزله أو مكتبه أو في مقهى للإنترنيت.
٦. إن الجناة في الجرائم الإلكترونية عادة من ذوي الاختصاصات في مجال تقنية المعلومات، أو على الاقل شخص لديه قدرة وقدر كافي من المعلومات أو الخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية، ومع ذلك يمكن أن يرتكب من خلال وسائل تقنية أخرى غير الحاسب الآلي جريمته مثل جهاز الموبايل المتطور، وغيرها من الأجهزة والتقنيات التي يمكن أن تظهر إلى الوجود في أي لحظة.

(١) عمر عباس خضير العبيدي، المصدر السابق، ص١٢.

٧. جريمة الإرهاب الإلكتروني مكلفة للضحايا، فإذا كانت هذه الجرائم مربحة للجناة فإنها في ذات الوقت مكلفة للضحايا، لذا فإن لهذه الجرائم خطورة كبيرة على إقتصاديات الدول، وإن مثل هذه الخسائر تدفع الضحايا إلى النأي عن الإخبار عن هذه الجرائم، خوفاً من أن يترتب على ذلك أضرار أخرى تلحق بهم وبسمعتهم(١).

الفرع الثاني: أهداف جرائم الإرهاب الإلكتروني: تهدف جريمة الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف والغايات غير المشروعة ويمكننا بيان أهم وأبرز تلك الاهداف في ضوء النقاط التالية:

١. بث ونشر الرعب والخوف بين الاشخاص والدول والشعوب المختلفة، وأن التأثير النفسي لهذه الجريمة كبير على عامة الناس من شأنه أن يؤدي إلى عدم الثقة بالسلطة الامنية وأنها غير قادرة على حمايتهم.
٢. الإخلال بالنظام العام والأمن المعلوماتي، وزعزعة الطمأنينة، وتعريض سلامة المجتمع وأمنه للخطر، وإثارة الرأي العام.
٣. إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها والاضرار بوسائل الاتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة.
٤. تهديد السلطات العامة والمنظمات الدولية وابتزازها.
٥. الأنتقام من الاشخاص.
٦. الدعاية والاعلان وجذب الانتباه وإثارة الرأي العام.
٧. جمع الاموال والاستيلاء عليها.

المطلب الثالث: أسباب جرائم الإرهاب الإلكتروني وصورها

إن لجريمة الإرهاب الإلكتروني أسباب وصور عديدة، وهي نفس أسباب ظاهرة الإرهاب عموماً، وذلك لإن الإرهاب الإلكتروني يعد نوعاً من أنواع الإرهاب وشكلاً من أشكاله، كما أن لظاهرة الإرهاب الإلكتروني دوافع وبواعث عديدة تجعلها موضوعاً مناسباً وسلاحاً سهلاً للجماعات الخارجة على القانون، حيث سنبين أسباب وصور جريمة الإرهاب الإلكتروني وفق الآتي:

(١) رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، ٢٠١٣، ص٢٩.

الفرع الأول: أسباب جرائم الإرهاب الإلكتروني: إن تحديد اسباب جريمة الإرهاب الإلكتروني يعد أمراً ضرورياً، وإن الأسباب التي تدفع بالافراد إلى ارتكابها يمكن ردها إلى :

أولاً: الدوافع الشخصية: وتتمثل في العوامل والامراض النفسية مثل عقدة الشعور باليأس والاحباط والظلم من قبل المجتمع مما يدفع الفرد إلى الإنتقام لإحداث تغيرات جذرية والتضحية بروحه وارواح الآخرين سواء أفراد السلطة أو الاشخاص العاديين(١). وعلى المستوى الفردي تلعب العوامل النفسية دوراً في غاية الأهمية في تحديد سلوكيات الإنسان المعادي للمجتمع، وخاصة عندما تتعرض تلك الجوانب لبعض الإضطرابات والتقلبات النفسية والمرضية التي يمكن إرجاعها لاسباب وراثية أو مفاجئة فمثل هذه الجوانب النفسية قد تكون الدافع الحقيقي لإقحام الفرد في عالم الإرهاب وتلعب وسائل الإعلام دوراً كبيراً في تحفيز العوامل النفسية للفرد وتأجيج روح الإنتقام لديه وعلى الصعيد الثقافي فإن شعوب العالم وخاصة العالم النامي تعاني من الإنعكاسات السلبية التي خلقتها العولمة المتمثلة بالتبعية الثقافية وأزمة الهوية الأمر الذي أدى إلى خلق صراعات ثقافية داخل المجتمع الواحد بعضه يؤيد الإرهاب والآخر يعارضه(٢).

وقد يكون السبب الرغبة في الظهور، وحب الشهرة وإيصال فكرة بإنه ليس أقل من غيره وبإمكانه القيام بأفعال كبيرة وإن كانت مخالفة للقانون ليثبت أنه يتمتع بمؤهلات كبيرة.

ثانياً: الدوافع الاقتصادية: تساهم المشاكل التي تمر بها دول العالم الثالث في ظهور حالة من الحرمان الاقتصادي، خاصة وأن الفقر والحاجة المادية الملحة وعدم المساواة في توزيع الموارد والثروة والفوارق الكبيرة في المجتمع، كل ذلك يمثل دافعاً قوياً نحو ممارسة الإرهاب، وتوسيع القائم منه بهدف التخلص من تلك الاوضاع(٣)، إذ أن معاناة الأفراد من المشكلات الاقتصادية المتعلقة بالإسكان والديون والفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية، وعدم تحسن دخل الفرد، وانتشار البطالة في المجتمع وزيادة

---

(١) عقيلة هادي عيسى وإسراء جواد حاتم، الارهاب المعلوماتي (الرقمي) وطرق مكافحته، مجلة السياسية والدولية، كلية العلوم السياسية، الجامعة المستنصرية، العدد ١٦، لسنة ٢٠١٠، ص ١٨٣.

(٢) مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية" دراسة مقارنة بين التشريع الاردني والعراقي"، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٧، ص٢١.

(٣) مصطفى سعد حمد مخلف، المصدر السابق، ص٢١.

العاطلين عن العمل وعدم توفر فرص العمل، كل ذلك من العوامل في إنشاء روح التذمر في الأمة، وربما دفعت بعض الشباب إلى التطرف والإرهاب(١).

ثالثاً: الاسباب الفكرية للإرهاب الإلكتروني: وتتمثل في الفراغ الفكري، والفهم الخاطئ لمبادئ الدين وسوء التفسير واعتماد الشباب على بعضهم البعض دون الرجوع إلى العلماء، كما أن الفراغ الفكري والجهل بقواعد الدين والجهل بمقاصد الشريعة الإسلامية والتشدد والغلو في الفكر كلها أسباب فكرية أدت في إزدياد ظاهرة الإرهاب، كما أنها ساهمت أو ساعدت في نشوء سياسات ظالمة وقاهرة(٢).

رابعا: الأسباب الفنية: توجد عديد من الاسباب والدوافع الفنية التي يسهل إرتكابها من قبل الجناة منها ضعف قاعدة البيانات المعلوماتية وسهولة إختراقها، وبذلك يمكن للإرهابيين والمنظمات الإرهابية من الولوج إلى قاعدة بيانات البنية التحتية وتخريبها، إذ أن شبكة المعلومات تتسم بالانفتاح وعدم وجود حواجز وقيود وربما إحتوائها على ثغرات تنظيمية تسهل عملية الولوج والدخول.

ومن الاسباب الفنية أيضا صعوبة إثبات جريمة الإرهاب الإلكتروني فكثير من هذه الجرائم لا يعلم بوقوعها، وأن صعوبة الإثبات تعد من أقوى الدوافع المساعدة على إرتكاب جرائم الإرهاب الإلكتروني لأنها تعطي أملاً للمجرم في الإفلات من العقوبة، وهنا أقترح على المشرع العراقي استحداث عضو الضبط القضائي الإلكتروني وذلك بتعديل نص المادة ٣٩ من قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل وذلك بإضافة فقرة إليها باستحداث عضو الضبط القضائي الإلكتروني ويفضل أن يكون من أفراد الشرطة ومن الحاصلين على شهادات علمية في مجال التكنولوجيا والبرمجيات، وتكون مهمتهم ضبط الجرائم المعلوماتية وخاصة الإرهابية منها وإعطائهم سلطة التفتيش الإلكتروني دون موافقة قاضي التحقيق وفي حدود ضيقة وفقط لمواجهة الجرائم الإرهابية، حتى لا يحسب بأنها تضيّق الخناق على الحريات العامة، وذلك لأن الجرائم الإلكترونية تنفذ خلال مدة قصيرة والجاني يقوم بتنظيف مسرح الجريمة بسرعة، حيث يقال أن وراء كل تطور حضاري ثمة جرائم مستحدثة ومتزايدة ولابد للقانون أن يساير التفنن الكبير التي يتمتع بها المجرمون لكي يتم ضبطهم وتقديمهم للعدالة.

