مكافحه الإرهاب الإلكترونى

(ببن القانون الدولى والتشريعات الوطنية)

د. محمد صلاح عبد اللاه ربيع

دكتوراة في القانون الدولى العام- كلية الحقوق- جامعة أسيوط

(ISSN: 2537 - 0758)

مكافحه الإرهاب الإلكترونى

(بين القانون الدولى والتشريعات الوطنية)

د. محمد صلاح عبد اللاه ربيع

الملخص:

تعتبر جريدة الإرهاب الإلكتروني من أهم وأحدث أشكال الإرهاب والأكثر تهديداً للمجتمع الدولِى؛ الأمر الذي أوجب على المجتمع الدولى عقد الإتفاقيات والمعاهدات الدولية، من أجل السعي إلى وضع نصوص قانونية خاصة بمعالجته والتصدي لآثاره؛ إلا أن حداثة هذا النوع من الجرائم أورد إختلافاً واضحاً في مواقف الدول تجاهه؛ بالإضافة إلى معرفة موقف المنظمات الدولية والدول بخصوص الإرهاب الإلكترونى وهذا ما تم تسليط الضوء عليه في بحثنا.

الكلمات المفتاحية: الإرهاب الإلكتروني، الإرهاب السيبرانى، الإرهاب الفضائى.

Abstract:

The crime of cyber terrorism is one of the most important and recent forms of terrorism that is most threatening to the entire international community; the states must be aware of its gravity and urge to conclude international conventions and treaties to seek legal texts in order to address this issue. However, the novelty of this type of crime makes a clear difference in the attitude of States towards it: which is highlighted in ourstudy.

المقدمة

مما لا شك فيه أن الشعوب والمجتمعات البشرية لطالما عانت من العنف، ولكن أبشع صور هذه الجرائم وأخطرها تتمثل في الإرهاب، ولكن مع التطور التكنولوجى الذي يشهده العالم تطورأيضاً الإرهاب وأصبح هناك ما يعرف بالإرهاب الإلكترونى والذي يُعد الجانب السلبي لهذا للتطور، وأصبح الإرهاب الإلكترونى من أحدث وأخطر الجرائم المعلوماتية التي تؤثر على حياة الأفراد والدول، وتجاوزت آثاره الإرهاب التقليدي حيث يصعب الوصول للإرهابيين أو التنبؤ ورصد الهجوم الإرهابى، كما يصعب إثبات المسئولية فيه.

وتعد ظاهرة الإرهاب من أخطر الظواهر التي أثرت بشكل سلبي على المجتمعات، ومع التطور التكنولوجي والتقدم العلمي في المجال المعلوماتي والتقني، أدى إلى ظهور أنماط مستحدثة من الجرائم الإرهابية، لها صلة بالثورة المعلوماتية التي تشهدها حضارة اليوم؛ وهو ما يعرف بجرائم الإرهاب الإلكتروني، وإن كانت تكنولوجيا المعلوماتية تتوفر على مجموعة من الجوانب الإيجابية، التي تظهر في سهولة الحصول على المعلومات، وبالرغم من ذلك فإن سلبيات هذه الظاهرة ونتيجة تطور في الوسائل الإلكترونية بجعل التفاعل عابراً للحدود الجغرافية؛ أصبح هناك ما يسمى بالمجتمعات الافتراضية التي تجمعها شبكة الإنترنت حول اهتمامات مشتركة، مما سهل نقل المعلومات بين الناس باختلاف أهوائهم، وهو ما زاد وجه الإرهاب قبحاً عما كان عليه في الماضي، في الوقت الذي ينطوي فيه على خطورة كبيرة جداً، قد تتجاوز أضراره ما يحدثه الإرهاب التقليدي ألا وهو الإرهاب الإلكتروني[١].

لم يقف الإرهاب عند نمط معين من أنماطه التي بدأ بها في الماضي، بل إن القائمين عليه يطورون أفكارهم الإرهابية بشتى السبل، حيث أصبحت الجرائم الإرهابية المرتبطة بالإنترنت، وأصبح الفضاء الإلكترونى مسرحاً للجريمة[٢].

لذلك تم إختيار موضوع هذا البحث للوقوف على مدى إمكانية مكافحة هذا النوع المستحدث من الجرائم فيما يسمى "بالإرهاب الإلكترونى"، ليكون عنوان البحث "مكافحة الإرهاب الإليكتروني: بين القانون الدولي والتشريعات الوطنية".

أهمية البحث

تكمن أهمية البحث في دراسة وتحديد معالم جريمة الإرهاب الإلكترونى بإعتباره من الجرائم شديدة الخطورة ويجب الاهتمام بها على قدر هذه الخطورة وخاصة في ظل الوضع العالمى الراهن، مما يلزم معه التعاون والتنسيق بين الدول على الصعيد العالمى، وسن قوانين داخلية في إطار تنظيم دولى موحد لمواجهة ومكافحة هذا النوع من الجرائم.

وعلى ذلك نأمل أن يكون هذا البحث المتخصص في دراسة الإرهاب الإلكترونى مساهمة لبداية مراجعة قوانين مكافحة الإرهاب الإلكترونى.

---

[١] د. مصطفى أحمد فؤاد، أصول القانون الدولي العام، منشأة المعارف، الإسكندرية، ٢٠٠٨، ص١٢

[٢] د. أميرة عبد العزيز العربي، جذور الإرهاب وآليات المواجهة، أطلس للنشر والإنتاج الإعلامي، مصر، ٢٠١٩، ص ١٦٧.

(ISSN: 2537 - 0758)

إشكالية البحث:

جريمة الإرهاب الإلكتروني صورة من صور الجريمة الإرهابية، ولكن جريمة الإرهاب الإلكتروني لم تظهر إلا بعد التقدم العلمي الذي شهده العلم، وعلى ذلك فالنصوص التقليدية لم تعد قادرة على مواجهة جريمة الإرهاب الإلكتروني وهو ما يعني بالضرورة إيجاد نصوص قانونية حديثة يمكن من خلالها مواجهة جريمة الإرهاب الإلكتروني، هذا من جهة، ومن جهة ثانية فإن الجريمة تحدث بوسائل لم تحصل بها الجريمة الإرهابية سرابقاً، وأحياناً تشكل هذه الوسائل جرائم بحد ذاتها دون حاجة لاقترانها بوقوع فعل أصلي معاقب عليه، وهذا يعني أن مواجهة جريمة الإرهاب الإلكتروني تستلزم بالضرورة استبعاد العديد من القواعد الجنائية، بل وحتى بعض المبادئ الجنائية الدستورية والدولية؛ كي يتسنى مواجهة هذه الجريمة ومعاقبة مرتكبيها، وبالتالي فإن القواعد التي تحكم الجريمة الإرهابية، سواء من حيث المسؤولية أو من حيث العقاب، تختلف عن القواعد التي تحكم الجرائم العادية، وأحياناً تمثل استثناء عن القواعد العامة، ومدى فعالية النصوص التجريمية في القانون المصرى لمواجهة جرائم الإرهاب الإلكتروني.

أهداف البحث

يهدف البحث إلى معرفة ماهية الإرهاب الإلكترونى وتمييزه عن الإرهاب التقليدي والوقوف على الجهود المبذولة في هذا المجال وإلقاء الضوء على التجربة المصرية في مكافحة الإرهاب وما يجب على الدولة المصرية فعله في الفترة المقبلة للتصدى لهذا النوع من الإرهاب لتكتمل المنظومة التشريعية المصرية.

منهج البحث

تم البحث في هذا الموضوع بالمنهج الوصفى التحليلى لفهم آراء الفقهاء وتحليل النصوص القانونية في التشريعات الداخلية والمعاهدات الدولية والخروج بنتائج من خلال تدقيق الأفكار وتحليلها والتعليق عليها.

وسوف نتناول موضوع الإرهاب الإلكترونى من خلال المبحثين الآتيين:

المبحث الأول: ماهية الإرهاب الإلكتروني

المطلب الأول: تعريف الإرهاب الإلكتروني وخصائصه وأركانه

المطلب الثانى: تأثيرالإرهاب الإلكترونى وصوره وتمييزه عن غيره من الجرائم

المبحث الثاني: الجهود المبذولة لمكافحة الإرهاب الإلكتروني

المطلب الأول: الجهود الدولية لمكافحة الإرهاب الإلكترونى

المطلب الثانى: الجهود العربية لمكافحة الإرهاب الإلكترونى

المطلب الثالث: التجربة المصرية في مكافحة الإرهاب التقليدي والإلكترونى.

المبحث الأول
ماهية الإرهاب الإلكتروني

أن مصطلح الإرهاب الإلكترونى على قدر من الحداثة مما أدى بطبيعة الحال إلى عدم تقديم تعريف واضح ومحدد له، بل يختلف من مكان لمكان ويتطور بقدر تطور التكنولوجيا الواجب توافرها لهذه الطائفة من الجرائم، **وسوف نتناول ماهية الإرهاب الإلكترونى في المطالب الآتية:**

المطلب الأول
تعريف الإرهاب الإلكتروني وخصائصه وأركانه

سوف نتناول في هذا المطلب تعريف الإرهاب الإلكترونى وخصائصه وأركانه من خلال الفرع الآتية:

الفرع الأول: تعريف الإرهاب الإلكتروني.

الفرع الثانى: خصائص الإرهاب الإلكتروني.

الفرع الثالث: أركان جريمة الإرهاب الإلكتروني.

الفرع الأول
تعريف الإرهاب الإلكتروني

أولاً: تعريف الإرهاب بصفة عامة

أن مصطلح الإرهاب يعد من بين المصطلحات التي لم تعرف تعريفاً موحداً حتى الأن، ولكن على أي حال ولكن على أي حال ارتأى الباحث أن يشير إلى بعض التعاريف من أجل الوقوف على تحديد مفهوم الإرهاب الإلكتروني فعلي سبيل المثال عرفته الموسوعة السياسة بأنه: "استخدام العنف– الغير قانوني– (أو التهديد به) بأشكاله المختلفة كالاغتيال والتشويه والتعذيب والتخريب والنسف بغاية تحقيق هدف سياسي معين مثل كسر روح المقاومة والالتزام عند الأفراد وهدم المعنويات عند الهيئات

(ISSN: 2537 - 0758)

والمؤسسات أو كوسيلة من وسائل الحصول على معلومات أو مال وبشكل عام استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية"[٣].

كما يقصد بالإرهاب "كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجانى تنفيذاً لمشروعى إجرامى فردى أو جماعى بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالإتصالات أو المواصلات أو الأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الإستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح"[٤].

وقد ذهب بعض الفقه في تعريفه بأنه "عملية رعب تتألف من ثلاثة عناصر فعل العنف أو التهديد باستخدامه، والخوف الناتج عن ذلك"[٥].

كما عرفت الاتفاقية العربية لمكافحة الإرهاب في الفقرة الثانية من المادة الأولى الإرهاب بأنه "كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعرض أحد الموارد الوطنية للخطر"[٦].

ثانياً: تعريف الإرهاب الإلكترونى

إن مصطلح الإرهاب الإلكتروني أو (cyber terrorism) يتألف من كلمتين: الأولى (cyber) وتعني الإنترنت، والثانية (terrorism) وتعني الإرهاب. كما يشير

---

[٣] د. هشام بشير، "الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي"، آفاق سياسية، العدد ٤٤، القاهرة: المركز العربي للبحوث والدراسات، يونية ٢٠١٤، ص٧٦.

[٤] د. أحمد فتحى سرور، المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠٨، ص٣٢.

[5] Eugen Walter: Terror and Resistance A Study of Political Violence with case studies of some Primitive African communities OXFORD University New, 1999 p.5

[٦] المادة الأولى الفقرة الثانية من الإتفاقية العربية لمكافحة الإرهاب ١٩٩٨.

أيضاً إلى الفضاء الإلكتروني، وهو العالم الافتراضي الذي يشير إلى التمثيل الرمزي والزائف والمجازي للمعلومات[٧].

وكانت بداية استخدام مصطلح الإرهاب الإلكترونى في فترة الثمانيات على يد بارى كولين والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب الإلكترونى ولكنه تبنى تعريف له مقتضاة أنه "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيدلبوجية وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبى مكافئ للأفعال المادية للإرهاب".

كما عرفه جميس لويس بأنه "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنية التحتية الوطنية المهمة مثل الطاقة والنقل أو بهدف ترهيب الحكومة والمدنيين"[٨].

أما دورثى دينينغ فترى أن الإرهاب الإلكترونى بأنه "الهجوم القائم على مهاجمة الحاسوب وان يكون التهديد بهدف الترويع أو إجبار الحكومات أو المجتمعات لنحقيق أهداف سياسية أو دينية أو عقائدية وينبغى أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب"[٩].

أما بالنسبة الإرهاب الإلكتروني فيمكن تعريفه بأنه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الفساد"[١٠].

وأيضاً يمكن تعريف الإرهاب الإلكتروني بأنّه "النشاط غير القانوني الذي يقوم به طرف ما بوساطة التقنية الإلكترونية الرقمية عبر شبكاتها لتحقيق غرض محدد"[١١].

---

[٧] د. حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، التسريبات، التجسس، الإرهاب الإلكتروني، دار الفكروالفن، مدينة السادس من أكتوبر، ٢٠١٤، ص٢٠.

[8] Alix DESFORGES "Cyberterrorisme: quel périmètre?" Fiche de l'Irsem n° 11 décembre 2011 p. 3

[9] DOROTHY E. DENNING "Cyber terrorism" Global Dialogue Autumn 2000 p1

[١٠] د. هشام بشير، "الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي"، آفاق سياسية، العدد ٤، القاهرة: المركز العربي للبحوث والدراسات، يونية ٢٠١٤، ص٧٧.

[١١] د. مصطفى محمد موسى، الإرهاب الإلكتروني "دراسة قانونية– أمنية– نفسية– إجتماعية"، دار الكتب والوثائق القومية المصرية، الطبعة الأولى، القاهرة، الطبعة الأولى، ٢٠٠٩، ص٥.

(ISSN: 2537 - 0758)

وكذلك يقصد الإرهاب الإلكتروني بأنه "النشاط غير القانوني الذي يقوم به طرف ما بوساطة التقنية الإلكترونية الرقمية عبر شبكاتها لتحقيق غرض محدد"[١٢].

كما يقصد بالإرهاب الإلكترونى أيضاً "القيام بعملية إرهابية من شأنها المساس وإحداث خلل يمس بإستقرار الدولة أو يهدف إلى الضغط على الحكومة بإستعمال طرق تدخل في صنف الجرائم المعلوماتية"[١٣].

ويعرفه البعض "الإرهاب الإلكترونى" بأنه "العدوان أو التخويف أو التهديد المادى أو المعنوى الصادر من الدول، أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى أصناف العدوان وصور الإفساد"[١٤].

كما عرف الصليب الأحمر الإرهاب الإلكترونى أنه "عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات أو التلاعب بها من قبل منفذ عملية الاختراق، واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبنية التحتية"[١٥].

ونلاحظ أيضاً أن الاتحاد الأوربي بدوره يقرر بجرائم الإرهاب الإلكتروني من خلال اتفاقية بودابست، سنة ٢٠٠١ فقد عرفته على أنه "هجمات غير مشرروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات والشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة".

---

[١٢] د. مصطفى محمد موسى، الإرهاب الإلكتروني "دراسة قانونية- أمنية- نفسية- إجتماعية"، دار الكتب والوثائق القومية المصرية، الطبعة الأولى، القاهرة، ٢٠٠٩، ص٥.

[١٣] د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، دار الوفاء القانونية، القاهرة، ٢٠١١، ص٢٠٦.

[١٤] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته، محاضرة ألقيت بملتقى دولى بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، أيام ٢-٤/ ٩/٢٠١٤، ص٩.

[١٥] د. حسن سعد محمد عيسى سند، جرائم الإرهاب الإلكترونى من منظور القانون الدولى العام، بحث منشور مجلة كلية الحقوق، جامعة المنيا، المجلد الخامس، العدد الثانى، ديسمبر ٢٠٢٢، ص١٢.

وبالتالي فلكي ينعت شخص ما بأنه إرهابي على الإنترنت، وليس فقط مخترقاً، فلابد أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب[١٦].

والجدير بالذكر أن وزارة الدفاع الأمريكية هي الأخرى عرفت الإرهاب الإلكترونى بأنه "استخدام أجهزة الكمبيوتر والأنترنت لإجراء حرب ضمن الفضاء الإلكترونى، وهذا وعرفته الإتفاقية الأولى لمكافحة الإجرام عبر الأنترنت في بوتسدام ٢٠٠١ على أنه "هجمات غير مشروعة أو تهديدات لهجمات ضد الحواسيب أو الشبكات أو المعلومات أو الشعوب أو المجتمع الدولى بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، وبالتالي ينعت الشخص بأنه إرهابى على الأنترنت وليس مخترفاً، فلابد أن تؤدى الهجمات التي يشنها إلى عنق ضد الأشخاص أو الممتلكات أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب"[١٧].

أما الاتفاقيات العربية فيلاحظ أنها في ظل حداثة مصطلح الإرهاب الإلكتروني، لم تتطرق إلى تعريف هذه الجريمة، بل اكتفت بتحديد السلوكيات الإجرامية المرتكبة بالتقنية الحديثة، ونجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ذهبت إلى تحديد أفعال الإرهاب الإلكتروني دون تقديم تعريف له، وذلك في نص المادة (١٥) للجرائم المتعلقة بالإرهاب، والمرتكبة بواسطة تقنية المعلومات:

١- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
٢- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
٣- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
٤- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات[١٨].

---

[١٦] د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية "معلقاً عليها"، دار النهضة العربية، القاهرة، ٢٠١١، ص ٢٠٠.

[١٧] د. حسن سعد محمد عيسى سند، جرائم الإرهاب الإلكترونى من منظور القانون الدولى العام، المرجع السابق، ص١٢.

[١٨] المادة (١٥) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢٠١٠/١٢/٢١، وكذلك في المادة (١٦) الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات:
١- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

(ISSN: 2537 - 0758)

ويمكن من خلال كل هذه التعريفات السابقة تعريف "الإرهاب الإلكتروني" بأنه "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. ولكي يعتبر المرء إرهابياً على الإنترنت، وليس فقط مخترقاً، فإن الهجمات التي يشنها يجب أن تؤدي إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب".

والملاحظ بخصوص هذه التعريفات السابقة هو الارتباط الوثيق للإرهاب المعلوماتي بالمستوى المتقدم الذي باتت تكنولوجيا المعلومات تلعبه في كافة مناحي الحياة، فضلاً عن حجم المخاطر التي يمكن أن يسببها والتي قد تلحق الشلل التام بأنظمة القيادة وتؤدي إلى قطع شبكات الاتصال بين الوحدات والقيادات المركزية، وتعطيل أنظمة الدفاع الجوي أو اختراق النظام المصرفي أو إرباك حركة الطيران المدني أو غيرها.

الفرع الثانى
خصائص الإرهاب الإلكتروني

يتسم الإرهاب الإلكتروني بمجموعة من السمات والخصائص تزيد من خطورته، والتي يعد معرفتها ودراستها مدخلاً مناسباً لمواجهته وتجنب مخاطره، وتتمثل أبرز خصائص الإرهاب الإلكتروني فيما يلي:

١. **الإرهاب الإلكتروني عابر للدول**:

حيث إنه في الغالب يكون الجاني في بلد والجريمة الإرهابية الواقعة في بلد آخر، ولعل الذي ساعد ذلك هو انتشار شبكات المعلومات "الانترنت"، وترابطها مع بعضها البعض حتى أصبح يُقال بأن العالم أصبح قرية واحدة[١٩].

٢- الترويج للمخدرات والمؤثرات العقلية أو الإتجار بها.

٣- الإتجار بألشخاص.

٤- الإتجار بالأعضاء البشرية.

٥- الإتجار غير المشروع بالأسلحة.

[١٩] د. محمد محي عوض، مشكلات السياسة الجنائية المعاصرة جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣، ص٦٠، د. محمد عبد الله،

فيرى بعض فقهاء القانون الجنائي أن جريمة الإرهاب الالكتروني جريمة دولية[٢٠]، وذلك إذا خالفت هذه الجريمة القواعد الدولية سواء كانت من القواعد المنصوص عليها في الإتفاقيات الدولية أو القواعد الدولية العرفية[٢١].

فالشبكة العالمية للمعلومات فتحت مجالاً حيوياً للأنشطة التي تقودها الجماعات الإرهابية، إذ بات مؤكداً اليوم العلاقة الوطيدة بين الإرهاب واستخدام الوسائل التكنولوجية بهدف زعزعة استقرار وأمن المجتمعات والدول، فالجريمة الإرهابية بعدما كانت محلية محضة تحولت لتصبح عابرة للحدود[٢٢].

٢. الإرهاب الإلكتروني صورة ناعمة من صور الإرهاب:

والسبب في ذلك هو مدي السهولة التي يتم بها ارتكاب جريمة الإرهاب الإلكتروني، حيث أنها لا تحتاج إلى مجهود عضلي كالجرائم الإرهابية التقليدية، فالجريمة الإلكترونية ومنها جرائم الإرهاب الإلكتروني ترتكز على الدراية الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات التكنولوجيا والمعلومات[٢٣].

فمن خلال الاعتماد على استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، حيث يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي في أنه يعتمد على التقنيات الحديثة في مجال المعلوماتية والاتصالات، وكل ما هو جديد في هذا المجال، واستغلال الإمكانات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، في ارتكاب وتنفيذ جرائمه. فعلى سبيل المثال أجهزة ونظام تحديد المواقع عبر الأقمار الصناعية (Global Positioning System) المعروفة بـ(GPS) والهواتف الجوالة المتصلة بالأقمار الصناعية، وبرامج الكمبيوتر للتعرف على الأصوات

موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص٩٧.

[٢٠] د. محمود صالح العدلى، الجريمة الدولية، دار الفكر الجامعى، الإسكندرية، ٢٠٠٤، ص٦٢-٦٣

[٢١] د. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٦، ص١٥٦-١٥٧.

[٢٢] د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٢، ص٥.

[٢٣] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص٨٢.

(ISSN: 2537 - 0758)

باللغات المختلفة، إلى غير ذلك، ما هي إلا أساليب تكنولوجية حديثة في العصر الرقمي، تحمل مع غيرها آفاقاً واعدة في الحاضر والمستقبل، ومع ذلك قد يساء استخدامها من قبل البعض في تحقيق أهداف واعتداءات إجرامية وإرهابية، الإرهاب الصوتي(٢٤)، فالتكنولوجيا الرقمية الحديثة وبخاصة في مجالي المعلومات والاتصالات في تقدم مذهل ومتسارع يومياً، وقد يساء استخدامها في اعتداءات إجرامية أو إرهابية، تتطلب من المجتمع الدولي كله اقتراح واتخاذ كافة أساليب وإجراءات العلاج العاجلة والفعالة لمكافحة الإرهاب في العصر الرقمي(٢٥).

٣. سهولة ارتكاب جرائم الإرهاب الإلكتروني:

والسبب الرئيس في ذلك هو غياب الرقابة والسيطرة على الشبكات المعلوماتية، حيث في ظل ما يتمتع به شبكة المعلومات العالمية من كونها شبكة افتراضية لا يمكن التحكم فيما يعرض عليها، حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة، ويقتصر إمكانية الجهات الرقابية على مجال الشبكات الافتراضية في منع الوصول إلى بعض المواقع من خلال حجبها أو إغلاقها وتدميرها بعد نشر المجرم ما يريد(٢٦).

فيمكن لمن لديه بعض المعارف والمعلومات البسيطة عن التعامل مع شبكة المعلومات الدولية الانترنت وادواتها وعلوم الحاسب ان يقوم بالعديد من جرائم الإرهاب الإلكتروني بسهولة ويؤدي إلى احداث خسائر عديدة تتجاوز حدود الدول وقد تمت إلى العالم اجمع، ومما زاد من سهولة استخدامه توفر خدمات الانترنت من خلال الاجهزة النقالة وحاسبات الجيب التي اصبحت في متناول الجميع في اي مكان وفي اي وقت، حيث يعتمد الإرهاب الإلكتروني على استغلال الإمكانات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار والدماء لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في منزله أو في مكتبه أو

---

(24) Haut-Commissariat des Nations Unies aux droits de l'homme Fiche d'information n° 32 chap. III sect. H

(٢٥) د. جمال على دهشان، الإرهاب في العصر الرقمى (الإرهاب الإلكترونى) "صوره، مخاصره، آليات مواجهته"، بحث منشور في مركز المعرفة الدولى، المجلد (١)، العدد (٣)، ٢٠١٨، ص٩٤.

(٢٦) د. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، ٢-٣ يونيو ٢٠٠٨، ص ٤٨.

في غرفته الفندقية، وبعيداً عن أنظار السلطة والمجتمع، فبدلاً من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، فكل ما يحتاجه الإرهابي المحترف في هذا المجال الحيوي والمعقد هو جهاز حاسب آلى واتصال بشبكة الإنترنت مما يتيح لهذا الإرهابي القيام بأعمال تخريبية وهو آمن في مقره بواسطة نقرات بسيطة على لوحة المفاتيح ودون أن يترك لنفسه أثراً، هذه النقرات على لوحة المفاتيح قد تنطوي على أوامر موجهة لبعض الخلايا للقيام بأعمال إرهابية معينة. ويجب أن نعترف أن الإنترنت لها مجال مفتوح وواسع وبلا حدود ويتوسع في كل يوم، ويمكنك من موقعك من أي بلد الوصول لأي مكان دون أوراق أو قيود، وكل ما تحتاجه هو بعض المعلومات لتستطيع اقتحام الحوائط الإلكترونية. كما أن تكاليف القيام بمثل هذه الهجمات الإلكترونية لا يتجاوز أكثر من حاسب إلى واتصال بشبكة الإنترنت[٢٧].

٤. صعوبة إكتشاف وإثبات جرائم الإرهاب الإلكترونى

إن الطابع الدولى لجرائم الإرهاب الإلكترونى التي تتجاوز حدود الدولة ليشمل عدة دول، وكذلك الخبرة والكفاءة العالية التي يتمتع بها الإرهابى الإلكترونى في مجال تقنية المعلومات تجعل من الصعب إكتشاف هوية مرتكب الجريمة وتحديد مكانه، ومن الصعب إثبات مثل هذه الجرائم أمام نقص الخبرة لدى بعض الجهات الأمنية والقضائية في البحث والتحرى وكشف هذه الجرائم التي يسهل على إرهابى خبير في المعلومات محو آثارها في الفضاء الإلكترونى[٢٨].

كما أن الإرهاب الإلكتروني لا يتخذ شكلاً واحداً او اسلوب واحد وانما تتعدد اشكاله وتتنوع صوره وأساليبه، تتمثل اشكاله في التجسُس الإلكتروني، والاختراقات، أو القرصنة على المواقع الحيوية للمُنشآت، والمؤسسات الرسمية في المجُتمعات المخُتلفة، والتجنيد الإلكتروني من خلال ما يُطلق عليه التلقين الإلكتروني، وأخيراً التهديد والترويع الإلكتروني، كما ان ادواته متعددة متمثلة في الفيروسات اختراق البيانات وتدميرها

---

[٢٧] د. جمال على دهشان، الإرهاب في العصر الرقمى (الإرهاب الإلكترونى) "صوره، مخاصره، آليات مواجهته"، المرجع السابق، ص٩٦-٩٧.

[٢٨] د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، دار الوفاء القانونية، القاهرة، ٢٠١١، ص٢١٩.

(ISSN: 2537 - 0758)

والتجسس وتجنيد الإرهابين وجمع الاموال وتمويل العمليات الإرهابية وحروب الدعاية للأفكار المتطرفة والهدامة وغيرها[٢٩].

وتعود صعوبة اكتشاف جريمة الإرهاب الإلكترونى إلى عدة أسباب أهمها:

١- الطابع الدولي لجرائم الإرهاب الإلكتروني، فهي تتجاوز حدود الدولة لتشمل مجموعة من الدول، ما يصعب تحديد مكان مرتكبي هذه الجرائم.