---

(١) إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني "دراسة مقارنة"، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة النهرين،٢٠١٢، ص٣٤.

(٢) عمر عباس خضير العبيدي، المصدر السابق، ص٢٠.

ومن الاسباب الفنية أيضاً سهولة إرتكابها وقلة تكلفتها إذ يتطلب توافر جهاز الحاسب الآلي متصل بالشبكة المعلوماتية وأحياناً يتم تنفيذها عن طريق جهاز الموبايل، فهو لا يكلف وقتاً ولا جهدا كبيراُ، ولا يحتاج إلى مصادر تمويل ضخمة.

خامساً: الدوافع السياسية: ومنها السياسات غير العادلة التي تمارسها بعض الدول ضد مواطنيها، ومنها الإحباط السياسي لأن كثيراً من الدول وقفت بوجه الجماعات السياسية وخاصة الاسلامية منها وتصدت لأربابها وحصرت نشاطاتها، ومنها أيضاً غياب العدالة الاجتماعية، وعدم المساواة في توزيع الثروة الوطنية، والتفاوت في توزيع الخدمات والمرافق الاساسية، والاستيلاء على الاموال العامة(١).

الفرع الثاني: صور جرائم الإرهاب الإلكتروني: لجرائم الإرهاب الإلكتروني صور عديدة وسنتناولها وفق الآتي:

أولاً: إختراق المواقع الإلكترونية وتدميرها: ويتمثل هذه الصورة باختراق المواقع والانظمة الإلكترونية عبر الشبكة والسطو على محتوياتها أو تغيرها أو إحداث الضرر أو حتى تدميرها لتحقيق أهداف غير مشروعة، والمقصود بالتدمير هنا: الدخول غير المشروع على نقطة إرتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال تظام آلي**(Server-pc)** أو مجموعة نظم مترابطة شبكياً**(Internet)**، بهدف تخريب نقطة الاتصال أو النظام، إذ يمكن أن يقوم الإرهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الاسواق المالية، بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات من الآثار. إذ يستطيع قراصنة الحاسب الآلي**(Hackers)** التوصل إلى المعلومات السرية والشخصية، واختراق خصوصية سرية المعلومات بسهولة، وذلك يرجع إلى التطور المذهل في عالم الحاسب الآلي والشبكة المعلوماتية يصحبه تقدم أعظم في الجرائم المعلوماتية وسبل إرتكابها، ولا سيما ان مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي. إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة وبرامج شبكة الانترنيت، وهي عملية تتم من أي مكان في العالم دون حاجة إلى وجود شخص المخترق في الدولة ألتي يتم إختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية، ولاتزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الآلي والشبكة المعلوماتية(٢).

---

(١) إسراء طارق جواد كاظم الجابري، المصدر السابق، ص٣٣.

(٢) د. سامر مؤيد عبداللطيف و د. منى محمد عبدالرزاق، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مجلة رسالة الحقوق، السنة العاشرة، العدد الثاني، ٢٠١٨، ص٥١.

ثانياً: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية: إن الشبكة المعلوماتية الدولية(الانترنيت) تتيح للمنظمات والجماعات الإرهابية نشر الافكار المتطرفة، والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراض غير مشروعة، والتي تتعارض مع مصلحة المجتمع، إذْ يستخدم الإرهابيون الشبكة الدولية للمعلومات(الانترنيت) بشكلٍ يومي لنشر أفكارهم الهدامة وتحقيق أهدافهم السيئة، ويمكن إبراز استخداماتهم للشبكة في عدة نقاط وهي كالآتي[١]:

١. **تجنيد الإرهابيين:** تستخدم الجماعات الارهابية الوسائل الإلكترونية لنشر الثقافة والترويج لنفسها، وبث أفكارها وفلسفتها، كما تسعى جاهدة إلى ضم تنظيماتها أكبر عدد من الراغبين في تبني أفكارها ومبادئها، فهذا يسهل من تجنيد الإرهابيين لتنفيذ هجمات إرهابية في المستقبل، حيث تحافظ التنظيمات الإرهابية على بقائها واستمرارها من خلال غرف الحوار والمنتديات والمواقع الإلكترونية بإسلوب عاطفي.

٢. **التدريب الإلكتروني:** يعد التدريب أهم هواجس التنظيمات الإرهابية، إذ يتم إنشاء معسكرات تدريبية سرية، لكن دائما ما تكون معرضة للخطر، ويمكن إكتشافها ومداهمتها في أي وقت، كما قامت الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وكيفية تصنيع المتفجرات والمواد الخارقة والأسلحة المدمرة[٢].

ثالثاً: التجسس الإلكتروني: هو استخدام وسائل تقنية المعلومات الحديثة لسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات، والتنصت على هذه المعلومات، أيّاً كان نوعها، حيث يأخذ أبعاداً جديدة فتعددت أهدافه من معلوماتٍ إقتصاديةٍ إلى معلومات سياسية وعسكرية وشخصية[٣]، وقد ساعدت تقنيات المعلومات والتطور التكنولوجي بتحول وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع استخدام الإنترنيت وخاصة في ظل ضعف الوسائل الأمنية المستخدمة لحماية الشبكات من التجسس. ولا يقتصر الخطر في التجسس على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحاً **(Hackers)** لأن مخاطر هؤلاء محدودة وتقتصر على العبث أو إتلاف المحتويات، وهذا يمكن التغلب عليه باستعادة نسخة أخرى مخزنة، إنما يكمن الخطر الحقيقي في عمليات التجسس التي تقوم بها

---

(١) عمر عباس خضير العبيدي، المصدر السابق، ص٢٢.

(٢) المصدر نفسه، ص٢٠.

(٣) د. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص٥٦٩.

الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة، وافشائها لدول أخرى أو استغلالها بما يضر بالمصلحة الوطنية لتلك الدولة(١).

ولا يقتصر التجسس على المعلومات العسكرية أو السياسية بل يتعداه إلى المعلومات التجارية والاقتصادية والثقافية، ويتم الاستعانة في عمليات التجسس بالأقمار الصناعية التي تصمم لالتقاط الاتصالات من خلال أجهزة كومبيوتر متطورة لتحليلها(٢)، هذا ويمكن أن نشير إلى أن طريقة التجسس الإلكتروني سوف يكون لها استخدام مكثف في المستقبل من قبل الجماعات الإرهابية لأهمية المعلومات التي تحصل عليها من المؤسسات والقطاعات الحكومية وتحديداً العسكرية والسياسية والاقتصادية وبالتأكيد إذا ما سرّبت هذه المعلومات فسوف يكون لها أثر وخطر كبير على مصلحة البلاد(٣).

رابعاً: غسيل الأموال: أثبتت الدراسات وجود علاقة بين غسيل الأموال وحركات الإرهاب والتطرف والعنف الداخلي فضلاً عن نشاط المافيا العالمية ودورها في حدوث زعزعة أمن واستقرار المجتمعات النامية في دول العالم الثالث كما تستخدم عمليات غسيل الأموال في توفير الدعم المالي وتمويل شراء السلاح اللازم للعمليات الإرهابية وذلك بالتعاون مع أجهزة متخصصة في تنظيم وإدارة الصراعات السياسية والإستراتيجية عالمياً، أضف إلى ذلك وجود علاقة وثيقة بين غسيل الأموال والإرهاب الإلكتروني يدفع الإرهابيين إلى اللجوء إلى بعض أجهزة المخابرات والتجسس واستخدام الأموال الهاربة في تأسيس منظمات إرهابية لمزاولة الأعمال غير المشروعة وتنفيذ بعض العمليات التخريبية أو التدميرية الموجهة إلى أنظمة أو حكومات معينة في مختلف الدول، عن طريق استخدام الشبكة المعلوماتية(٤).

---

(١) بدرة هويمل الزبن، الإرهاب في الفضاء الإلكتروني" دراسة مقارنة"، أطروحة دكتوراه غير منشورة، كلية القانون، جامعة عمان العربية، ٢٠١٢، ص ص١٧٧- ١٧٨.

(٢) بدرة هويمل الزبن، المصدر السابق، ص١٧٨.

(٣) د. حسن تركي عمير و سلام جاسم عبدالله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، جامعة ديالى، عدد خاص، ص٣٣٧.

(٤) إسراء طارق جواد كاظم الجابري، المصدر السابق، ص٤٦.