٢- الخبرة والكفاءة العالية التي يتمتع بها بع الإرهابيين في مجال تقنيرة المعلومات، التي تمكنهم من محو آثار الجرائم التي يرتكبونها بكل سهولة في الفضاء الإلكتروني، ونقص الخبرة لدى بعض الجهات الأمنية والقضائية في اكتشاف هذه الجرائم.

٣- التطورالتكنولوجي السريع في تقنية المعلومات، الذي يصعب من الإلمام بجميع جوانبه، واستخلاص الدليل الرقمى من بيئة افتراضية[٣٠].

وبعد التوصل لتحديد مصطلح الإرهاب الإلكتروني، تبقي إلى أن نشير إلى الأسباب التي تجعل الجماعات الإرهابية أن تلجأ إلى استخدام الفضاء الإلكتروني في ارتكاب جرائمها الإرهابية **وهذه الأسباب يمكن إجمالها على النحو التالي:**

١- انخفاض تكلفة الآليات الإلكترونية مقارنة بالأدوات التقليدية التي تتم بها العمليات الإرهابية كالقنابل والأسلحة.

٢- صعوبة ملاحقة القائمين على عمليات الإرهاب الإلكتروني.

٣- الفضاء الإلكتروني يوفر للإرهابين أهدافا متعددة يستطيعون مهاجمتها لتحقيق أهدافهم، كمهاجمة شبكات الحاسب الخاصة بالحكومات أو الشركات الخاصة وغيرها.

٤- لا تحتاج هجمات الإرهاب الإلكتروني إلي تواجد المهاجم والهدف في المكان ذاته، حيث تتم الهجمات الإلكترونية عن بعد.

٥- تستطيع هجمات الإرهاب الإلكتروني أن تلحق الضرر بعدد أكبر من الأفراد مقارنة بالهجمات التقليدية، وهو ما يساعد تلك الجماعات الإرهابية على جذب المزيد من الاهتمام الإعلامي والحكومي[٣١].

---

[٢٩] د. جمال على دهشان، الإرهاب في العصر الرقمى (الإرهاب الإلكترونى) "صوره، مخاصره، آليات مواجهته"، المرجع السابق، ص٩٥.

[٣٠] المستشار/ عبد الفتاح بيومى، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧، ١٩٨.

الفرع الثالث
أركان جريمة الإرهاب الإلكتروني

إن جريمة الإرهاب الإلكتروني لا تختلف في أركانها عن جريمة الإرهاب بالمعنى التقليدي، إلا من حيث الوسيلة والأداة التي تستخدم في ارتكابها، فهي تقوم على ركن مادي وركن معنوي.

أولاً: الركن المادي:

الركن المادي للجريمة هو فعل خارجي له طبيعة مادية ملموسة تدركه الحواس، ولا توجد جريمة بدون ركن مادي، إذ بغير ماديات الجريمة لا ينال المجتمع اضطراب ولا يصيب حقوق الأفراد عدوان، وقيام الجريمة على ركن مادي يجعل إقامة الدليل عليها ميسوراً، وعناصر الركن المادي ثلاثة: الفعل أو السلوك والنتيجة وعلاقة السببية بينهم:

أ) السلوك الإجرامي:

هو النشاط الخارجي الذي يصدر من الجاني ليحقق النتيجة الإجرامية التي يعاقب عليها القانون، بحيث يكون الموضوع الذي يقع عليه السلوك أو الفعل الإجرامي محل حماية من المشرع. إن السلوك الإجرامي بوصفه عنصراً في الركن المادي للجريمة التقليدية يمكن رؤيته بشكل ملموس والتأكد منه كفعل القتل أو السرقة، ولكن صعوبة الجريمة الإلكترونية، أن الجريمة ترتكب عن طريق معلومات تتدفق عن طريق الحاسب الآلي والتي لا يمكن الإمساك بها مادياً[٣٢]، والنشاط الإجرامي في جريمة الإرهاب الإلكتروني يتطلب بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، فيقوم المجرم مثلاً بتحميل برامج اختراقية، أو تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، وكما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها، ويصعب الفصل

---

[٣١] د. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، ٢-٣ يونيو ٢٠٠٨، ص١٤.

[٣٢] د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص١١٤، د. محمد أبو المجد محمد سليم، بحث بعنوان المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، مجلة البحوث القانونية والإقتصادية (المنصورة)، ٢٠٢١، ص١٠.

(ISSN: 2537 - 0758)

بين العمل التحضيري والبدء في نشاط إجرامي في جرائم الإرهاب الإلكتروني، فشراء برامج اختراق، ومعدات لفك شفرات وكلمات المرور تمثل جريمة في حد ذاتها[٣٣].

وقد يتخذ الفعل الإجرامي في جرائم الإرهاب الإلكتروني صوراً وأشكالاً متعددة منها التهديد بواسطة المواقع الإلكترونية باستخدام العنف وتعريف سلامة المجتمع للخطر، أو استخدام برامج إلكترونية لتعطيل سبل الاتصالات واختراق الشبكات أو التشويش عليها أو تعطيل وسائل النقل، أو استخدام برامج إلكترونية خبيثة للدخول إلى أنظمة الحاسب وسبل الاتصال وتعطيلها من خلال محو جميع البيانات والبرامج أو تدميرها.

وكذلك استخدام الشبكة الإلكترونية لنشر أو إعلان أو إنشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بعمل إرهابي، أو الترويج لأفكارها أو تمويلها. والسلوك في جريمة الإرهاب الإلكتروني يتم عن طريق وسيلة وهي عبارة عن جهاز إلكتروني أيا كان نوعه أو شكله واتصال بشبكة الإنترنت، وقد يكون السلوك إيجابي بمباشرة الفعل من الجاني وهذه أغلب صور الإرهاب الإلكتروني وقد يكون سلبي بالامتناع عن فعل كان من الواجب اتيانه، كعدم إبلاغ السلطات المختصة بوجود مخطط إرهابي[٣٤].

ومن أهم وسائل الإرهاب الإلكتروني المستخدمة في جريمة الإرهاب الإلكتروني:

١ – <u>البريد الإلكتروني:</u>

يعد من أبرز وسائل الإرهاب الإلكترونى، حيث يستخدم البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، وترويج الأفكار ونشرها عبر المراسلات الإلكترونية، حيث يعتبر البريد الإلكتروني هو خدمة تسمح بتبادل الرسائل الإلكترونية والمعلومات مع الآخرين عبر شبكة الإنترنت لما تمثله من سرعة في إيصال الرسائل وسهولة الاطلاع عليها في كل مكان.

وكذلك يقوم الإرهابيون باختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم والتجسس عليها وذلك للاستفادة منها في عملياتهم الإرهابية[٣٥].

---

[٣٣] د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص١١٣.

[٣٤] د. محمد أبـو المجـد محمد سـليم، بحث بعنوان المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، مجلة البحوث القانونية والإقتصادية (المنصورة)، ٢٠٢١، ص١١.

[٣٥] د. محمد أبو المجد محمد سليم، المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، المرجع السابق، ص١٢.

٢- إنشاء مواقع الانترنت:

سهلت على المنظمات الإرهابية توسيع أنشطتهم من خلال تبادل الآراء والأفكار والمعلومات، حيث يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة المعلوماتية (الإنترنت) لنشر أفكارهم وتعليم الوسائل التي تساعد على القيام بالعمليات الإرهابية، مثل مواقع لتعليم صناعة المتفجرات وكيفية اختراق المواقع وتدميرها، وطرق نشر الفيروسات وكذلك اختراق البريد الإلكتروني، كما أن الإرهابيون يستخدمون المواقع لنشر معلومات حول كيفية إعداد المتفجرات والمواد السامة وصناعة الصواعق وتعتمد في خططها على طرق بسيطة تتيح للجميع الدخول إلى مواقع محجوبة[٣٦].

٣- اختراق وتدمير المواقع:

تتم عملية الاختراق السيبراني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وتدمير المواقع هو الدخول غير المشروع بهدف تخريب الموقع أو نشر رسائل تشيد بالإرهاب[٣٧].

ب) النتيجة الإجرامية:

وهي العنصر الثاني من عناصر الركن المادي، وهي عبارة عن الأثر أو الضرر الذي يترتب على السلوك الإجرامي، وهي ترتبط بشكل كبير بعنصر الخطر وتتعلق بالترويع والتخويف، ويستخدم لتحقيق هذه النتيجة وسائل نفسية، وتظهر النتيجة في جريمة الإرهاب الإلكتروني من خلال ارتباطها بالآثار السلبية التي صاحبت ظهور الإنترنت، فقد تغيرت أنماط الحياة بظهور الحاسبات الآلية، والنتيجة الإجرامية في جريمة الإرهاب الإلكتروني تتحقق من خلال حالة الخطر التي يوقعها الجناة في المجتمعات، فهو يهدد المصالح العامة ويؤدي بالإخلال بالنظام العام للمجتمع[٣٨].

---

[٣٦] د. محمد عبد اللطيف عبدالعال، جريمة الإرهاب، دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٤م، ص٥٤.

[٣٧] د. عبد الله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكترونى في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة، ٢٠٠٠.

[٣٨] د. محمد عبد الحميد عرفه، د. أمين مصطفى محمد، علم الإجرام والعقاب، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٦، ص١٤٤.

(ISSN: 2537 - 0758)

ج) علاقة السببية:

يقصد بعلاقة السببية هي العلاقة بين السلوك الإجرامي والنتيجة الإجرامية، بمعنى أن السلوك الإجرامي هو السبب في إحداث هذه النتيجة الإجرامية، ولولا هذا السلوك ما كانت لتحدث هذه النتيجة، وترجع أهمية علاقة السببية أن تحققها شرطاً أساسياً من شروط المسئولية الجنائية، فلو كانت النتيجة الإجرامية ناتجة عن سلوك وكان هناك إرادة حرة واعية توافرت أسباب قيام المسئولية الجنائية، أما إذا لم يكن هناك علاقة بين النتيجة الإجرامية والسلوك انتفت بذلك المسئولية الجنائية.

وبذلك يستطيع أن تقول أن الركن المادي لجريمة الإرهاب الإلكتروني يتكون من ثلاثة عناصر هي: السلوك والتمثل في أعمال التهديد والترويع في حين النتيجة الإجرامية تتمثل في إيذاء الأشخاص وإلقاء الرعب بينهم أو تعريض حياتهم وأمنهم للخطر أو إلحاق الضرر بالبيئة أو الاتصالات أو المواصلات أو المباني والأملاك العامة والخاصة والرابطة السببية تتمثل في أن يكون السلوك من شأنه أن يؤدي إلى النتيجة وفقا للمجرى العادي للأمور[٣٩].

ثانياً: الركن المعنوي:

لا يكفي لتقرير المسئولية الجنائية أن يصدر عن الجاني سلوك إجرامي بل لابد أن يتوافر ركن معنوي، وهو الحالة النفسية للجاني وقت ارتكاب الجريمة، حيث لا تقوم الجريمة بدونه، فلابد من توافر الإرادة لدى الجاني وقت ارتكاب الجريمة، وجريمة الإرهاب الإلكتروني من الجرائم المقصودة والتي يلزم توافر القصد الجنائي لارتكابها بشقيه العلم والإرادة، وكذلك قصد خاص وهو الهدف البعيد الذي يرمي إليه الجاني من الفعل وهو تعريض سلامة المجتمع وأمنه للخطر وإلقاء الرعب بين الناس.

وجريمة الإرهاب الإلكتروني لابد من توافر القصد الجنائي منها لأنها من الجرائم المقصودة، وذلك بأن يكون الجاني محيطا بحقيقة النشاط الإجرامي وأن نشاطه عدواناً على حق يحميه القانون، ويحيط الجاني علما بأن من شأن هذه الأفعال الإرهابية المساس بحق المجني عليه، وأن هدفها هو الإضرار بالغير، لذلك يجب أن يعلم الجاني بحقيقة سلوكه، أن يأتي عملاً إرهابيا يمثل الاعتداء على مصلحة أو حق يحميه القانون

[٣٩] د. محمد أبو المجد محمد سليم، المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، المرجع السابق، ص١٣.

ويعلم بعناصر الركن المادي وأن يتوقع علاقة السببية بين ما يقوم به من عمل إرهابي والنتيجة الإجرامية(٤٠).

ولا يكفي لتوافر القصد الجنائي علم الجاني بأن الأفعال التي يقوم بها من شأنها أن تؤدي إلى النتيجة الإجرامية وإنما يلزم أيضاً أن تتجه إرادة إلى إتيان الفعل مع وقوع الخطر وعلمه بما ينتج عنه وانصراف إرادته الحرة الواعية إلى تحقيق تلك النتيجة، والإرادة تنصب على السلوك الإجرامي وعلى النتيجة المعاقب عليها، فيجب أن تتجه إرادة الجاني إلى تبني السلوك الإجرامي، باستخدام الوسائل الإلكترونية والتي تهدف إلى إثارة الشغب والخوف بين الناس، وتعريض سلامة وأمن المجتمع للخطر، ويجب أن يكون الجاني متمتعاً بإرادة حرة واعية حال ارتكاب الجريمة، فلا ينسب السلوك معنويا لمن لم يكن لديه القدرة على الاختبار أو التمييز ساعة ارتكاب الجريمة، ولابد أن يكون أيضاً لدى الجاني قصد خاص في جريمة الإرهاب الإلكتروني وهو الإخلال بالنظام العام عن طريق بث الرعب واثارة الخوف والاضطراب في المجتمع، وهو الهدف البعيد للجاني وهو إثارة الرعب والخوف في المجتمع(٤١).

المطلب الثانى

تأثير الإرهاب الإلكترونى وصوره وتمييزه عن غيره من الجرائم

للإرهاب الإلكترونى تأثير مدمر وخطير وتختلف صوره على الأفراد والدول والمؤسسات، وذلك ما يجعله يتداخل مع غيره من الجرائم لذلك **سوف نتناول تأثيره وتمييزه عن غيره من الجرائم من خلال الفروع التالية:**

الفرع الأول: تأثير الإرهاب الإلكترونى

الفرع الثانى: صور الإرهاب الإلكترونى

الفرع الثالث: تمييز جريمة الإرهاب الإلكتروني عن غيرها من الجرائم

---

(٤٠) د. محمد أبو المجد محمد سليم، المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، المرجع السابق، ص١٤.

(٤١) د. كامل السعيد، شرح الأحكام العامة في قانون العقوبات، الدار العلمية للنشر والتوزيع، ٢٠٠١، ص٢٨٢.

(ISSN: 2537 - 0758)

الفرع الأول
تأثير الإرهاب الإلكترونى

إن مجال عمل جريمة الإرهاب الإلكتروني هو البيئة الافتراضية، ولها تراثيرات عدة، فإما أن تحقق الهدف النهائي للعمليات الإرهابية، أو تكون بمنزلة مرحلة في رحلة الإرهاب تحقيقاً لأغراضه وبواعثه، وعند تحليل أهداف الهجمات الإرهابية الإلكترونية والنتيجة النهائية التي قد يحدثها الهجوم، نجد أن لجريمة الإرهاب الإلكتروني أربعة تأثيرات، بعضها يتناسق مع تأثيرات الإرهاب التقليدي، والأخرى يتميز بها (الإرهاب الإلكتروني) **ومن أهم هذه التأثيرات التي تسببها جريمة الإرهاب الإلكتروني:**

أ) فقدان السلامة والكفاءة نظم المعلومات:

إن أساس تكامل النظم والبيانات هو حماية المعلومات من التعديل أو التغيير غير الصحيح بها، فإذا تم إجراء تغييرات غير مصرح بها على البيانات أو نظام تكنولوجيا المعلومات من خلال أفعال متعمدة أو عرضية ولم يتم تصحيحه أو إعادة الأمر لطبيعته، فقد يؤدي الاستخدام المتواصل للنظام الملوث أو البيانات التالفة إلى عدم الدقة أو الاحتيال أو اتخاذ قرارات خاطئة، وبالتالي فقدان السلامة والكفاءة من ضمان أنظمة تكنولوجيا المعلومات[٤٢].

ب) عدم التوفر نظم المعلومات:

إذا تم مهاجمة نظام تكنولوجيا المعلومات ذي الأهمية الكبيرة، وجعله غير متاح للمستخدمين، فمن المحُتمل أن تتأثّر مهمة المنظومة المستهدفة، فمثلا قد يؤدي فقدان وظائف النظام والفعالية التشغيلية إلى ضياع الوقت الإنتاجي، ما يعوق أداء المستخدمين النهائيين لوظائفهم في دعم مهمة المنظومة[٤٣].

ج) التأثير على سرية البيانات والمعلومات:

تهدف سرية النظم والبيانات إلى حماية المعلومات الحساسة من الانتشار لدى عموم الناس، وقد يؤدي الكشف غير المصرح به أو المفاجئ إلى نتائج كارثية، ومن أمثلة ذلك

---

[٤٢] د. أحمد يوسف جمعة، الإرهاب السيبراني والعملات الافتراضية والتجسس الإلكتروني، دار الأهرام للنشر والتوزيع، المنصورة، ٢٠٢١، ص٦٣.

[٤٣] د. أحمد يوسف جمعة، الإرهاب السيبراني والعملات الافتراضية والتجسس الإلكتروني، المرجع السابق، ص٦٤.

في عام ٢٠٠١ تم الهجوم على البرلمان الهندي عبر الإنترنت، حيث تمكن المهاجمون من تزوير بوابة الدخول للموقع، وقاموا بتحميل الشعار الرسمي لوزارة الشؤون الداخلية ومخطط لمبنى البرلمان ووثائق أخرى سرية، وقد اتهمت باكستان بذلك كون؛ لأن اللاب توب الذي استعمل في الهجوم تم تزويده بالإنترنت من باكستان.

د) الضرر المادي أو البدني أو إحداث الوفاة:

وذلك من خلال التأثير على أنظمة تكنولوجيا المعلومات التي تتحكم في تشغيل جزء كبير من البنية التحتية، مثل شركات النقل والطاقة والمياه، وما قد يترتب عليه من أضرار جسيمة[٤٤].

الفرع الثانى
صور الإرهاب الإلكترونى

من أهم خصائص الإرهاب الإلكترونى أنه يتم بواسطة تكنولوجيا المعلومات فتتعدد أشكاله وصوره بحكم أنه ينشا في عالم إفتراضى غير مرئى ولذلك يصعب رصده وملاحقته، **وتتمثل صور الإرهاب الإلكترونى في الآتى:**

أ- الإرهاب الإلكترونى ضد الأفراد

يتمثل الإرهاب الإلكتروني الموجه ضد الأفراد كل التصرفات التي يقوم بها من خلال وسائل التكنولوجيا (الانترنيت الفاكس الهاتف .... الخ) مهما كان نوعها أو حجمها ضد شخص طبيعي لاختراق خصوصيته، بعدما أصبح من الممكن التداول إلى الأحاديث عبر الشبكات، إذ شهدت شبكة الانترنيت عدة حالات للابتزاز المعلوماتي من قبل أشخاص تمكنوا بوسيلة أو بأخرى من اختراق نظام الأمن للبريد الإلكتروني أو التنصت على حلقات الدردشة عبر الإنترنت.

ما يساعد على استخدام الانترنيت- مثلا- كوسيلة للابتزاز أن التواصل عن بعد يتيح فرصا عدة لتقمص الشخصيات لخداع الآخرين عبر الجهة الأخرى من العالم وراء هواتفهم أو حواسيهم، لعدة أسباب كالبوح بأسرارهم الشخصية حتى يمكن استغلالها صدهم، علاوة على ذلك تتيح التكنولوجيا وسائل مبتكرة للتهديد، الابتزاز، القرصنة أو الاختراق نذكر منها على سبيل المثال التهديد بالوثائق المزورة التي يتم تزويرها إلكترونياً بشكل إحترافي لا يمكن ملاحظة الفارق بينها وبين الأصلية وكذلك التهديدات الأمنية

[٤٤] د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، ٢٠٠٦، ص٩٠.

(ISSN: 2537 - 0758)

اختراق حساب بنكي او السرقة باستخدام بطاقات الائتمان الخاصة بالتجارة الإلكترونية[٤٥].

ب- الإرهاب الإلكتروني ضد المؤسسات

بعد من أخطر مصادر التهديد الإلكتروني للمؤسسات من خلال اختراق شبكات اتصالاتها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة، وفي ظل المنافسة التي تشهدها معظم الأسواق الحالية، أصبح التجسس على مختلف أنشطة الشركات من قبل منافسيها مصدر قلق حقيقي.

من المظاهر الأخرى لإرهاب المؤسسات إلكترونياً، إسقاط موقع المؤسسة على الإنترنت، وذلك بأن يصوب إليه العديد من الرسائل المولدة تلقائياً التي تظل تنهمر إلى أن تصل إلى حد يعجز فيه الموقع تماماً عن ملاحقتها ليسقط، وتسقط بالتالي معه جميع المعاملات التجارية والمالية الإلكترونية التي يوفرها موقع المؤسسة لعملائه وشركاته.

ومن الوسائل الأخرى التي تتعرض لها المؤسسات، فك شفرة حماية سرية البيانات التي تتبادلها مع الآخرين خارج المؤسسة من عملاء ووكلاء وما شبه، وقد سبق أن عرف العالم تهديد حيث قام شاب من النرويج نشر برنامج في عدة أسطر يمكن به فك الشفرة الرقمية التي تبث بها الأفلام عبر الشبكة، وهو دليل الإرهاب في سطو المؤسسات وهو التهديد نفسه الذي تواجهه حماية الملكية الفكرية[٤٦].

ج- الإرهاب الإلكتروني ضد الدول

صورة الإرهاب الإلكتروني ضد الدول تكمن في الدخول إلى شبكات التحكم في المرافق العامة، مما يتسبب في شلل للبنى التحتية الأساسية، بل واحتمال تدميرها كلياً فالدول أصبحت معرضة لما يسمى الدمار الشامل باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في جيوش الفيروسات التي تخترق حدود الدول وتحطم البنية التحتية المعلوماتية، كما تزايد الترابط بين هذه الشبكات زاد من تعرض الدول لهذا التهديد حيث

---

[٤٥] د. علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص٩.

[٤٦] د. علاء الصراط الغامدي، المرجع السابق، ص١٥.

أن أغلب الدول تستخدم شبكات المعلومات في إدارة معظم شئونها الداخلية والخارجية، وهذا النوع يمس مباشرة المصالح الاقتصادية للدولة[٤٧].

الفرع الثالث

تمييز جريمة الإرهاب الإلكتروني عن غيرها من الجرائم

قد تتشابه جريمة الإرهاب الإلكتروني من حيث مضمونها وطبيعتها مع بع الصور الإجرامية الخطيرة الأخرى، لذلك كان من الضروري تمييز جريمة الإرهاب الإلكتروني عن غيرها من الصور الإجرامية فيما يلي:

أولاً: التمييز بين جريمة الإرهاب التقليدي والإرهاب الإلكتروني:

يتفق الإرهاب التقليدي والإرهاب الإلكتروني باعتبارهما من الأعمال غير مشروعة التي جرمتها التشريعات والاتفاقيات الدولية، ويتفقان أيضاً من حيث الهدف أو الغاية التي يسعيان إلى تحقيقها، ألا وهي نشر الرعب والخوف في نفوس الآخرين، وابتزاز الدول، ومحاولة السيطرة على نظامها الداخلي وتمويل الأنشطة الإرهابية، وتجنيد أعضاء جدد، كما أن الجريمتين، ترتكبان لغرض المساس بالنظام العام، وتعريض أمن المجتمع وسلامته للخطر وكلتاهما تقوم لنفس الدواعي سواء كانت دينية أو اقتصادية أو سياسية.

وبالرغم من التداخل الكبير بين الجريمتين فإن هذا لا يمنع وجود اختلافات فيما بينهما، أهمها:

أ) الجريمتان تختلفان من حيث الوسيلة المتخذة لارتكاب الأفعال الإرهابية، فالأولى تعتمد على وسائل تقليدية مادية في تنفيذ الهجمات الإرهابية، باستعمال أسلحة تترك آثاراً على الواقع، كاستعمال القنابل والمتفجرات والأسلحة الفتاكة المصنوعة يدوياً، أما الإرهاب الإلكتروني فيعتمد على وسائل ناعمة لا تحدث أضراراً مادية، كونه مرتبطاً بالإنترنت الذي يقع في البيئة الافتراضية، من اختراق للمواقع الإلكترونية وتردميرها عن طريق نشر الفيروسات، واستخدامهم برامج للتجسس على الدول، وتخريب البيانات ومحوها، وغيرها من الأنشطة التخريبية على شبكات الإنترنت، وهو الاختلاف الجوهري بين الإرهاب التقليدي والإرهاب الإلكتروني.

---

[٤٧] د. هشام محمد فريد رستم، الإرهاب الدولي، دار النهضة العربية، القاهرة، ٢٠٠٣، ص١٠٦.

(ISSN: 2537 - 0758)

ب) يختلف الإرهاب التقليدي عن الإرهاب الإلكتروني بأن الأول يسهل كشف آثاره من قبل أجهزة الأمن، على عكس الثاني الذي يصعب كثيراً إثباته؛ لنقص خبرة أجهزة الشرطة في التعامل مع العالم الافتراضي.

ج) يختلف الإرهاب التقليدي عن الإرهاب الإلكتروني، من حيث خصوصية المجرم، فالمجرم الإرهابي التقليدي غير متعلم وجاهل غالباً، على عكس المجرم الإرهابي المعلوماتي الذي يكون على درجة عالية من المعرفة في مجال التقنية الرقمية.

د) المجرم الإرهابي المعلوماتي لا يحتاج الانتقال إلى ساحة الهجوم، فهو يبقى بعيداً عن الخطر، على عكس المجرم الإرهابي التقليدي الذي لا يأبه ويضحي بحياته في سبيل تحقيق قضيته الإرهابية.

هـ) يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي من حيث إن الأول لا يلجأ إلى العنف والقوة للوصول إلى أهدافه، على عكس الإرهاب التقليدي الذي يستعملها في تحقيق أغراضه، وهو الفارق الجوهري بين الجريمتين.

و) يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي من حيث باتساع نطاق الهجوم ومساحته، وذلك يرجع إلى اتساع شبكات الاتصال والمعلومات، على عكس الإرهاب التقليدي الذي ينحصر نطاق هجومه في دولة او إقليم[٤٨].

ثانياً: التمييز بين جريمة الإرهاب الإلكتروني والجريمة الإلكترونية:

في الواقع أن هناك تداخلاً واضحاً بين جريمة الإرهاب الإلكتروني والجريمة الإلكترونية، يكون من شأنه عدم تمييز بعض الناس بين الاستخدام السيئ للفضاء الإلكتروني أو الاستخدام ذي الطابع الإجرامي أو كأداة إرهابية، وهناك عدد من الأنماط يمكن اعتبارها جميعاً إذا ما وجهت إلى هدف معين تكون جريمة إرهاب إلكتروني، أما إذا فقدت ذلك الهدف فإنها تصنف ضمن الجرائم الإلكترونية.

الجريمة المعلوماتية هي الأخرى لم يتفق على وضع تعريف لها، ويرى البعض بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب"[٤٩].

---

[٤٨] د. عماد مجدي عبد الملك، د. عماد مجدي عبد الله، جرائم الكمبيرتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١١، ص٢٩.

[٤٩] د. عماد مجدي عبد الملك، د. عماد مجدي عبد الله، جرائم الكمبيرتر والإنترنت، المرجع السابق، ص٣٢.

أ) أوجه التشابه بين جريمة الإ رهاب الإلكتروني والجريمة الإلكترونية:

كلتا الجريمتين، جريمة الإرهاب الإلكتروني والجريمة الإلكترونية، تتشابهان في الوسيلة المستعملة في ارتكابها، وهي ضرورة استعمال التكنولوجيا الحديثة، إضافة لذلك تعدان من الجرائم ذات الطبيعة الخاصة، وتعدان من الجرائم المستحدثة في العالم وان كليهما من الجرائم التي يمكن أن تعبر الحدود، بالإضافة إلى أنهما من الجرائم الناعمة التي لا تتطلب العنف والقوة، كذلك تشترك جريمة الإرهاب الإلكتروني والجريمة الإلكترونية في خصوصية المجرم الذي يمتاز بالذكاء في أسلوب ارتكابه للجريمة، والقدرة على التعامل مع الوسائل التقنية فهو لا يعرض نفسه للخطر كما يتصرف بالتكيف مع محيطه، فلا يبين عدوانيته وكراهيته وخطورته الإجرامية[٥٠].