المبحث الثاني

سبل التصدي لجرائم الإرهاب الإلكتروني

لا يمكن لأي بلد في الألفية الثالثة أن تعيش بمعزل عن التكنولوجيا، للأنها أصبحت من أهم وسائل التواصل العالمي، وأداة ترابط والتواصل بين مختلف أنحاء بقاع المعمورة، وفي ظل هذا الترابط بين أنحاء العالم عبر تقنيات المعلومات والإتصالات والتطبيقات والتي سمحت وبسهولة مرور ونقل الافكار والمعلومات بين مستخدمي تلك التقنيات، أصبحت حماية الأفراد والمؤسسات من الامور الحتمية الملقاة على عاتق الدولة، مع إدراك الجميع للفوائد الكبيرة لتكنولوجيا المعلومات، فإن مخاطر تغلغل هذه التكنولوجيا في جميع مناحي الحياة يتطلب من الأفراد والمجتمع والدولة جميعاً للحيلولة دون حصول تلك المخاطر بجميع أشكالها، وهنا لابد للتصدي لجرائم الإرهاب الإلكتروني، وللتصدي للجرائم الإرهابية الإلكترونية سبل وطرق متعددة منها سبل قانونية عن طريق النصوص القانونية وهي الأصل وسبل فنية للتصدي لهكذا جرائم وأيضاً سبل وتدابير إجتماعية وثقافية وتدريبية تقوم بها الجامعات لمواجهة جرائم الإرهاب الإلكتروني، وسنتناولها وفق الآتي:

المطلب الأول: السبل الفنية للتصدي لجرائم الإرهاب الإلكتروني

تتخذ السبل الفنية الجانب الأهم في مجال التصدي ومكافحة جرائم الإرهاب الإلكتروني، وذلك مع عدم التقليل من شأن السبل غير الفنية للتصدي للجرائم الإرهابية الإلكترونية وخاصة السبل القانونية منها، إلا أنه في مجال التصدي ومكافحة الجرائم المعلوماتية والإرهاب الإلكتروني والذي يتم أساساً بوسائل وسبل فنية وإلكترونية، فإن قيمة هذه التدابير تظهر بشكل أكثر جلاءً، خاصة إذا ما عرفنا أن الإثبات في هكذا جرائم صعب جداً يحتاج إلى خبراء فنيين يستعين بهم القضاء لكشف الجناة. ونرى أن واجب التصدي لجرائم الإرهاب الإلكتروني والإعتداءات الإلكترونية بسبل فنية عامة يجب أن تعتمد من قبل السلطة العامة.

السبل الفنية العامة: هذه الوسائل والسبل التي تفرض وتمارس من قبل الدولة لمواجهة خطورة الجرائم الإرهابية الإلكترونية، وأهم هذه السبل هي:

الفرع الأول: إعتماد نظام الحجب والترشيح: نظام الحجب والترشيح هو أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية أو إباحية بالنسبة لمستخدمي الإنترنيت، فإذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبلغه أن الوصول إلى هذه

الصفحة غير مسموح به[١]، ولتغلغل الإنترنيت وغزوه العالم بأسره، حتى بات الجميع غير قادرين على العيش بعزله عن التواصل مع مجريات الأحداث في العالم من خلال شبكة الإنترنيت، إلا أن من الحلول الممكنة للسيطرة أو التقليل من مخاطر الدخول للإنترنيت هو عملية ترشيح الدخول، ويتم ذلك من خلال حجب المواقع الضارة التي تستخدمها الجماعات والتنظيمات الإرهابية، والتي تدعو إلى الفساد والشر، وتلجأ الدول عادة إلى استخدام هذه التقنيات من خلال حجب بعض المواقع الضارة على الشبكة، وهذا قد يستدعي تركيب أجهزة وأدوات تعمل على فلترة وتنقية المواقع وحجب بعضها[٢]، وجاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم، ولذلك سعت مدينة الملك عبدالعزيز للعلوم والتقنية إلى حجب المواقع الإباحية عن مستخدمي(الإنترنيت) في المملكة العربية السعودية حفاظاً على الأخلاق وصيانة للأمة من عبث العابثين وإفساد المجرمين[٣]"ورغم فعالية نظام الحجب والترشيح في منع النفاذ إلى المواقع الإباحية ومواقع المخدرات والميسر، إلا أن كفاءتها تبقى محدودة بالنسبة للمواقع السياسية والدينية.

ورغم الانتقادات التي يمكن أن توجه لنظام الحجب والترشيح، والمتمثلة أساساً في تقييده لحرية الإبحار عبر الإنترنيت ومحدودية نجاعته بالنسبة لبعض المواقع، إلا أنه يبقى ضرورياً لحماية الشباب وخاصة القصر من مواقع المخدرات والإرهاب وخاصة المواقع الإباحية. وتشير دراسات أمريكية إلى أن المدمنين على المواقع الإباحية تتغير لديهم المفاهيم حول ما يعتبرونه مقبولاً إجتماعياً. كما تبين الإحصائيات أنّ ٥٠% من المغتصبين قد أطلعوا على مواد خليعة لتنشيط أنفسهم جنسياً قبل مباشرة جرائمهم الجنسية. وقد قام عدد من ضباط الشرطة الأمريكيين بدراسة ظواهر الاغتصاب والقتل الجماعي، فوجدوا أنّ تداول المواد الإباحية سمة معروفة وموحدة لدى العديد من القتلة والمغتصبين. وقد قام مكتب التحقيقات الفيدرالي الأمريكي باستجواب ٢٤ مجرماً في السجون، أدينوا من أجل جرائم اغتصاب وقتل، فتبيّن أن ٨١% منهم كانوا مدمنين على المواد الإباحية وكانت جرائمهم تطبيقاً لما شاهدوه إباحياً. وفي هذا السياق قامت أستراليا منذ سنة ١٩٩٩ بتكليف هيئة مستقلة بمراقبة الإنترنيت، وقد أعتمدت هذه الهيئة قائمة سوداء في المواقع الاسترالية المخالفة للقانون، والتي يتعين على

(١) ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط١، الرياض، ٢٠٠٩، ص١٧٧.

(٢) بدرة هويمل الزبن، المصدر السابق، ص١٩٢ و ١٩٣.

(٣) د.عبدالقادر الشيخلي، طبيعة الإرهاب الإلكتروني، بحث مقدم إلى المؤتمر الإسلامي العالمي المنعقد في مكة المكرمة، ٢٠١٥، ص١٦.

مزودي الاستضافة إغلاقها مثل المواقع الإباحية التي تستهدف الاطفال والمواقع العنصرية، إضافة إلى المواقع التي تخرق قواعد الملكية الفكرية، وفي نفس السياق، صدر سنة ٢٠٠٠ في الولايات المتحدة الامريكية قانون لحماية الأطفال **Children s Internet (Protection Act)** يفرض على المكتبات العامة استخدام مرشحات تحجب المواقع الاباحية حتى تكون مستحقة للدعم الفيدرالي(١).

ونحن بدورنا كباحث في هذا المجال نحث السلطات الرسمية في العراق بضرورة القيام بحجب المواقع الإلكترونية المشبوهة التي تسعى إلى نشر الإرهاب والأفكار المتطرفة، وتلك المواقع التي تدعو وتعلّم الإرهاب والعدوان والإعتداء على الآخرين وذلك لخطورتها على المجتمع العراقي.

الفرع الثاني: إعتماد تقنية التشفير: التشفير هو استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها *، وتعتبر تقنية التشفير من أنجع الوسائل للحفاظ على سرية المعلومات المتبادلة إلكترونياً وعلى سلامتها من الآخرين. وهي تقنية تستخدم لحماية سرية الوثائق الإلكترونية استناداً إلى نظام العد العشري الذي يسمح بجعل البيانات غير مفهومة بالنسبة لمن لا يملك المفتاح اللازم لفك الرموز، وبذلك يمكن القول بأن التشفير لا يخرج عن كونه كتابة بالرموز. وكلما كانت هذه الرموز معقدة كلما كانت إختراقها أصعب، ولا يخفى ما تضمنه تقنية التشفير من أمن على مستوى مواقع الإنترنيت الحساسة، كتلك التي تمس الأمن القومي أو تلك المختصة في التجارة والمبادلات المالية الإلكترونية. وقد أثبت الواقع العملي أن تقنية التشفير تكفل درجة عالية من تحقيق السلامة المعلوماتية، بما جعلها الحل الأمثل لقطع الطريق أمام القرصنة المعلوماتية(٢).

ففي بريطانيا أعلنت المملكة المتحدة في بداية شهر نوفمبر من عام ٢٠١٥ من خلال المركز السيبراني للأمن الوطني **(The National Cyber Security Center((NCSC))** عن استراتيجيات وخطط جديدة فيما يتعلق بخططها الإلكترونية، والسيبيرانية الجديدة ليس فقط في مجالات التأمين الدفاعية المعتادة ولكن إعتمادها على ماسمَّته)

---

(١) أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد ١٧، العدد ٠١، ٢٠١٨، ص٧٣٥.

* هذا التعريف اعتمده التشريع التونسي في الفصل ٢ من القانون عدد ٨٣ لسنة ٢٠٠٠ المتعلق بالمبادلات والتجارة الإلكترونية.