ب) أوجه الختلاف بين جريمة الإرهاب الإلكتروني والجريمة الإلكترونية:

بالرغم من التدخل الكبير بين جريمة الإرهاب الإلكتروني والجريمة الإلكترونية فإن هناك اختلافاً بينهما من حيث ما يلي:

١- إذا كانت الجريمة الإلكترونية تهدف غالباً إلى تحقيق الربح المادي، فإن جريمة الإرهاب الإلكتروني بالإضافة إلى تحقيق الربح تهدف أيضاً لتحقيق أغراض سياسية، دينية، اقتصادية...الخ.

٢- المجرم الإلكتروني أقل خطورة من المجرم الإرهابي الإلكتروني، فالأول قد يوجد داخل المنظومة المعلوماتية، سواء عن طريق الصدفة أو لمجد التسلية، بينما الثاني يوجد فيها، سواء للبحث عن مصادر تمويل، أو لنشر الفكر الإرهابي، أو لاستقطاب أعضاء جدد، أو للتواصل فيما بينهم للتنسيق للعمليات الإرهابية.[٥١]

ثالثاً: التمييز بين الجريمة المنظمة وجريمة الإرهاب الإلكتروني:

تعد الجريمة المنظمة من أقدم الجرائم التي عرفتها البشرية، والتي كان يطلق عليها عصابات المافيا ومع التطور وانفتاح الحدود بين الدول ليصبح العالم قرية واحدة جعل الجريمة المنظمة تتطور لتصبح عابرة للحدود وتكتسي أعمالها غير المشروعة من الطابع التجاري والاقتصادي، كالتجارة بالمخدرات وغسيل الأموال والإتجار بالبشر...

---

[٥٠] د. دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢، ص٣٢.

[٥١] د. دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، المرجع السابق، ص٣٩.

(ISSN: 2537 - 0758)

ومع التقدم التكنولوجي زادت خطورتها وأختلفت الاتجاهات في تعريف الجريمة المنظمة على عدة اتجاهات، يعرفها البعض بالتنظيم المرتبط بتأسيسها، وعرفها آخرون على اعتبارات تتعلق بباعث الربح الذي تسعى الجماعة إلى تحقيقه، بينما ذهب آخرون إلى تعريفها على أساس الاستمرارية[٥٢].

وعلى ذلك يمكن القول أن الجريمة المنظمة تعتبر سلوك إجرامى يتصف بالتنظيم الدقيق والإحتراف والإستمرارية، وذات بيان هرمى متدرج، ويعمل به أفراد محترفون لهم أهداف إجرامية تنفذ بدقة عالية، وتسعى إلى تحقيق الربح والنفوذ السياسي من خلال استخدام العنف على المستويان المحلى والدولى.

أوجه التشابه بين جريمة الإرهاب الإلكتروني والجريمة المنظمة:

توجد عدة مظاهر للتشابه بين جريمة الإرهاب الإلكتروني والجريمة المنظمة، سواء من حيث الهيكل التنظيمي وأساليب التنفيذ، **ويمكن تلخيصها في التالي:**

أ) تتشابه جريمة الإرهاب الإلكتروني والجريمة المنظمة بالتنظيم والسرية والدقة، من حيث القواعد التي تحكم النظام الداخلي للجماعة، من حيث الاحترام والتخطيط المحكم في تنفيذ الأعمال الإجرامية، كذلك بوجود علاقة هرمية داخل تنظيماتها وتجمعاتها، وإلى جانب الذكاء والدقة التي يمتاز بها أعضاؤها، والاحتراف في تسيير أنشطتها الإجرامية[٥٣].

ب) تشترك جريمة الإرهاب الإلكتروني والجريمة المنظمة، في أن كلتيهما تُعود من أبرز التهديدات لإعاقة التنمية الاقتصادية للدول، وكلتيهما تسعى للبحث عن إيجاد جهات تمولها في سبيل القيام بأعمالها الإجرامية، والسعي وراء استقطاب أعضاء جدد لاستمراريتها.

ج) كذلك تتشابه جريمة الإرهاب الإلكتروني والجريمة المنظمة بأن كلتا الجريمتين من الجرائم التي يمكن أن تكون عابرة للحدود.

---

[٥٢] د. محمد على سويلم، الأحكام الموضوعية والإجرائية للجريمة المنظمة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩، ص٣٢.

[٥٣] د. محمد على سويلم، الأحكام الموضوعية والإجرائية للجريمة المنظمة، المرجع السابق، ص٢٣٠

د) اعتماد الجريمتين على وسائل الاتصال الحديثة والأجهزة المعقدة التي أفرزتها تكنولوجيا العصر في تطوير أساليب إجرامها[٥٤].

أوجه الاختلاف بين جريمة الإرهاب الإلكتروني والجريمة المنظمة:

رغم التشابه الكبير بين الجريمتين نظراً لوجود رابطة وطيدة بينهما، لكن توجد نقاط جوهرية تتميز بها كل جريمة على الأخرى:

أ) تختلف الجريمة المنظمة عن جريمة الإرهاب الإلكتروني من حيث الدافع والغاية، حيث يكون هدف الجريمة المنظمة من العنف لكسب مصالح شخصية وأرباح مادية، أما هدف جريمة الإرهاب الإلكتروني فغير محدد، سواء أكانت سياسية، مادية، اجتماعية، دينية...إلخ.

ب) جريمة الإرهاب الإلكتروني يمكن أن ترتكب في إطار فردي أو جماعي، على عكس الجريمة المنظمة إذ تشترط عنصر الجماعة والاستمرارية.

ج) قيام المجرم الإرهابي المعلوماتي بإشهار أعماله الإرهابية عن طريق الإعلام، ومواقع التواصل الاجتماعي، أما مجرم الجريمة المنظمة فهو يقوم بأعماله الإجرامية بكل سرية والتخفي عن الأنظار.

د) قد تقوم الحكومات بالتفاوض مع الجماعات الإرهابية، وهو ما يعبر عن الاعتراف بهذه الجماعات ويضفي عليها الشرعية، بغض النظر عما ترتكبه من جرائم، الأمر الذي لا يتصور حدوثه مع جماعات الجريمة المنظمة[٥٥].

وعلى ذلك يمكن القول أن الجريمة المنظمة والإرهاب الإلكترونى هما وجهان لعملة واحدة حيث يتفقان في كثير من الأمور وخاصة أن أعضاء المنظمات الإرهابية في أغلب الأحيان هم في الأساس محترفى جرائم منظمة ويستفيدوا من خبراتهم الإجرامية في مجال الإرهاب الإلكترونى.

---

[٥٤] د. محمد على سويلم، الأحكام الموضوعية والإجرائية للجريمة المنظمة، المرجع السابق، ص٢٣٥

[٥٥] د. عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩، ص١٢٩.

(ISSN: 2537 - 0758)

الفرع الرابع
التصنيف القانوني لجريمة الإرهاب الإلكتروني

هناك إختلاف بين الفقه الجنائى والدولى بخصوص التكييف القانوني لجريمة الإرهاب الإلكترونى فيعتبرها البعض جريمة جنائية تخضع للقانون الداخلى، والبعض الآخر يعتبرها جريمة دولية.

أولاً: جريمة الإرهاب الإلكتروني جريمة داخلية

وقد اهتم مكتب الأمم المتحدة للمخدرات والجريمة في فيينا على أثر قرار مجلس الأمن الصادر سنة ٢٠٠٧ بوضع دليل للوثائق الدولية التي تكافح الإرهاب، وقد أشار هذا الدليل إلى أن الإطار القانوني لمكافحة الإرهاب يمكن أن يتم بتعديل القانون الجنائي الوطني في شقيه العقابي والإجرائي حيث أن سيادة القانون هي أساس توفير الأمن والعدالة للجميع، ولهذا فهي حجر الزاوية في عمل المكتب، وقد ساعد المكتب في إعداد الصكوك الدولية بشأن المخدرات والجريمة، فهو أمانة ووديع اتفاقيات وبروتوكولات المخدرات والجريمة، وتعتبر استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، التي قررت فيها الدول الأعضاء إدانة الإرهاب بجميع أشكاله ومظاهره، أيا كان مرتكبوه، وحيثما ارتكب، وأيا كانت أغراضه، واعترفت بمكتب الأمم المتحدة المعني بالمخدرات والجريمة بوصفه المكتب الرئيسي لتوفير المساعدة القانونية في منع الإرهاب، ومن أشكال المساعدة المقدمة من المكتب وأهدافه:

(أ) تعزيز التدابير الفعالة لمواجهة الجريمة والمخدرات والإرهاب، بناء على طلب الدول الأعضاء، من خلال تيسير تنفيذ الصكوك القانونية الدولية ذات الصلة؛

(ب) تعزيز إقامة نظم عدالة جنائية فعالة وعادلة وإنسانية بناء على طلب الدول الأعضاء، عن طريق استعمال معايير وقواعد الأمم المتحدة المتعلقة بمنع الجريمة والعدالة الجنائية وتطبيقها[٥٦].

وعلى ذلك يمكن القول أن مكتب الأمم المتحدة للمخدرات والجريمة أعتبر أن الإرهاب أياً كان شكله أو صوره يتم معالجته من خلال القوانين الداخلية ويكون المكتب مرجعاً لتصديق على البروتوكولات والمعاهدات والإتفاقيات وتنفيذها بين الدول،

[٥٦] تقرير لجنة منع الجريمة والعدالة الجنائية عن أعمال دورتها السادسة عشرة، فيينا، ٢٨ أبريل ٢٠٠٦، ٢٣-٢٧ أبريل ٢٠٠٧، ص ١٩ وما بعدها

والمساعدة في تحسين القدرات الوطنية لسن قوانين محلية تتماشى مع البروتوكلات والإتفاقيات الدولية[٥٧].

وأمام خطورة هذه الجريمة يخضع الإرهاب لنظام إجرائى متميز يراعى فيه مدى جسامتها ومختلف أبعادها، ومنها البعد الدولى إذا ما تجاوزت أفعاله حدود دولة معينة[٥٨].

ثانياً: جريمة الإرهاب الإلكتروني جريمة دولية

يرى بعض فقهاء القانون الجنائي أن جريمة الإرهاب الإلكتروني جريمة دولية، وذلك أذا ما خالفت القواعد الدولية التي تترتب عليها المسؤولية الجنائية الشخصية، سواء تلك التي نصت عليها الاتفاقيات الدولية، أو التي تضمنتها القواعد الدولية العرفية[٥٩].

وسوف نتناول بيان أن جريمة الإرهاب جريمة دولية من خلال بيان معيار الجريمة الدولية، وصور الإرهاب الإلكترونى بوصفه جريمة دولية.

أ) معيار الجريمة الدولية

يجب لإعطاء الوصف الدولى للجريمة أن يتوافر العنصر الدولى ويتحدد ذلك على عدة أسس وهي:

١) المساس بالقيم والمصالح الدولية

يفترض في الإرهاب كجريمة دولية وقوعها على المجتمع الدولي بأسره بقيمه ومصالحه، فهو عدو للمجتمع الدولي، كما أنه يقع بالمخالفة للقواعد التي وضعها المجتمع الدولي، سواء من خلال الاتفاقيات الدولية، أم من خلال القواعد الدولية العرفية، والأمر ذاته على الإرهاب الإلكتروني، فالأخير صورة من صور الإرهاب الحديثة يستخدم التكنولوجيا، إما كأداة أو كهدف لتنفيذ الأغرا ض الإرهابية الخبيثة[٦٠].

---

[٥٧] تقرير لجنة منع الجريمة والعدالة الجنائية، المرجع السابق، ص ٢٠.

[٥٨] د. محمود شريف بسيونى، الجرائم ضد الإنسانية في القانون الجنائى الدولى، الطبعة الثانية، ١٩٩٩، ص٨٩.

[٥٩] د. أحمد يوسف جمعة، الإرهاب السيبرانى والعملات الافتراضية والتجسس الإلكتروني، مرجع سابق، ص ٧٠.

[٦٠] د. أحمد فتحى سرور، حكم القانون في مواجهة الإرهاب، الدار الجامعية، ٢٠٠٥، ص١٠٩.

(ISSN: 2537 - 0758)

٢) جسامة النشاط الإجرامي:

أن يترتب على النشاط الإجرامي حد كبير من الجسامة، وذلك نتيجة استخدام التكنولوجيا الحديثة، الأمر الذي يجعل من هذه الأعمال الإرهابية أعمالاً ضد الإنسانية، وذلك أن يترتب على استخدام الأدوات الحديثة آثار كبيرة ذات نطا ق واسع، وإذا زاد عدد الضحايا فإنه لا ينظر إلى المجني عليهم كأفراد بل ينظر إلى الإنسانية كلها محلاً لهذا الاعتداء[٦١].

ب) صور الإرهاب الإلكتروني بوصفه جريمة دولية

يتنازع الإرهاب الإلكتروني بوصفة جريمة دولية نوعين من الأوصاف القانونية وفقاً للقانون الدولي:

١) جرائم الحرب وفقاً للقانون الإنساني الدولي

تناولت مبادئ نورمبرورج، واتفاقيات جنيف الأربع، وبروتوكرول جنيف سنة ١٩٧٧ الأفعال الخطرة، سواء كانت أفعالاً، أو إمتناعاً التي توصف بأنها جرائم حرب، إلا أنها لم تضع أركانها وعناصرها بشكل محدد وتركت الأمر للتشريعات الوطنية[٦٢].

وينطبق القانون الدولي الإنساني على أنشطة المنظمات الإرهابية وجهود مكافحة الإرهاب، في سياق نزاع مسلح داخلي أو دولي، كما يطبق القانون الدولي الإنساني، سواء كان الاستخدام الأصلي للقوة قانونياً أو مشروعاً أو غير ذلك[٦٣].

وفي مجال تحديد أركان الإرهاب كجريمة حرب، فإن للإرهاب نطاق أضيق من فكرته كجريمة في القانون الدولي، فالسلوك الإجرامي للإرهاب كجريمة حرب يتكون من فعل من أفعال العنف أو التهديد به ضد المدنيين، أو ضد أشخاص لا يساهمون مباشرة في النزاع المسلح أسرى الحروب والجرحى، ومن حيث الركن المعنوي فإنه باستقراء ٥١/٢ من البر وتوكول الأول والمادة ١٣ من البرتوكول الثاني الملحقين باتفاق جنيف، نجد أن الأعمال الإرهابية في سياق النزاع المسلح يقصد به بث الرعب بين السكان

---

[٦١] د. أمير فرج يوسف، جريمة مكافحة الإرهاب الإلكتروني، مرجع سابق، ص١٥٦.

[٦٢] د. حمد عبد المنعم عبد الخالق، الجرائم الدولية د راسة تأصيلية للجرائم ضد الإنسرانية والسلام والحرب، الطبعة الأولى، دار النهضة المصرية، القاهرة، ١٩٨٩، ص٣٣٩.

[٦٣] منشور اللجنة الدولية للصليب الأحمر بعنوان "القانون الدولي الإنسانى إجابات على أسئلتك، جنيف سويسرا، ٢٠١٥، ص ٨٠.

المدنيين أو الأشخاص الأخرى المحمية، فالإرهاب في جر ائم الحرب يتطلب لها توافر النية الإرهابية، بل إن يكفي لقيام الجريمة توافر القصد الاحتمالي[٦٤].

٢) <u>الجرائم ضد الإنسانية</u>

وقد أشار نظام روما المنشئ للمحكمة الجنائية الدولية، وتحديداً في المادة السابعة إلى مجموعة من الأعمال التي لو تم ارتكابها في إطار هجوم واسع النطاق أو منهجي ضد مجموعة من السكان المدنيين، وعن علم بالهجوم (النية الإرهابية) فإنها تعد جرائم ضد الإنسانية[٦٥]. وعليه قد تندرج بعض الأعمال الإرهابية تحت مظلة "الجرائم ضد الإنسانية " إذا كانت واسعة النطاق أو منتظمة ضد مجموعة من السكان المدنيين تنفيذاً لأجندة دولة ما، أو منظمة بارتكاب مثل تلك الهجمات[٦٦].

المبحث الثاني
الجهود المبذولة لمكافحة الإرهاب الإلكتروني

في عالم مزدحم بشبكات اتصال دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية متباعدة بإستخدام تقنيات لا تكفل للمعلومات أمناً كاملاً يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضراراً فادحة، يغدو التعاون الدولي واسع المدى في مكافحة الإرهاب أمراً ضرورياً، وإزاء ذلك كان لابد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات.

وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ولمعاقبة مرتكبيه، ولهذا سوف نتناول بالبحث التعاون الدولي في مجال مكافحة الإرهاب الإلكتروني من خلال المطلب الآتية:

---

[٦٤] الملحقان البروتوكولان الإضافيان إلى اتفاقيات جنيف المعقودة في ١٢ أغسطس١٩٤٩، اللجنة الدولية للصليب الأحمر، الطبعة الثانية عشرة، جنيف، سويسرا، ٢٠١٠، ص ٤١، ٥٧.

[٦٥] المادة (٧) من نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في ١٧ يولية ١٩٩٨، متاح على الموقع الرسمي للجنة الدولية للصليب الأحمر، https://www.icrc.org

[٦٦] د. أحمد يوسف جمعة، الإرهاب السيبرانى والعملات الافتراضية والتجسس الإلكتروني، مرجع سابق، ص ٩١.

(ISSN: 2537 - 0758)

المطلب الأول: الجهود الدولية لمكافحة الإرهاب الإلكترونى
المطلب الثانى: الجهود العربية لمكافحة الإرهاب الإلكترونى
المطلب الثالث: التجربة المصرية في مكافحة الإرهاب التقليدي والإلكترونى

المطلب الأول
الجهود الدولية لمكافحة الإرهاب الإلكترونى

في بداية التسعينات من القرن العشرين عقد مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا بكوبا، الذي أكد في قراره رقم ٤٥/ ١٢١ الصادر في ١٤ ديسمبر ١٩٩٠ المتعلق بالجرائم ذات الصلة بالحاسب الآلي أن الدول الأعضاء مطالبة بتكثيف جهودها لكي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسب الآلي التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في:

أ- تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءات بشأن سلطات التحقيق وقبول الأدلة على نحو ملائم.

ب- النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي[٦٧].

كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالإرهاب الإلكتروني، بما في ذلك دخولها حسب الاقتضاء أطرافاً في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، وفتح آفاق جديدة للتعاون الدولي في هذا المضمار ولاسيما فيما يتعلق بوضع أو تطوير ما يلي:

أ- معايير دولية لأمن المعالجة الآلية للبيانات.

ب- تدابير ملائمة لحل مشكلات الإختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.

---

[٦٧] د. غازي عبد الرحمان هيان الرشيد: الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق بالجامعة الإسلامية في لبنان، ٢٠٠٤، ص١٨٦.

ج- اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول[٦٨].

أما منظمة الإنتربول فقد واصلت جهودها في مجال مكافحة جرائم الحاسب والانترنت وأنشأت لذلك وحدة متخصصة في جرائم الانترنت تحديدا وشكلت فرق عمل بدأت في أوروبا عام ١٩٩٠ وفي مختلف الدول لبحث ورصد جرائم التقنية ومن ضمنها الإرهاب الإلكتروني[٦٩].

- **الأمم المتحدة ودورها في مكافحة الإرهاب الإلكترونى**

أن النظرة للإرهاب الإلكتروني وحرب المعلومات تقع ضمن ميثاق ومقاصد الأمم المتحدة، كما ورد في الفصل السابع من ميثاق الأمم المتحدة فيما يتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان في المادة ٣٩ التي تنصُّ على: "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملا من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقًا لأحكام المادتين ٤١ و٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه"[٧٠].

وأورد ميثاق الأمم المتحدة في مادته الثانية فقرة (٣) ما نصه: "يفضُّ جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر"[٧١].

- **إجراءات وتدابير الأمم المتحدة لمكافحة الأعمال الإرهابية**

- الامتناع عن تقديم أي شكل من أشكال الدعم الصريح والضمني للكيانات الإرهابية تم وضع حد لعملية تجنيد أعضاء الجماعات الإرهابية ومنع تزويد الإرهابيين بالسلاح.

---

[٦٨] د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ٢٠٠٠، ص. ٤٨ -٤٩.

[٦٩] د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، ٢٠١١، ص١٣٥.

[٧٠] المادة ٣٩ من الفصل السابع من ميثاق الأمم المتحدة.

[٧١] المادة ٢ فقرة ٣ من الفصل الاول لميثاق الأمم المتحدة.

(ISSN: 2537 - 0758)

- عدم توفير الملاذ لمن يمولون الأعمال الإرهابية أو يديرونها أو يرتكبونها، منع استخدام أراضي الدول في تنفيذ تلك المآرب، نص ضوابط مشددة على الحدود وعلى إصدار الأوراق الثبوتية ووثائق السفر.
- تعزيز التدابير الرامية إلى كشف ووقف تدفق التمويل والأموال للأغراض الإرهابية.
- وضع الإرهابيين من استغلال الأنشطة الإجرامية الأخرى (كالاختطاف، والاتجار بالبشر والمخدرات والأسلحة) لتمويل أنشطتهم الإرهابية، وتجريم ومحاسبة كل من يمول الأعمال الإرهابية أو يدريها أو يدعمها أو يرتكبها أو يورد السلاح إليهم.
- تشجيع الدول على تبادل المعلومات على وجه السرعة مع الدول الأعضاء وتقديم تقارير إلى لجنة مكافحة الإرهاب حسب جدول زمني تحدده اللجنة.
- دعوة المنظمات الدولية لتعزيز التعاون مع الأمم المتحدة في نطاق ولايتها بهدف تطوير قدراتها على معاونة الدول الأعضاء في جهودها على التصدي لتهديدات الإرهابية[٧٢].

- **الاتفاقيات الدولية لمكافحة جريمة الإرهاب الالكتروني**

واجهت الدول صعوبات في مكافحة الجريمة المعلوماتية عبر قوانينها الداخلية إلا أنها واجهة العديد من التحديات، لذلك كرست الدول جهودها بالتعاون على مواجهة هذا الإجرام الجديد، وعقد اتفاقيات دولية لمواجهة هذه الظاهرة والوصول إلى حلول مشتركة لمكافحة هذا النوع من الجرائم التي تعتبر هي الأخطر من نوعها ومن بين هذه الاتفاقيات:

أولا: اتفاقية بودابست لمكافحة جريمة الإرهاب الالكتروني

وتعرف بالاتفاقية الأوربية لمكافحة جريمة الإرهاب الالكتروني ووضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت ودخلت حيز التنفيذ في ٢٠٠١/١١/٢٣ للتوقيع في بودابست في ٢٠٠١.

---

[٧٢] د. عادل عبد الصادق، الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني، مقالة منشورة على موقع المركز العربي لأبحاق الفضاء الإلكتروني https://accronline.com/article-detail.aspx?id=22762 تاريخ زيارة الموقع ٢٠٢٤/٣/٦م.

تعد معاهدة بودابست لمكافحة جرائم الانترنت أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الانترنت اولاستخدام السيء لها[٧٣].

وقد وقعت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام وتتضمن ٤٨ مادة موزعة على أربعة فصول. تم توقيع هذه الاتفاقية، بسبب المخاوف والقلق إزاء سوء استخدام شبكات الانترنت والمعلومات الالكترونية، ومن اجل توفر ما يلزم لردع أي عمل موجه ضد سرية نظم الحاسوب والشبكات والبيانات[٧٤]، **وتهدف الاتفاقية إلى:**

- السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية.
- التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والانترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والانترنت.
- ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي[٧٥].

---

[٧٣] د. منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي، ط ١، الاسكندرية، ٢٠٠٤، ص ٩.

[74] John Arquilla David Ronfeld: Networks and Netwars: The Future of Terror Crime and Militancy. USA Rand publication 2001 p. 281.

[٧٥] د. هلالي عبد اللاه أحمد، جرائم المعلوماتية وأساليب المواجهة وفقاً لاتفاقية بودابست، دار النهضة، ط ١، القاهرة، ٢٠٠٧، ص٣٠.

(ISSN: 2537 - 0758)

ثانياً: توصيات المجلس الأوروبي

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية أهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم ١٣/٩٥ في ١٩٩٥/٩/١١ في شأن مشاكل الإجراءات الجزائية المتعلقة تكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم من التطور في هذا المجال، **ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي**(٧٦):

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.
- أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محل للتفتيش مع بيان المعلومات التي تم ضبطها، ويسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط اولتفتيش.
- أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضرورياً.
- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.
- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية اولاحترام للمعلومات التي يفرض القانون لها حماية خاصة.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

(76) Ushie Henry Ekpe: The Impact of Terrorism (Including Cyber Terrorism) and Threats of Terrorism on International Business (or Nation Sate). Journal of the International Relations and Affairs Group Volume 3 Issue 1 2013 p. 38.

- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
- يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة
- للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال وسلطات التحقيق التحقيق بالاطلاع عليها.
- يجب تطوير وتوحيد أنظمة التعامل مع الأدل ة الالكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.
- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.
- قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.
- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع أدلة معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط. ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائم[٧٧].

المطلب الثانى
الجهود العربية لمكافحة الإرهاب الإلكترونى

إن مكافحة الإرهاب الإلكتروني باعتباره من أخطر الجرائم العابرة للحدود التي أصبحت تهدد الأمن المعلوماتي، تقتضي تبني الدول في قوانينها الداخلية لمجموعة من الأحكام الإجرائية، وتكثيفها لجهود التعاون القانوني والقضائي والتقني فيما بين الدول.

[٧٧] د. شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية العدد١، المجلد ١٧ كلية القانون الامارات يونيو ٢٠٢٠، ص٧٥٢-٧٥٣.

(ISSN: 2537 - 0758)

ومن هذا المنطلق، نصت هذه الاتفاقية على حزمة من الآليات الفعالة لمكافحة هذه الجريمة، التي سنتطرق إليها في هذا المطلب بالتفصيل من خلال (الفرع الأول) المتعلق بالآليات الإجرائية، (والفرع الثاني) الذي يتناول آليات التعاون القانوني والقضائي بين الدول الأطراف.

الفرع الأول
الآليات الإجرائية التي نصت عليها التفاقية العربية لمكافحة جرائم تقنية المعلومات

يمكننا إيجاز الآليات الإجرائية التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فيما يلي:

١ – <u>الحفظ العاجل للبيانات المعلوماتية المخزنة والأمر بتسليمها:</u>

تعرف البيانات المعلوماتية حسب هذه الاتفاقية بأنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها"[٧٨].

أما التحفظ العاجل للبيانات المعلوماتية، فيقصد به "توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية".

وعليه يقتضي الحفظ أن تكون البيانات المعلوماتية المخزنة في تقنية معلومات، محمية بشكل آمن من كل المخاطر التي قد تؤدي إلى المساس بسلامتها كالتغيير أو التعديل أو الحذف...إلخ، ولا يعني الحفظ بالضرورة أن تكون البيانات المخزنة مجمدة، لا يمكن لأي كان النفاذ إليها أو استخدامها أو استخدامُ نسخ منها، بل يمكن للشخص الذي يوجه له الأمر القيام بذلك في حدود ما يسمح به أمر الحفظ[٧٩].

ويعد هذا الإجراء من أهم الإجراءات التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة ٢٣ منها، التي ألزمت بموجبها الدولة الأطراف باتخاذ التدابير التشريعية اللازمة لما تقتضيه إجراءات التحقيق في الجريمة الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني لتمكين السلطات المختصة من توجيه الأمر لشخص بحفظ البيانات المعلوماتية المخزنة التي في حوزته أو تحت سيطرته لمدة أقصاها ٩٠

---

[٧٨] المادة ٣/٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٧٩] التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية الصادر في ٢٣ نوفمبر ٢٠٠١.