(٢) أنيس العذار، المصدر السابق، ص٧٣٧.

(Active Cyber Defense، والذي عرفته بأنه سلسلة من الإجراءات الفنية التقنية التي تتخذها الحكومة بالتعاون مع مزودي خدمات الاتصالات ليصبح من الصعب مهاجمة الأفراد المستخدمين لشبكات الإنترنيت البريطانية، وكذلك الشبكات نفسها ومن خلال تعزيز قدراتها على التشفير بشكل جديد وغير تقليدي إضافة إلى الربط والمزامنة بين أسلحتها الهجومية واقعياً وسيبرانياً، واستخدامها تلك القدرات للدفاع عن مصالحها الحيوية في ذلك الفضاء السيبراني بما يضمن استقلالياتها وسيادة الدولة الكاملة على قدراتها التشفيرية[١].

ونحن نرى أنه من الضروري لمقاومة الجرائم الإلكترونية أن يتبنى الحكومة العراقية مجموعة من آليات العمل في التعامل مع البيانات والأجهزة التابعة للدولة وخاصة في الدوائر الحساسة، ومن ضمن هذه الآليات أن تقوم الدولة بأمور منها:

١. تشفير البيانات والمعلومات المهمة لدوائرالدولة والتي يتم تداولها عبر الانترنيت.
٢. إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.
٣. ضرورة توفير برامج للكشف عن الفايروسات لحماية أجهزة الحاسب الآلي.
٤. عمل نسخ احتياطية من البيانات المخزنة،
٥. عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية، مع عمل وسائل التحكم في الدخول إلى المعلومات والمحافظة على سريتها.
٦. توفير كادر متخصص يتولى الاشراف والسيطرة على هذه البرامج وإدارتها، وتوزيع العمل بين العاملين، فمثلاً لا يتم إعطاء المبرمج وظيفة تشغيل الحاسب الآلي إضافة إلى وظيفة البرمجة. كما يمكن توزيع مهام البرنامج الواحد على مجموعة من المبرمجين الأمر الذي يجعل كتابة البرامج الضارة أمراً صعباً.

الفرع الثالث: إستحداث مديرية مقاومة الجرائم والإعتداءات الإلكترونية في وزارة الداخلية:

للتصدي للجرائم الإرهابية الإلكترونية تتطلب إستحداث مديرية متخصصة في الأمن والسلامة المعلوماتية، على غرار ما هو معمول به في كثير من دول العالم، حيث نصت المادة ١٤ من نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية على ما يلي (تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصاتها تقديم الدعم والمساعدة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة).

ويعد استحداث مديرية متخصصة في وزارة الداخلية لمكافحة الجريمة الإلكترونية أمراً ضرورياً، نظراً لصعوبة الإثبات في الجريمة المعلوماتية، وقد أنشأت عدة دول في العالم وحدات متخصصة في مجال مكافحة جرائم الإنترنيت من ذلك الصين والولايات المتحدة

---

(١) د. راجي يوسف محمود البياتي، الإرهاب السيبراني، مجلة تكريت للعلوم السياسية، العدد١٨، ٢٠٢٢، ص١٠٨.

الامريكية وبريطانيا[١]، وفي فرنسا اقترح وزير الداخلية السابق" ميشال دي فيلبان" مشروع قانون يهدف إلى مكافحة الجريمة الإلكترونية، ومن بين الحلول الواردة في مشروع القانون الترفيع في قوات الشرطة والدرك المتخصصين في المعلوماتية، وقد ذهب وزير الداخلية الفرنسي إلى حد اقتراح " البحث عن وسائل خاصة للتحقيق تمكّن من اكتشاف الجرائم الخطيرة في الوقت المناسب فلا يمكن مثلاً للمحققين أن يشاركوا تحت اسم مستعار في المحادثات الإلكترونية بدون ان يكونوا مسؤولين جزائياً[٢].

ونرى أن يكون منتسبي هذه المديرية من الضباط الحائزين على شهادات فنية في مجال البرمجيات والحاسوب الآلي بالاضافة إلى تخصصهم وشهاداتهم في مجالهم الأمني، ومن المدنيين الحائزين على شهادات عليا في مجال البرمجة والحاسوب، متدربين ومتخصصين للتصدي ولمكافحة جرائم المعلوماتية عموماً وجرائم الإرهاب الإلكتروني خصوصاً ومزودين بكافة الإمكانيات المادية والنظم المعلوماتية والتكنولوجية. والأهم من كل ذلك منح أعضاء هذه المديرية من الأمنيين والمدنيين سلطة عضو الضبط القضائي الإلكتروني وذلك بتعديل نص المادة (٣٩) من قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل[٣]، حيث يكون لهؤلاء المنتسبين سلطة التحري عن الجرائم الإلكترونية وضبط مرتكبيها أثناء تلبسهم بالجريمة وسلطة التفتيش الإلكتروني، على أن تكون

---

(١) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، ٢٠١٣، ص١٠٧.

(٢) نبيلة هبة هروال، المصدر نفسه، ص١١٥.

(٣) المادة ٣٩ من قانون أصول المحاكمات الجزائية العراقي: اعضاء الضبط القضائي هم الاشخاص الآتي بيانهم في جهات اختصاصهم- :

١-ضباط الشرطة ومأمورو المراكز والمفوضون.

٢-مختار القرية والمحلة في التبليغ عن الجرائم وضبط المتهم وحفظ الاشخاص الذين تجب المحافظة عليهم.

٣- مدير محطة السكك الحديدية ومعاونه ومأمور سير القطار والمسؤول عن ادارة الميناء البحري او الجوي وربان السفينة او الطائرة ومعاونه في الجرائم التي تقع فيها.

٤-رئيس الدائرة او المصلحة الحكومية او المؤسسة الرسمية وشبه الرسمية للجرائم التي تقع فيها.

٥- الاشخاص المكلفون بخدمة عامة الممنوحون سلطة التحري عن الجرائم واتخاذ الاجراءات بشأنها في حدود ما خولوا به بمقتضى القوانين الخاصة.

سلطة التفتيش الإلكتروني فقط لجرائم الإرهاب الإلكتروني وفي حدود ضيّقة وللحالات الحرجة والخطرة فقط، حتى لا يحسب ضمن تضييق الخناق على الحريات العامة.

إن جرائم الإرهاب الإلكتروني يتم إرتكابها في الفضاء المجازي لدنيا المعلوماتية وهؤلاء الجناة ذوي خبرة عالية وتفنن سريع ويقومون بتنفيذ مخططاتهم بسرعة وتنظيف مخلفاتهم في مسرح الجريمة، إذ يحرص الجاني بعد إرتكابه لجريمته على محو آثارها التي تدل على وقوعها، وذلك من خلال تقنيات معدة لهذا الغرض، مع الأخذ بنظر الإعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام به في أزمان قياسية متناهية القصر تقاس باللحظات والثواني(١).

إن إكتشاف الجرائم عموماً ومن ضمنها الجرائم المعلوماتية بعد وقوعها يدخل ضمن المفهوم العام للتحريات التي تعد بدورها من إجراءات الإستدلال(٢) التي تدخل ضمن مهام أعضاء الضبط القضائي المكلفين قانوناً بعدة واجبات من ضمنها التحري عن الجرائم والكشف عنها(٣) بكافة الوسائل المتاحة والمشروعة، وهذا الواجب يشمل أيضاً محاولة إكتشاف أية جريمة يمكن أن تكون قد وقعت.

ونرى أيضاً أن يلقى على عاتق المديرية المقترح استحداثها، مهمة التوعية لتحقيق الأمن الفكري، وغرس المفاهيم الأمنية في العقول الناشئة، ومن الوسائل الهامة في تحقيق الأمن الفكري وتكريسه دور الأسرة والمجتمع، والتربية على المثل والقيم والأخلاق الحميدة، والتركيز على حماية الشباب من الانحرافات الفكرية التي تولد الكثير من المشاكل الاجتماعية، والتنشئة الدينية السليمة بعيداً عن الغلو والتطرف، والتركيز على القيم السامية والنبيلة للمجتمع. ونرى أن تقوم بهذا الدور المديرية المقترحة وبالتنسيق مع وزراة التربية ووزارة الأوقاف وغيرها من الجهات المعنية في الدولة عن طريق التعاون فيما بينهم بعمل الدورات والمؤتمرات والحلقات النقاشية وغيرها من الامور التي يمكن أن تساهم في نشر فكر التوعية وبيان أضرار هذه الأعمال والنتائج المترتبة على استخدامها وتجريم مستخدميها، ويشمل التعاون بين مزودي خدمة الانترنيت من خلال قيامهم بالإبلاغ عن الأنشطة الإرهابية التي تتضمن أفعالاً مخلة بالأمن والنظام.

---

(١) رشاد خالد عمر، المصدر السابق، ص٦٤.

(٢) د. قدري عبدالفتاح الشهاوي، ضوابط الإستلالات والإيضاحات والتحريات والإستخبارات في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية ٢٠٠٢، ص١٦٢.

(٣) أنظر المادة(٤١) من قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل.

المطلب الثاني: السبل القانونية للتصدي لجرائم الإرهاب الإلكترونية

إن جرائم الإرهاب الإلكتروني ذات صبغة عالمية وهذا ما يستدعي تعاوناً بين جميع الدول للتصدي لها، وهذا ما يستوجب إبرام إتفاقيات ومعاهدات دولية توحّد الحلول والإجراءات لمجابهتها وحتى لا يكون المجرم المعلوماتي في مأمن من التتبع والعقاب أينما وجد في العالم، مع هذا تبقى التشريع الداخلي الرادع الأساسي لهكذا جرائم، عليه سنتناول الجهود القانونية الدولية والداخلية للتصدي لجرائم الإرهاب الإلكتروني، وذلك وفق الآتي:

الفرع الأول: السبل القانونية الدولية للتصدي لجرائم الإرهاب الإلكتروني: أثبت الواقع العملي أنَّ أي دولة لوحدها غير قادرة على التصدي للجرائم الإلكترونية وذلك للسمة العالمية لهذه الجرائم ولكونها عابرة للحدود، فإن التصدي لها لا يتحقق إلا بوجود تعاون دولي لتوحيد الإجراءات لمواجهته، وعليه سنتناول جهود الأمم المتحدة والدول الأوروبية والدول الاقليمية لمواجهته وفق الآتي:

أولاً: جهود منظمة الأمم المتحدة: تحركت الأمم المتحدة لمقارعة خطر الإرهاب الدولي بخط تصاعدي يؤشر بوضوح تطور الوعي الدولي بمخاطر الإرهاب وتداعياته على الأمن والسلم العالمي. ويمكن التمييز في هذا التحرك الأممي بين مرحلتين رئيستين اتمثلت الأولى في مواجهة الإرهاب التقليدي بصورته المادية والدموية على أرض الواقع، وكان أكبر رصيد من الانجازات حققته منظومة الأمم المتحدة في هذا المنظار يتمثل بوضع نظام معاهدات وإتفاقيات دولية يتألف من ستة عشرة إتفاقية دولية لمكافحة الانشطة الإرهابية وتجريم الدول والكيانات التي تلجأ الى استخدامها، والثانية تتمثل الدعوة الأممية لدول العالم إلى إتخاذ الإجراءات والتدابير العملية الفاعلة لمكافحة الاعمال الإرهابية وملاحقة ومحاسبة مقترفيها[١].

ومع تزايد خطر الإرهاب الدولي وبروز وإنتشار نوع جديد من الجريمة المرتبطة بالحاسوب الآلي بفعل تسارع وتيرة التطور التقني في أنظمة المعلومات والاتصالات وما أفرزه ذلك التهديد من اضرار ومخاطر على أمن البلدان والافراد لا سيما بعد دخول الشبكة الدولية للمعلومات بوسائلها المتنوعة والمتطورة على خط الإرهاب الدولي ومواجهته، تزايدت الحاجة إلى تضافر الجهود الدولية وتعاضدها تحت مظلة المنظمات الدولية والإقليمية لمواجهة هذا التهديد، وكانت الأمم المتحدة المحفل العالمي الأهم لترجمة هذه الجهود واستثمارها الأمثل في هذه المواجهة، لما تتمتع به من مصداقية في مجال تعزيز التعاون الدولي لتحقيق مقاصدها في ضمان السلم والأمن الدوليين في مواجهة مختلف التهديدات العالمية بضمنها خطر

(١) د. سامر مؤيد عبداللطيف وآخرون، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مجلة رسالة الحقوق، السنة العاشرة، العدد الثاني، ٢٠١٨، ص٥٥.

الإرهاب الدولي[١]، بذلت منظمة الأمم المتحدة جهوداً كبيرة من أجل مكافحة جرائم الأنترنيت، وقد توصلت المنظمة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المعلوماتية وقع التنصيص فيه على الإجراءات التي يتعين اتخاذها من طرف الدول الاعضاء لمكافحة الجرائم الإلكترونية. وفي سنة ٢٠٠٠ تبنّت منظمة الأمم المتحدة الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية، وشددت على ضرورة التنسيق بين الدول على مستوى تتبّع الجرائم المعلوماتية، وشدّدت على ضرورة تكوين الأشخاص المعنيين بالتتبّع وتمكينهم من الوسائل الضرورية لذلك، كما عقدت منظمة الأمم المتحدة سنة ٢٠١٠ المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية. وقد ناقشت الدول الأعضاء آخر التطورات في استخدام التكنولوجيا الحديثة من طرف المجرمين، بما في ذلك الجرائم الإلكترونية، واحتلت الجريمة المعلوماتية موقعاً بارزاً في جدول أعمال المؤتمر[٢].

ثانياً: إتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة ٢٠٠١: جاءت إتفاقية بودابست تتويجاً للجهود التي بذلها الاتحاد الأوربي من أجل إيجاد صيغة قانونية لمكافحة الجريمة الإلكترونية، وهي تعد حالياً الإطار المرجعي لمكافحة الجرائم المعلوماتية، وضعت هذه الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، وقد دخلت حيز التنفيذ في سنة ٢٠٠٤ ويمكن لأي دولة الانضمام إليها. أبرزت هذه الاتفاقية في صلب توطئتها مدى اقتناع الدول المصادقة عليها بخطورة الجريمة المعلوماتية، وبضرورة تضافر الجهود الدولية لمواجهتها. وقد تعرضت إلى بعض المفاهيم، منها مفهوم النفاذ غير الشرعي ومفهوم الجريمة المعلوماتية وغيرها من المفاهيم التي تستدعي اعتماد مفهوم موحد لتسهيل تطبيق الاتفاقية، كما تضمنت قواعد متعلقة بالتعاون في ميدان مواجهة الجريمة الإلكترونية، كالقواعد الخاصة بالاختصاص الترابي للمحاكم (المادة ٢٢) وتسليم المجرمين (المادة ٢٤) واعتماد شبكة مفتوحة كامل الأسبوع مخصّصة لبقية الدول الأعضاء لتوفير المساعدة في الأبحاث المرتبطة بالجرائم المعلوماتية(المادة٣٥)[٣].

ثالثاً: الجهود الاوربية لمكافحة جرائم الإنترنيت: يعد الإتحاد الأوربي من أهم الهيئات التي تبذل العديد من الجهود لمكافحة الجرائم الإرهابية الإلكترونية بأنماطها كافة، ويعد من واجبات الإتحاد العمل على توافق الأنظمة القانونية للإتحاد الأوربي بهذا الشأن، وتعد الرؤية الأوربية الأكثر شمولاً ونضجاً في مجال تنظيم مسائل تقنية المعلومات، لأنها أدركت أهمية وخطورة

---

(١) محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥، ص٢٥٣.

(٢) أنيس العذار، المصدر السابق، ص٧٣٩.

(٣) المصدر نفسه، ص٧٤٠.

التحديات الناجمة عن هذه التقنية[١]، ومن الجهود الأوربية أيضاً إهتمام لجنة الوزراء بالإتحاد الأوربي بالمشكلات الخاصة بالجرائم الإرهابية الإلكترونية من خلال الإشارة في توصياتها المتعددة إلى تشجيع الدول الأوربية على تبني سياسات مشتركة تهدف إلى تحقيق التفاهم والتعاون في مكافحة جرائم الإرهاب الإلكتروني، ومن هذه التوصيات توصية رقم (١٠/٨٥) الخاصة بالتطبيق العملي للإتفاقية الأوربية بشأن المساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية، وبشأن إعتراض الإتصالات السلكية واللاسلكية، والتوصية رقم (٢/٨٨) بشأن القرصنة في مجال التأليف والحقوق المجاورة وحقوق النشر، والتوصية رقم (١٥/٨٧) التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم (٤/٩٥) بشأن حماية البيانات الشخصية في مجال خدمات الإتصال وخاصة الخدمات التليفونية، وكذلك التوصية رقم (٩/٨٩) بشأن الجرائم المتعلقة بالكومبيوتر التي تُقدّم الإرشادات للهيئات التشريعية الوطنية فيما يتعلق بتعريف جرائم معينة تتعلق بالكومبيوتر، وأخيراً التوصية رقم (١٣/٩٥) التي تتعلق بمشكلات قانون الإجراءات الجنائية ذات الصلة بتكنولوجيا المعلومات[٢]، ومن ضمن أبرز الجهود الأوربية التي أثمرت هو صدور الإتفاقية الأوربية لمكافحة الجرائم المعلوماتية في بودابست والتي تتضمن بشكل رئيسي التزام الدول الأطراف فيها بسن الحد الأدنى من القوانين الضرورية للتعامل مع الجرائم التقنية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكومبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي[٣]، ويضاف إلى ذلك البروتوكول الإضافي لها بشأن تجريم الأفعال ذات الطبيعة العنصرية بكراهية الأجانب والتي تتم عن طريق أنظمة الكومبيوتر، فضلاً عن قرار إطار العمل الصادر عن المجلس الأوربي رقم (JHD/٢٢٢/٢٠٠٥) بتاريخ ٢٤ شباط ٢٠٠٥ حول الإعتداءات ضد الأنظمة الإلكترونية[٤].