يوماً تكون قابلة للتجديد خاصة إذا كانت هذه الأخيرة معرضة للفقدان أو التعديل، واتخاذ الإجراءات الضرورية التي من شأنها الحفاظ على سرية المعلومات المخزنة طيلة الفترة القانونية المنصوص عليها في قوانينها الداخلية(٨٠).

كما تلزم هذه الاتفاقية الدول المتعاقدة باعتماد إجراءات تستطيع من خلالها السلطات المختصة من توجيه الأمر إلى أي شخص كان على إقليمها قصد تقديم البيانات التي بحوزته سواء أكانت المخزنة في تقنية معلومات أم في دعامة تخزين كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية...إلخ، أو إلى أي مزود خدمة لتسليم معلومات المشتركين في الخدمة المقدمة التي بحوزته أو تحت سيطرته(٨١).

ولكن ما يؤخذ على هذه الاتفاقية أنها لم تحدد عدد مرات تمديد مدة حفظ البيانات المعلوماتية المخزنة التي نصت عليها في المادة ٢٣ منها، وإنما اكتفت بعبارة "٩٠ يوماً قابلة للتجديد"، كما لم تعرف "مزودي الخدمة" على عكس اتفاقية بودابست لسنة ٢٠٠١ المتعلقة بالجرائم المعلوماتية التي عرفت هذه الكيانات على النحو التالي "أي كيان عام أو خاص يقدم لمستغلي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية؛ أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها"(٨٢).

٢- <u>تفتيش المعلومات المخزنة</u>

يعتبر تفتيش البيانات المخزنة في تقنية معلومات أحد أهم الإجراءات للكشف عن ملابسات الجريمة والوصول إلى مرتكبيها، ولهذا تلزم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف باتخاذ التدابير التشريعية اللازمة حتى تتمكن سلطاتها المختصة من تفتيش تقنية معلومات أو جزء منها أو إحدى وسائط تخزين المعلومات الإلكترونية.

٣- <u>ضبط المعلومات المخزنة (الحجز والمصادرة):</u>

نظراً لأهمية هذا الإجراء في مكافحة الجريمة الإلكترونية، نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة ٢٧ منها على ضرورة اعتماد الدول الأطراف

---

(٨٠) المادة ٢٣ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(٨١) المادة ٢٥ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(٨٢) المادة الأولى من اتفاقية بودابست المتعلقة بالجرائم المعلوماتية لسنة ٢٠٠١.

(ISSN: 2537 - 0758)

لإجراءات تمكن السلطات المختصة من ضبط وتأمين تقنية المعلومات أو جزء منها أو وسائط تخزين المعلومات كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية... إلخ، ونسخ المعلومات والاحتفاظ بها ومحوها أو إزالتها من التقنية التي اكتشفت فيها أو منع أي شخص آخر من الوصول إليها، وتمكين هذه السلطات من الاستعانة بالأشخاص الذين لهم خبرة ومعرفة في هذا المجال[٨٣].

٤- <u>الجمع الفوري لمعلومات تتبع المستخدمين:</u>

إلى جانب الإجراءات السابق ذكرها، ألزمت هذه الاتفاقية الدول الأطراف باتخاذ التدابير اللازمة التي من شأنها أن تمكن السلطات المختصة من جمع أو تسجيل المعلومات المتعلقة بتتبع المستخدمين عن طريق مختلف الوسائل الفنية وتلزم مزودي الخدمة في حدود اختصاصهم أيضاً للقيام بذلك مع الحفاظ على سرية هذه المعلومات[٨٤]، ولكنها لم تحدد الشروط القانونية الواجب اتخاذه لجمع وتسجيل المعلومات ما عدا إلزامها الدول الأطراف بتبني إجراءات لإلزام مزودي الخدمة بالحفاظ على سرية المعلومات.

٥- <u>اعتراض بيانات المحتوى:</u>

تنص المادة ٢٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، على إلزامية تبني الدول الأطراف في تشريعات الداخلية للتدابير اللازمة، لتمكين السلطات المختصة من اعتراض بيانات المحتوى في ما يتعلق ببعض الجرائم المنصوص عليها في قوانينها الداخلية.

وهنا تجب الإشارة إلى أن هناك نوعين من البيانات التي يمكن جمعها أو تسجيلها، وهي "بيانات المحتوى" و"بيانات الحركة"، إلا أن هذه الاتفاقية لم تعرف أي منهما، في حين عرفت اتفاقية بودابست لسنة ٢٠٠١ "بيانات الحركة" بأنها "أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءا في سلسلة الاتصالات توضح المنشأ والوجهة، الزمن، والتاريخ، والحجم، والمدة أو نوع الخدمة الأساسية"[٨٥]، ولكنها لم تعرف هي الأخرى "بيانات المحتوى"، غير أنها تشير إلى محتوى الاتصال أي الرسالة أو المعلومات التي ينقلها الاتصال، ونظرا لخطورة هذا

---

[٨٣] المادة ٢٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٨٤] المادة ٢٨ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٨٥] التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية الصادر في ٢٣ نوفمبر ٢٠٠١.

الإجراء ومساسه بحق الحياة الخاصة، فإنه يقتصر على بعض الجرائم الخطيرة المحددة في القوانين الداخلية للدول[٨٦].

الفرع الثاني

آليات التعاون القانوني والقضائي لمكافحة جرائم الإرهاب الإلكتروني

يقصد بالتعاون القضائي الدولي "مجمل الإجراءات التي تتخذها السلطات القضائية داخل الدولة بصدد جريمة محددة أو مجرمين محددين (متهمين أو محكوم عليهم) والمنصوص عليها في الاتفاقيات الدولية التي تكون الدول طرفاً فيها بمقتضى التشريعات الوطنية النافذة".

١- <u>تسليم المجرمين:</u>

يعرف تسليم المجرمين بأنه "ذلك الإجراء القانوني الذي تقوم به دولة ما لتسليم شخص متواجد على إقليمها إلى دولة أخرى تطلب تسليمه لمحاكمته أو لتنفيذ العقوبة المحكومة بها أو كإجراء وقائي"[٨٧].

وعرفه نظام روما الأساسي بأنه "نقل دولة ما شخصاً إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني"[٨٨].

وتتجلى أهمية هذا الإجراء في عدم توفير المكان الذي يفلت فيه مقترف وهذه الجرائم من العقاب وتفادي خطرهم على أمن واستقرار الدول، ولهذا ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتسليم مرتكبي الجرائم التي نصت عليها في الفصل الثالث، بما فيها الجرائم المتعلقة بالإرهاب والمرتبكة بواسطة تقنية المعلومات المحددة في المادة ١٥ منها، شريطة أن تكون عقوبة هذه الجرائم في التشريعات الجنائية للدول الأطراف سالبة للحرية تساوي أو تزيد عن سنة أو بعقوبة أشد منها.

وفي حال اشتراط إحدى الدول الأطراف وجود معاهدة لتسليم المجرمين، وتقدمت إليها دولة أخرى طرف لا تربطها بها اتفاقية ثنائية في هذا الشأن، أو عدم اشتراط الدول الأطراف لوجود معاهدة لتسليم المجرمين، فإن الاتفاقية العربية لمكافحة جرائم تقنية

---

[٨٦] التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية الصادر في ٢٣ نوفمبر ٢٠٠١.

[٨٧] د. عبد الله نور شعت، التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، ٢٠١٧، ص٣٠٨.

[٨٨] المادة ١٠٢ من نظام روما الأساسي للمحكمة الجنائية الدولة لسنة ١٩٩٨، الذي دخل حيز النفاذ في ١/ ٢٠٠٢/٧.

(ISSN: 2537 - 0758)

المعلومات تعتبر كأساس قانوني لتسليم المجرمين، كما أجازت هذه الاتفاقية لكل دولة طرف أن تمتنع عن تسليم مواطنيها على أن تتعهد للدول الأطراف الأخرى التي تتقدم إليها بطلب الملاحقة بأن توجه الاتهام لمواطنيها الذين ارتكبوا جرائم إلكترونية في هذه الدول، ومباشرتها لإجراءات التحقيق والمحاكمة والتزامها بإعلام الدولة الطالبة بما تم اتخاذه بشأن طلبها المتعلق بالملاحقة[٨٩].

٢- <u>المساعدة المتبادلة بين الدول الأطراف</u>

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جملة من الإجراءات لتنظيم طلبات المساعدة المتبادلة بين الدول الأطراف، **يمكننا أن نوجزها في ما يلي:**

- يتعين على كل دولة طرف أن تقوم بتعين سلطة مركزية تعنى بإرسال ودراسة طلبات المساعدة المتبادلة والإجابة عليها وتنفيذها أو تقديمها إلى السلطات المختصة لتنفيذها، على أن يتم قيد هذه السلطة في سجل خاص تعده الأمانة العامة لوزراء الداخلية العرب والأمانة الفنية لوزراء العدل العرب لهذا الغرض[٩٠]، غير أنه في الحالات المستعجلة يمكن أن توجه أي دولة طرف طلب المساعدة مباشرة إلى السلطة القضائية للدولة المطلوب منها المساعدة، مع التزام الدولة الطالبة بإرسال نسخة من هذا الطلب إلى السلطة المركزية للدولة المطلوب منها المساعدة. وفي وحالة عدم اختصاص السلطة القضائية تحيل هذه الأخيرة طلب المساعدة إلى السلطة المختصة شريطة إعلامها للدولة الطالبة بذلك فوراً، كما أجازت هذه الاتفاقية للدول الأطراف إرسال طلبات المساعدة إلى بعضها البعض عن طريق المنظمة الدولية للشرطة الجنائية "INTERPBOL"[٩١].
- توجه طلبات المساعدة المتبادلة من الدولة الطرف الطالبة للمساعدة إلى الدولة المطلوب منها بشكل خطي كقاعدة عامة، غير أنه يجوز أن ترسل هذه الطلبات في الحالات المستعجلة عن طريق وسائل الاتصال الحديثة كالفاكس أو البريد الإلكتروني مع مراعاة أمن وسرية الاتصالات بين الأجهزة المختصة للدول التي

---

[٨٩] المادة ٣١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٠] المادة ٣٤/١، ٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩١] المادة ٣٤/٨ "أ، ب، ج" من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

تقدمت بطلب المساعدة والدولة التي تلقت هذا الطلب كاستعمال طريقة تشفير المعلومات مثلاً[٩٢].

- خضوع طلب المساعدة للشروط المحددة في قانون الدولة الطرف المطلوب منها المساعدة أو في الاتفاقيات الثنائية المتعلقة بالمساعدة المتبادلة بما في ذلك الأسس التي يمكن للدول المتلقية لطلب المساعدة الاعتماد عليها لرفض هذا الطلب[٩٣]، كما يجوز للدولة المطلوب منها المساعدة رفض هذا الطلب إذا كان قانونها الداخلي يعتبر هذه الجرائم من قبيل الجرائم السياسية أو أن تنفيذ طلب المساعدة سيشكل انتهاكاً لسيادتها أو خطراً على أمنها أو مصالحها الجوهرية[٩٤].
- يجوز للدولة الطرف المطلوب منها المساعدة تأجيل الإجراءات التي اتخذتها بشأن طلب المساعدة إذا كان من شأنها التأثير سلباً على التحقيقات التي تقوم بها أجهزتها المختصة. وقبل رفض أو تأجيل المساعدة تقرر هذه الأخيرة بعد استشارة الدولة الطالبة ما إذا كانت ستقدم لها المساعدة بشكل جزئي أو بشروط خاصة، كما تلتزم بإعلامها بنتائج تنفيذ هذا الطلب، وفي حالة رفضه أو تأجيله يتعين عليها أيضاً إعلامها بأسباب الرفض أو التأجيل[٩٥].
- إذا تقدمت دولة طرف بطلب مساعدة إلى دولة أخرى طرف، تجيز هذه الاتفاقية للدول المطلوب منها المساعدة أن تشترط الحفاظ على سرية هذه المعلومات المقدمة، وأن تستخدمها في حدود الطلب ولا تستخدمها في تحقيقات أخرى لا تتعلق بالجريمة موضوع التحقيق. وإذا لم تستطع الدولة الطالبة الالتزام بالحفاظ على سرية المعلومات، يجب عليها كما سبقت الإشارة إعلامُ الدولة المطلوب منها تقديم المساعدة[٩٦].

---

[٩٢] المادة ٣١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٣] المادة ٣٢/٤ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٤] المادة ٣٥ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٥] المادة ٣٤/ف ٤، ٥، ٦ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٦] المادة ٣٦ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(ISSN: 2537 - 0758)

- **مجالات المساعدة المتبادلة في التفاقية العربية لمكافحة جرائم تقنية المعلومات:**

تتمثل مجالات المساعدة المتبادلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ما يلي:

أ- التقديم التلقائي للمعلومات بين الدول الأطراف

أجازت هذه الاتفاقية على غرار اتفاقية بودابست لسنة ٢٠٠١ للدول الأطراف أن تقدم لبعضها البعض بصفة تلقائية لمعلومات تحصلت عليها من خلال التحقيقات التي تقوم بها مصالحها المختصة بدون طلب مسبق للمساعدة في إطار التعاون من أجل مواجهة الجريمة الإلكترونية والإرهاب الإلكتروني[٩٧]، كما أجازت هذه الاتفاقية للدولة التي تحيل المعلومات بصفة عرضية أن تطلب من الدول التي أحالت لها المعلومات أن تحافظ على سريتها في حالة ما إذا كانت هذه المعلومات حساسة أو إذا ما تم الكشف عنها قد تتعرض المصالح الجوهرية للدولة المقدمة للمعلومات للخطر. وإذا كشف التحقيق المسبق أن الدولة الطرف المتلقية للمعلومات لا تستطيع الالتزام بالسرية كما لو كانت هذه المعلومات مطلوبة كدليل في محاكمة علنية[٩٨]، فيتعين عليها إعلام الدولة التي أحالت إليها هذه المعلومات، أما إذا قبلت المعلومات بشرط الحفاظ على سريتها فيجب عليها التقيد بهذا الشرط[٩٩].