رابعاً: جهود الدول العربية: تبدو جهود الدول العربية في مكافحة الجرائم الإلكترونية، من خلال اجتماع ممثلي الدول العربية في المؤتمر العربي للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات في الفترة الممتدة من ١٦ إلى ١٨ يونيو ٢٠٠٣. وقد حضر المؤتمر ممثّلو ١٩ دولة عربية إضافة إلى مندوبي ٩ دول إفريقية كمراقبين وعدة شخصيات مرموقة

(١) عمر عباس خضير العبيدي، المصدر السابق، ص٧٧.

(٢) المصدر نفسه، ص٧٨.

(٣) بدرة هويمل الزبن، المصدر السابق، ص٢١١.

(٤) عمر عباس خضير العبيدي، المصدر السابق، ص٧٩.

عالمياً في مجال الإتصالات والمعلوماتية. وأوصى المشاركون في المؤتمر بإنشاء فريق عمل تحت مظلة جامعة الدول العربية لتأمين شبكة المعلومات العربية وحماية المستهلك العربي من جرائم الإنترنيت(١).

وفي ظل تنامي المخاطر الأمنية والاقتصادية والفكرية والأخلاقية لجرائم البيئة الرقمية في الدول العربية، وقصور تشريعاتها الجنائية في مواجهة هذا النمط من الإجرام العابر للحدود الوطنية، وافق وزراء الداخلية ووزراء العدل العرب في إجتماعهما المشترك في ٢١ ديسمبر ٢٠١٠ بمدينة القاهرة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، من أجل توحيد السياسة الجنائية لحماية المجتمع العربي من خطر وآثار هذه الجرائم بما فيها جريمة الإرهاب الإلكتروني، وقد اعتمدت هذه الاتفاقية على نوعين من الآليات لمكافحة الجرائم الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني، تتمثل الأولى في إلزامية اتخاذ الدول الأطراف للتدابير اللازمة والإجراءات الخاصة في قوانينها الداخلية لتمكين سلطاتها المختصة للبحث والتحقيق عن هذه الجرائم التي يصعب فيها التعرف على هوية المجرم، ويسهل فيها محو الدليل الرقمي، أما الثانية فتكمن في ضرورة تكثيف جهود التعاون القضائي والقانوني بين هذه الدول لعدم إفلات المجرمين من العقاب(٢).

الفرع الثاني: السبل القانونية الداخلية للتصدي لجرائم الإرهاب الإلكتروني: لمّا كان القانون هو الوسيلة المثلى لتنظيم المجتمع وضمان أمن وأستقرار الأفراد في حياتهم وأعراضهم وأموالهم، ولمّا كان المجتمع في تطور مستمر ودائم في جميع مجالات الحياة المختلفة، فإن ذلك يفرض على التشريعات أن تتطور هي أيضاً وبشكل تواكب معه حركة المجتمع المتنامية، وتساير التطورات التكنولوجية والاقتصادية والاجتماعية وغيرها من خلال تنظيمها بأحكام تتلاءم مع هذه المتغيرات والتطورات، وتضمن التصدي لكل ما يخل بأمن المجتمع ويعرقل حركة التطور الإنساني، وذلك من خلال نصوص وأحكام مستحدثة تنطوي على عقوبات حازمة تستهدف الردع الخاص للجناة والردع العام للآخرين(٣)،وتعتبر العقوبة الجزائية من أهم العقوبات التي تفرض على مرتكب الجريمة فعندما ترتكب الجريمة فإنه يتوجب على المحكمة المختصة إيقاع هذه العقوبة على مرتكب الجريمة حال ثبوت ذلك.

---

(١) ناصر بن محمد البقمي، المصدر السابق، ص١٠٠.

(٢) توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، مجلة العلوم القانونية والسياسية، المجلد٠٩، العدد٠٣، ص٩٧.

(٣) رشاد خالد عمر، المصدر السابق، ص٤٤.

والجدير بالذكر لايوجد في العراق تشريع خاص يتناول جرائم الإرهاب الإلكتروني، وإنما تناول الجرائم محل الدراسة كجريمة إرهابية بموجب نص المادة (٤) من قانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥ وهو نص يتناول الإرهاب التقليدي، ولاشك أن القضاء العراقي يكيّف الوصف القانوني لجرائم الإرهاب الإلكتروني بموجب نص المادة الثانية من القانون المذكور ويفرض العقوبة على مرتكبها وفق المادة الرابعة منها، وعلى الرغم من أن القضاء العراقي طبق حكم المادة الرابعة على مرتكبي جرائم الإرهاب الإلكتروني في أكثر من مناسبة، إلا إننا نرى هذا قصور في التشريع العراقي وعلى المشرع مسايرة التطور الذي حصل في مجال جرائم المعلوماتية، وذلك بإضافة نص إلى قانون مكافحة الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥ على غرار نص المادة (٢٩) من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥[١]، لتكون أكثر ملاءمة لملاحقة مجرمي الإرهاب الإلكتروني.

إذ بيّنَ قانون مكافحة الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥ عقوبة جريمة الإرهاب التقليدية، وحدد عقوبة الفاعل فيها، كما بين الأعذار المخففة لهذه الجريمة والإعفاء من العقوبة، حيث تنص المادة (٤) من قانون مكافحة الإرهاب العراقي على أنه (يعاقب بالإعدام كل من إرتكب بصفته فاعلاً أصلياً أو شريكاً عملاً من الأعمال الإرهابية في المادة الثانية والثالثة من هذا القانون). ويستفاد من هذا النص أن عقوبة مرتكب الأعمال الإرهابية هي الإعدام، وحدد القانون المذكور عقوبة الشريك والمتدخل والمساعد بنفس عقوبة الفاعل، فالمحرض على إرتكاب جريمة الإرهاب وكل شخص مكن الإرهابيين من القيام بالعمليات الإرهابية ومساعدتهم على إرتكابها يعاقب بعقوبة الإعدام، والسبب في تشديد العقوبة يعود إلى

---

(١) تنص المادة ٢٩ من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠٠٥ على:
يُعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها.

خطورة هذه الجريمة على المجتمع، وتهديدها للأمن والنظام فيه، وبما أن القضاء العراقي يطبق عقوبة المادة الرابعة من القانون المذكور فإن مرتكبي جرائم الإرهاب الإلكتروني تطبق بحقهم أيضاً نص المادة السابقة لعدم وجود نص خاص بجرائم الإرهاب الإلكتروني.

بالإضافة إلى هذا التعديل نرى وبسبب المخاطر التي تحيط بالتعاملات الإلكترونية أنَّ الحاجة باتت ملُحّة لإيجاد آلية للمعلومات تسمح بضبط التعاملات الإلكترونية، إلا أنه ومع التطورات الحاصلة في المجال الإلكتروني لا زالت التشريعات القانونية لا تواكب هذه التطورات. وهنا ظهرت الحاجة الملحة لتشريع وتقنين القوانين والأنظمة واللوائح اللازمة لتحقيق الإستفادة القصوى من تقنية المعلومات وتحصينها وحماية المتعاملين من مخاطرها. وهذه المسؤلية ملقاة على المشرع العراقي في أن يسارع الخطى بتشريع هكذا قوانين والأنظمة واللوائح بالإستعانة بالخبراء من القانونين والفنيين والأمنيين وذلك لتنظيم سلوك الأفراد والمؤسسات في مجال التعامل مع تقنية المعلومات، دون أن يكون قيداً على حرية المجتمع، مع مراعاة نص المادة (١٥)[١] والمادة(٤٠)[٢] من الدستور العراقي لسنة ٢٠٠٥ النافذ. ومن الأمثلة للقوانين والتشريعات المقترحة، التشريعات الخاصة بضبط التعاملات الإلكترونية، والتشريعات اللازمة لتجريم الإعتداءات الإلكترونية التي تتم عن طريق الإنترنيت، والتشريعات الخاصة بتجريم العدوان الإلكتروني، وأنظمة ولوائح للحد من الاختراقات الإلكترونية.

المطلب الثالث: دور الجامعات في التصدي لجرائم الإرهاب الإلكتروني

الجامعة هي أحدى خلايا المجتمع الهامة، فهي لم تنشأ في فراغ، وإنما في وليدة المجتمع وتؤثر فيه وتتأثر به سلباً وإيجاباً، والجامعة بدون شك ظهرت نتيجة لحاجات احس بها أبناء مجتمعاتها وقادة الفكر فيها، وهي تعمل دائماً لسد هذه الحاجات بصورة دائمة ومتجددة. وتوسعت مهام الجامعة في الوقت الراهن، إذ لم تعد أولوياتها تخريج عدد من الكفاءات العلمية في مختلف الاختصاصات، بل اصبحت لها دور في مجال تنمية المجتمع، تسهم في مواجهة تحديات الظروف الراهنة ومتطلباتها بما تكفل من حقائق وما تسهم به من

(١) تنص المادة (١٥) من الدستور العراقي لسنة ٢٠٠٥ على أنه: لكل فرد الحق في الحياة والأمن والحرية، ولايجوز الحرمان من هذه الحقوق أو تقييدها إلا وفقاً للقانون، وبناءً على قرار صادر من جهة قضائية مختصة.

(٢) تنص المادة (٤٠) من الدستور العراقي لسنة ٢٠٠٥ على أن: حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، الا لضرورةٍ قانونيةٍ وأمنية، وبقرارٍ قضائي.

الحلول للمشاكل الحالية والمستقبلية وبما تنشره من المعرفة، إذ يجب أن ترتبط الجامعة ديناميكياً بمحيطها ومجتمعها.

على الرغم من تعدد أهداف الجامعة وتنوعها، إلا أن مضمون هذه الأهداف يتركز حول ثلاث وظائف رئيسية كالاتي:

١. **البحث العلمي:** ان الوظيفية الرئيسة لاي مؤسسة جامعية هي توسعة المعرفة من خلال نشاط الاساتذة في الجامعات ومراكز البحوث، ويحتاج هذا النشاط إلى آليات وأجهزة وتسهيلات وباحثين أكفاء فينعكس ذلك التقدم على مختلف المجالات بالفائدة والمنفعة على جميع الاطراف ذات العلاقة.

٢. **التعليم:** تسهم الجامعة بتثقيف الطالب في مختلف مجالات المعرفة ومحاولة العمل على تطوير قدراته التفكيرية بما تقدمه الجامعة من إمكانيات وخبرات للتعليم والتدريب المستمر بحيث يصبح الهدف الأول للتعليم الجامعي تطوير المجتمع والنهوض به إلى أفضل المستويات التقنية والاقتصادية والاجتماعية والثقافية.

٣. **خدمة المجتمع:** يكمن هذا الدور في الاستفادة من المعرفة المتطورة في الجامعات بشكل مباشر بهدف تمكين أفراد المجتمع ومؤسساته وهيئاته من تحقيق أقصى إفادة ممكنة من الخدمات المختلفة التي تقدمها الجامعة بوسائل واساليب متنوعة تتناسب مع ظروف المستفيد وحاجاته الفعلية(١).

وبما أن ثورة الإتصالات والرقميات أفرزت وسائل جديدة للمجتمع الإنساني تجعل الحياة أفضل من ذي قبل، إلا أنها من جانب آخر فتحت الباب على مصراعيه لظهور أنماط وصور من السلوك المنحرف إجتماعياً التي لم يكن من الممكن وقوعها في الماضي، وتخرج عن دائرة التجريم والعقاب القائمة. وترتبط فكرة الإرهاب الإلكتروني بالتطورات التي حدثت في مجال المعلومات، وتركز جماعات الإرهاب الإلكتروني على تأجيج العواطف وتهييج انفعالات الشباب، لذلك لابد من الحصانة الفكرية للشباب من خلال تنمية وعيهم بخطورة الجرائم المعلوماتية وهو ما يجب أن تقوم به الجامعات من ضمن الوظائف الثلاث أعلاه لأنها وظائف متكاملة، ولايمكن رؤيتها منفصلة، وذلك ما نسعى بدورنا إليه من تفعيل دور الجامعات العراقية في تنمية وعي الشباب بخطورة الجرائم المعلوماتية لدعم قضايا التصدي للإرهاب الإلكتروني، ونرى أن دور الجامعات يمكن أن يفعل وفق مجموعة من الرؤى والآليات التي يجب أن يضطلع بها، وأهمها :

---

(١) زرزار العياشي، دور الجامعات العربية في خدمة المجتمع في ضوء مسؤوليتها الاجتماعية، مجلة آداب ٥، الكوفة، العدد ٣٢، ٢٠١٧، ص٢٥٦.

١. تصميم وتنفيذ برامج وقائية للشباب للتوعية بجرائم المعلوماتية وجرائم الإرهاب الإلكتروني.
٢. إقامة الندوات والحلقات النقاشية والمؤتمرات العلمية في مجال وقاية الشباب من مخاطر جرائم المعلوماتية وجرائم الإرهاب الإلكتروني.
٣. تنسيق العمل مع منظمات المجتمع المدني والمنظمات الحكومية في توجيه برامج التوعية والوقاية للشباب من مخاطر جرائم المعلوماتية وجرائم الإرهاب الإلكتروني.
٤. دعم الأبحاث والدراسات التي تقوي وتدعم الشباب من أجل التصدي لجرائم المعلوماتية.
٥. وضع خطط ومناهج لتطوير بعض مناهج التعليم بما يحقق التوعية من مخاطر جرائم المعلوماتية.
٦. التعاون مع المؤسسات والجهات التعليمية وخبراء التربية لتطوير طرق الوقاية من جرائم المعلوماتية.
٧. التعاون مع وسائل الإعلام لتفعيل أنجح وأنسب الوسائل وطرق وقاية الشباب من الجرائم المعلوماتية وجرائم الإرهاب الإلكتروني في وسائل الأعلام المختلفة.
٨. إنشاء قسم جديد في كليات القانون في الجامعات العراقية يختص بدراسة جرائم المعلوماتية ودراسة الحماية القانونية للمعلوماتية.

الخاتمة

أولاً: الاستنتاجات:

١. لا يوجد إتفاق دولي حتى الآن على تعريف جامع مانع متفق عليه للإرهاب عامة وجرائم الإرهاب الإلكتروني خاصة، ويمكننا القول أن الإرهاب الإلكتروني هو : العمل العدواني أو التهديد المادي او المعنوي الصادر من الدول أو المنظمات أو الأفراد بوسائل إلكترونية بهدف ترويع الافراد أو إجبار الحكومة على القيام بعمل أو الامتناع عن القيام بعمل ما، أو تدمير وتخريب المؤسسات الأساسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو زعزعة استقرارها.

٢. جريمة الإرهاب الإلكتروني جريمة إرهابية عابرة للحدود بل عابرة للقارات وغير خاضعة لنطاق إقليمي محدد، وترتكب من دون الحاجة إلى الحركة والتنقل ما بين الدول.

٣. عدم الحاجة عند ارتكاب جريمة الإرهاب الإلكتروني إلى ممارسة القوة والعنف فقط يحتاج إلى توافر حاسب آلي متصل بالشبكة المعلوماتية ومجهز ببعض البرامج اللازمة.

٤. صعوبة إكتشاف جريمة الإرهاب الإلكتروني، وبالتالي صعوبة الإثبات فيها، وذلك لإن مسرح الجريمة هي الفضاء المجازي في عالم الرقمي ولإنها تقع في بيئة إلكترونية يتم تنظيف مسرح الجريمة من قبل الجناة بسهولة وسرعة، وكل هذا بدوره يترتب عليه جملة من المشاكل والصعوبات التي تعوق إكتشاف هذه الجرائم وبالتالي التحقيق فيها.

٥. إن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم، نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى وبعيد عن الأنظار، مع توفير قدر كبير من السلامة والأمان للإرهابيين.

٦. إن أسباب الإرهاب الإلكتروني ودوافعه متعددة ومتنوعة، وهي عينها أسباب ظاهرة الإرهاب عموماً، وذلك لأن الإرهاب الإلكتروني يعتبر نوعاً من أنواع الإرهاب وشكلاً من أشكاله، كما أن هناك عوامل عديدة تجعل من ظاهرة الإرهاب الإلكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الإرهابية.

٧. إن اعتماد الدول على وسائل الاتصالات والشبكة العنكبوتية سيكون عاملاً فاعلاً في فتح المجال أمام الإرهابيين لتحقيق أهدافهم، فالإرهاب الإلكتروني يهدف إلى تدمير البنية التحتية المعلوماتية وتعريض المجتمعات العالمية إلى مخاطر غير محتملة و غير متوقعة.

٨. إن أهم مظاهر الإرهاب الإلكتروني وأشكاله تتمثل في تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، وإنشاء المواقع الإرهابية الإلكترونية، وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والتهديد الإلكتروني، والتجسس الإلكتروني.

٩. تقوم المجاميع الإرهابية بشن هجمات إلكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالباً، وهي الأهداف العسكرية، والسياسية، والاقتصادية

ثانياً: التوصيات:

١. نوصي بعقد مؤتمر دولي بإشراف هيئة الأمم المتحدة يتم من خلاله تعريف الإرهاب عامة وتعريف الإرهاب الإلكتروني خاصة، ووضع خطة عملية دولية لمكافحته بجميع صوره.

٢. التحذير من تزايد مخاطر الإرهاب الإلكتروني، والتأكيد على أنه رغم التزايد المطرد للجرائم المعلوماتية إلا أن العالم لم يشهد بعد إرهابا إلكترونياً من نوع مُشابه للإرهاب العادي، والتنبيه إلى الهشاشة الأصيلة في البنية التحتية للشبكة العالمية للمعلومات، مما يُمهد لهجمات إرهابية ربما تؤدي إلى نتائج كارثية على المجتمعات الدولية والاقتصاد العالمي.

٣. نوصي السلطات الرسمية في العراق بضرورة القيام بحجب المواقع الإلكترونية المشبوهة التي تسعى إلى نشر الإرهاب والأفكار المتطرفة، وتلك المواقع التي تدعو وتعلّم الإرهاب والعدوان والإعتداء على الآخرين وذلك لخطورتها على المجتمع العراقي.

٤. من الضروري لمقاومة الجرائم الإلكترونية أن تتبنى الحكومة مجموعة من آليات العمل في التعامل مع البيانات والأجهزة التابعة للدولة، ومن ضمنها أن تقوم الدولة: تشفير البيانات المهمة لدوائر الدولة والتي يتم تداولها عبر الانترنيت وإيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات الضرورية مع توفير برامج للكشف عن الفايروسات لحماية أجهزة الحاسب الآلي وتوفير كادر متخصص يتولى الإشراف والسيطرة على هذه البرامج وإدارتها.

٥. نوصي بإستحداث مديرية متخصصة في الأمن والسلامة المعلوماتية، تحت مسمى مديرية مقاومة الجرائم والإعتداءات الإلكترونية في وزارة الداخلية، وأن يكون منتسبو هذه المديرية من الضباط الحائزين على شهادات فنية في مجال البرمجيات والحاسوب الآلي بالاضافة إلى تخصصهم وشهاداتهم في مجالهم الأمني، ومن المدنيين الحائزين على شهادات عليا في مجال البرمجة والحاسوب، متدربين للتصدي ولمكافحة جرائم المعلوماتية عموماً والإرهاب الإلكتروني، خصوصاً ومزودين بكافة الإمكانيات المادية والنظم المعلوماتية والتكنولوجية، وأن يلقى على عاتق المديرية المقترحة استحداثها، مهمة التوعية لتحقيق الأمن الفكري، وغرس المفاهيم الأمنية في العقول الناشئة.

٦. نوصي بتعديل نص المادة (٣٩) من قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل، ومنح أعضاء مديرية مقاومة الجرائم والاعتداءات الإلكترونية من

الأمنيين والمدنيين سلطة عضو الضبط القضائي الإلكتروني ويكون لهؤلاء المنتسبين سلطة التحري عن الجرائم الإلكترونية وضبط مرتكبيها أثناء تلبسهم بالجريمة وسلطة التفتيش الإلكتروني.

٧. نوصي بإضافة نص إلى قانون مكافحة الإرهاب العراقي رقم ١٣ لسنة ٢٠٠٥ على غرار نص المادة (٢٩) من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥، لتكون أكثر ملاءمة لملاحقة مجرمي الإرهاب الإلكتروني.

٨. نوصي المشرع العراقي أن يسارع الخطى بتشريع القوانين والأنظمة واللوائح الخاصة بتنظيم سلوك الأفراد والمؤسسات في مجال التعامل مع تقنية المعلومات، ومن الأمثلة للقوانين والتشريعات المقترحة، التشريعات الخاصة بضبط التعاملات الإلكترونية، والقوانين الخاصة لتجريم الإعتداءات الإلكترونية التي تتم عن طريق الإنترنيت، والتشريعات الخاصة بتجريم العدوان الإلكتروني، وأنظمة ولوائح للحد من الاختراقات الإلكترونية.

٩. تفعيل دور الجامعات العراقية في تنمية وعي الشباب بخطورة الجرائم المعلوماتية لدعم قضايا التصدي للإرهاب الإلكتروني.

ثبت المصادر

أولا: الكتب

- الإرهاب والجريمة الإلكترونية، د. غادة نصار، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٧.
- جرائم الإرهاب في التشريع المقارن، محمد العفيفي، المكتبة الوطنية، الأردن، ٢٠٠٧.
- جرائم الحاسوب وأبعادها الدولية، محمود أحمد عبابنة، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٥.
- جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص، د. علي عبود جعفر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٣.
- الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، نبيلة هبة هروال، دار الفكر الجامعي، ٢٠١٣.
- ضوابط الإستلالات والإيضاحات والتحريات والإستخبارات في التشريع المصري والمقارن، د. قدري عبدالفتاح الشهاوي، منشأة المعارف، الإسكندرية ٢٠٠٢.
- لسان العرب (المجلد الاول)، إبن منظور العربي، منشورات مؤسسة الاعلمي للمطبوعات، بيروت. ٢٠٠٥.
- المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، رشاد خالد عمر، المكتب الجامعي الحديث، الاسكندرية، ٢٠١٣.
- ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط١، الرياض، ٢٠٠٩.

ثانياً: الرسائل والأطاريح الجامعية

- الإرهاب الإلكتروني في نطاق القانون الدولي، عمر عباس خضير العبيدي، رسالة ماجستير مقدمة إلى كلية الحقوق جامعة تكريت، ٢٠١٩.
- الإرهاب في الفضاء الإلكتروني" دراسة مقارنة"، بدرة هويمل الزبن، أطروحة دكتوراه غير منشورة، كلية القانون، جامعة عمان العربية، ٢٠١٢.
- جريمة الإرهاب الإلكتروني "دراسة مقارنة"، إسراء طارق جواد كاظم الجابري، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة النهرين،٢٠١٢.
- جريمة الإرهاب عبر الوسائل الإلكترونية" دراسة مقارنة بين التشريع الاردني والعراقي"، مصطفى سعد حمد مخلف، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٧.

❖ جريمة الإرهاب في التشريع الكويتي، خالد دليل محمد العازمي، رسالة ماجستير مقدمة إلى كلية الدراسات القانونية العليا، عمان، سنة ٢٠٠٧.

ثالثاً: الدوريات والمجلات

❖ الإرهاب الإلكتروني ومخاطره في العصر الراهن، د. حسن تركي عمير و سلام جاسم عبدالله، مجلة العلوم القانونية والسياسية، جامعة ديالى، عدد خاص المؤتمر العلمي الدولي الثاني للكلية – إشكالية التداخل بين مفهومي الإرهاب وحقوق الإنسان، ٢٠١٣.

❖ الإرهاب السيبراني، د. راجي يوسف محمود البياتي، مجلة تكريت للعلوم السياسية، العدد١٨، ٢٠٢٢.

❖ الارهاب المعلوماتي (الرقمي) وطرق مكافحته، عقيلة هادي عيسى وإسراء جواد حاتم، مجلة السياسية والدولية، كلية العلوم السياسية، جامعة المستنصرية، العدد١٦، لسنة ٢٠١٠.

❖ التحقيق في جرائم الحاسب الألي والانترنيت، محمد الامين البشري، المجلة العربية للدراسات الامنية والتدريب، الرياض، ١٤٢٢هجرية.

❖ جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، توفيق مجاهد، مجلة العلوم القانونية والسياسية، المجلد٠٩، العدد٠٣.

❖ دور الجامعات العربية في خدمة المجتمع في ضوء مسؤوليتها الاجتماعية، زرزار العياشي، مجلة آداب ٥، الكوفة، العدد ٣٢، ٢٠١٧.

❖ دور المنظمات الدولية في مكافحة الإرهاب الرقمي، د. سامر مؤيد عبداللطيف و د. منى محمد عبدالرزاق، مجلة رسالة الحقوق، السنة العاشرة، العدد الثاني، ٢٠١٨.

❖ دور المنظمات الدولية في مكافحة الإرهاب الرقمي، د. سامر مؤيد عبداللطيف وآخرون، مجلة رسالة الحقوق، السنة العاشرة، العدد الثاني، ٢٠١٨.

❖ طبيعة الإرهاب الإلكتروني، د.عبدالقادر الشيخلي، بحث مقدم إلى المؤتمر الإسلامي العالمي المنعقد في مكة المكرمة، ٢٠١٥.

رابعاً: الروابط الالكترونية

❖ مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية، د. بن يحيى الطاهر ناعوس، بحث منشور على شبكة الألوكة، ص٦، الرابط الالكتروني: FwieUr٣http://bit.ly/.