ب- المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة

وتتمثل المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة حسب هذه الاتفاقية في الحفظ العاجل للبيانات المخزنة في تقنية معلومات، والكشف العاجل للبيانات المتعلقة بتتبع المستخدمين، **وهذا ما سنكتشفه في ما يلي:**

- الحفظ العاجل للبيانات المخزنة في تقنية معلومات:

تجيز المادة ٣٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لأي دولة طرف أن تقدم طلباً للحصول على الحفظ العاجل للبيانات المخزنة في تقنية المعلومات الموجودة على إقليم الدولة الطرف للطلب، على أن يشتمل هذا طلب اسم الهيئة

---

[٩٧] المادة ٣٣/ف ١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[٩٨] التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية الصادر في ٢٣ نوفمبر ٢٠٠١.

[٩٩] المادة ٣٣/ف ٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

المصدرة له، نوع الجريمة الإلكترونية محل التحقيق، ملخصاً للوقائع، البيانات التي يتعين حفظها وبيان علاقتها بهذه الجريمة، المعلومات المتعلقة بالمسؤول عن البيانات المخزنة وموقعها وكذا الهدف المتوخى من طلب المساعدة والذي يكون إما للوصول أو البحث أو ضبط أو كشف عن البيانات المخزنة، كما تلزم هذه الاتفاقية في المادة نفسها الدول الأطراف التي تتلقى طلب الحفظ العاجل للبيانات المخزنة في تقنية معلومات اتخاذ التدابير والإجراءات الضرورية لحفظ البيانات المذكورة في الطلب وفقا لقانونها الداخلي وعدم تمسكها بمبدأ ازدواجية التجريم كشرط لحفظ البيانات في الجرائم المنصوص عليها في الفصل الثاني منها، غير أنها أجازت للدول الأطراف المطلوب منها المساعدة أن ترفض هذا الطلب إذا كان تنفيذه يعرض سيادتها أو أمن مصالحها الجوهرية للخطر أو إذا كانت الجريمة موضوع التحقيق تعتبر من قبيل الجرائم السياسية في قوانينها الداخلية[١٠٠].

والجدير بالملاحظة أن هذه الاتفاقية حددت المدة الدنيا للحفظ العاجل للبيانات المخزنة في تقنية معلومات المترتب على طلب المساعدة في الفقرة ٠٧ من المادة ٣٧ منها بستين (٦٠) يوماً، دون أن تحدد المدة القصوى لذلك.

- الكشف العاجل لبيانات تتبع المستخدمين:

يتعين على الدولة المتلقية لطلب المساعدة إذا ما اكتشفت، أن بيانات الحركة التي تم التطرق إليه سابقاً، تفيد بأنه تم توجيه الإرسال من مزود خدمة في دولة ثالثة أو من الدولة الطالبة للمساعدة أن تقدم إلى هذه الأخيرة قدراً كافياً من بيانات تتبع المستخدمين لتمكينها من معرفة مزود الخدمة وتحديد مسار بث الاتصال، أما إذا كان ذلك يمس بأمنها أو سيادتها أو مصالحها أو من قبيل الجرائم السياسية فيجوز لها رفض طلب الكشف عن بيانات المستخدمين[١٠١].

ج- المساعدة المتبادلة للوصول إلى البيانات المخزنة واعتراض بيانات المحتوى

في إطار تعزيز التعاون بين الدول الأطراف في مجال مكافحة الإجرام المعلوماتي، تجيز المادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات للدول الأطراف أن تطلب من بعضها البعض القيام بأي إجراء من شأنه البحث أو النفاذ أو الضبط أو

---

[١٠٠] المادة ٣٧ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[١٠١] المادة ٣٨ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(ISSN: 2537 - 0758)

التأمين أو الكشف عن البيانات المخزنة في تقنية معلومات موجودة داخل أراضها، مع مراعاة الدول المطلوب منها المساعدة للأحكام المنصوص عليها في هذه الاتفاقية التي تنظم المساعدة القانونية المتبادلة، وكذا التزامها بالتعجيل بالرد على طلب المساعدة للدولة الطالبة في الأحوال التي تكون فيها البيانات المخزنة معرضة للحذف أو التغيير أو التعدي[١٠٢].

كما أجازت المادة ٤٠ من هذه الاتفاقية أيضا للدول الأط راف أن تحصل على المعلومات المتوفرة للعامة في أي مكان دون حصولها على تفويض من دولة أخرى طرف، والتزامها أيضاً بتقديم المساعدة لبعضها البعض بالجمع الفوري لبيانات تتبع المستخدمين التي تتم عن طريق إحدى تقنية المعلومات[١٠٣].

ونظراً لخطورة التدخل التي تتسم بها عملية الاعتراض، قيدت هذه الاتفاقية على غرار اتفاقية بودابست المساعدة المتبادلة لاعتراض بيانات المحتوى في حدود ما تسمح به المعاهدات والقوانين الداخلية السارية المفعول للدول الأطراف[١٠٤].

المطلب الثالث

التجربة المصرية في مكافحة الإرهاب التقليدي والإلكترونى

واكب المشرع المصرى التطور الحاصل في مجال مكافحة الإرهاب خاصة في العقد الأخير بسبب زيادة وتيرة إرتكاب الجرائم الإرهابية على مستوى العالم وذلك في إطار تعاون دول العالم فى مكافحة الإرهاب فقد عقدت الكثير من المؤتمرات وتعاهدات الدول في اتفاقيات ومعاهدات دولية وإقليمية بهدف مكافحة الإرهاب الدولى.

وقد قامت دولة جمهورية مصر العربية ودولة الكويت بسن تشريعات داخلية في إطار التزامها الدولى في مكافحة هذا النوع من الإجرام، ولكن تختلف التجربة المصرية عن غيرها لذلك سوف نتناول التجربة المصرية من خلال الآتى:

---

[١٠٢] المادة ٣٩ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[١٠٣] المادة ٤١ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

[١٠٤] المادة ٤٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

الفرع الأول
مكافحة جرائم الإرهاب التقليدي في التشريع المصرى

مر التشريع المصرى بخصوص جرائم الإرهاب بالعديد من المراحل إلى أن وصل إلى التشريع الحالي وقد أكد المشرع المصرى في العديد من المناسبات حضوره بسن وتعديل القوانين التي تواجه الإرهاب بصفة مستمرة لمواكبة التطور التشريعى في مجال مكافحة الإرهاب.

ويعد التزام جمهورية مصر العربية التزاماً دستورياً حيث تنص المادة (٢٣٧) من الدستور المصرى لسنة ٢٠١٤ على أنه "تلتزم الدولة بمُواجهة الإرهاب بكافة صورة وأشكاله، وتعقب مصادر تمويله. وينظم القانون أحكام وإجراءات مكافحة الإرهاب والتعويض العادل عن الأضرار الجسيمة عنه وبسببه"[١٠٥].

وقد تبنت الدولة رؤية مؤداها أن مكافحة الإرهاب لا يعد إلتزاماً على عاتق الدولة لحماية أمنها القومي فحسب، وإنما يستهدف أيضاً حماية أحد المبادئ الأساسية لحقوق الإنسان وهو الحق في الحياة.

وإنطلاقاً من الإلتزام الدستوري بمكافحة الإرهاب، فقد وضع المشرع حزمة متكاملة من التشريعات الوطنية التي تتسق مع إلتزامات مصر بموجب قرارات مجلس الأمن والاتفاقات الإقليمية والدولية ذات الصلة بمكافحة الإرهاب التي إنضمت إليها، وكذلك استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب على نحو يحقق مكافحة فاعلة وشاملة لظاهرة الإرهاب بكافة أبعادها، كما استهدفت التشريعات تعزيز سبل التصدي للطرق المستحدثة في مجال تمويل الإرهاب.

ويأتي على رأس هذه التشريعات القانون رقم ٨٠ لسنة ٢٠٠٢ بشأن مكافحة غسل الأموال والمعدل بالقرار بقانون رقم ٣٦ لسنة ٢٠١٤، والذي جاء ليواكب التطورات السريعة في مجال تمويل العمليات الإرهابية، وصدرت لائحته التنفيذية رقم ٨٠ لسنة ٢٠٠٢ في ٩ يونيو ٢٠٠٣ بموجب قرار رئيس مجلس الوزراء ٩٥١ لسنة ٢٠٠٣، والتي تهدف إلى وضع أُطر تفصيلية وتفسيرية لأحكام القانون المذكور وتعديلاته، فضلاً عن مواكبة المستجدات في المعايير الدولية لمواجهة جرائم الإرهاب.

---

[١٠٥] المادة (٢٣٧) من الدستور المصرى لسنة ٢٠١٤.

(ISSN: 2537 - 0758)

وصدر بعد ذلك القانون رقم (٩٤) لسنة ٢٠١٥ لمكافحة الإرهاب، وهو قانون شامل للتصدي لجرائم الإرهاب وتمويله من الناحيتين الموضوعية والإجرائية.

ثم صدر القانون رقم (١١) لسنة ٢٠١٧ بتعديل القانون رقم (٩٤) لسنة ٢٠١٥، ثم صدر القانون رقم (٢٢) لسنة ٢٠١٨ بتنظيم إجراءات التحفظ والحصر والإدارة والتصرف في أموال الجماعت الإرهابية والإرهابيين.

ثم صدر القانون رقم (١٤) لسنة ٢٠٢٠ بتعديل أحكام القانون رقم (٨) لسنة ٢٠١٥ بشأن تنظيم قوائم الكيانات الإرهابية والإرهابيين.

ثم صدر القانون رقم (١٥) لسنة ٢٠٢٠ بتعديل أحكام القانون رقم (٩٤) لسنة ٢٠١٥ فيما يخص أموال الجماعات الإرهابية.

ويتضح من خلال هذا العرض أن المشرع المصرى دائم التدخل بالتعديل لمواكبة التطور في مواجهة الجرائم الإرهابية، وكذلك يتبين أن المشرع المصرى تبنى عدة استراتيجيات لمكافحة الإرهاب فقد تبنى المواجهة إلى جانب المواجهة الأمنية، المواجهة المالية والتعاون الدولى في مكافحة مكافحة الإرهاب، **وعلى ذلك سوف نتناول ما قام به المشرع المصرى من قوانين في مجال مكافحة الإرهاب من خلال الآتى:**

أولاً: قبل القانون رقم (٩٤) لسنة ٢٠١٥ لمكافحة الإرهاب

ثانياً: بعد القانون رقم (٩٤) لسنة ٢٠١٥ لمكافحة الإرهاب

أولاً: قبل القانون رقم (٩٤) لسنة ٢٠١٥ لـمكافحة الإرهاب

برغم تعدد الأخطار التي لحقت بالمجتمع المصري من جراء العمليات الإرهابية في فترات زمنية مختلفة، إلا أن المشرع المصري ظل لفترة طويلة مفضلاً الاكتفاء بالنصوص العقابية الواردة بقانون العقوبات رقم ٥٧ لسنة ١٩٣٧ وتعديلاته لمواجهة الظاهرة الإرهابية الطارئة على المجتمع.

وقد كشف الواقع المصرى عن وجوب التدخل التشريعى لمواجهة هذه الظاهرة الإجرامية فقد آثر المشرع المصرى إلى إدخال بعض التعديلات على هذه القوانين في مجال التجريم والعقاب والإجراءات الجنائية كأحد الأدوات التي تسهم في مواجهة الإرهاب وردعه من خلال عقوبات رادعة وإجراءات سريعة وحاسمة تلتزم في نفس الوقت باحترام وسيادة القوانين، فصدر القانون رقم (٩٧) لسنة ١٩٩٢ بتعديل بعض نصوص

قوانين العقوبات والإجراءات الجنائية وإنشاء محاكم أمن الدولة وسرية الحسابات بالبنوك والأسلحة والذخائر[١٠٦].

وعلى ذلك لم يجد المشرع مناصاً من التدخل فأصدر بعض التشريعات التي واجهت تلك الأحداث التي تندرج تحت مسمى الإرهاب، حيث أصدر المشرع المصري القانون رقم (٩٧) لسنة ١٩٩٢، بتعديل بعض نصوص قانوني العقوبات والإجراءات الجنائية، بإضافة مجموعة الجرائم الخاصة بالإرهاب إلى المدونة العقابية، وقد نصت المادة الأولى من هذا القانون على أنه "يقسم الباب الثاني من الكتاب الثاني من قانون العقوبات إلى قسمين: **الأول** ويضم المواد من ٨٦ إلى ٨٩ **والثاني:** يضم المواد من ٨٩ مكرر حتى نهاية مواد هذا الباب، وقد أضيفت جرائم الإرهاب إلى مواد القسم الأول.

وقد عرفت المادة (٨٦) الإرهاب بأنه "كل استخدام للقوة أو العنف أو التهديد أو الترويع، يلجأ إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي، بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أمنه للخطر، إذا كان من شأن ذلك إيذاء الأشخاص، أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو الحاق إلحاق الضرر بالبيئة أو بالاتصالات أو بالمواصلات، أو بالأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور أو القوانين أو اللوائح"[١٠٧].

ونلاحظ هنا أن المشرع قد توسع توسعاً ملحوظاً في تعريف الإرهاب فاعتمد على العبارات والمرنة كما اعتمد على الإطلاق اللفظي خروجاً على مبدأ الشرعية الجنائية الذي يحتم أن تصاغ المواد الجنائية في نصوص جامدة وثابتة، وذلك حتى لا تقف جمود النصوص وثباتها عائقا أمام ملاحقة تلك الأفعال الإرهابية ونتائجها.

---

[١٠٦] د. حسنين المحمدى بوادى، تجربة مواجهة الإرهاب، دار الفكر الجامعى بالإسكندرية، الطبعة الأولى، سنة ٢٠٠٤، ص ٥٥-٥٦.

[١٠٧] المادة (٨٦) من القانون رقم ٩٧ لسنة ١٩٩٢ بتعديل بعض نصوص قانون العقوبات والإجراءات الجنائية وإنشاء محاكم أمن الدولة، تم إلغاء محاكم أمن الدولة بموجب القانون رقم ٩٥ لسنة ٢٠٠٣.

(ISSN: 2537 - 0758)

ومن خلال التعريف السابق يمكن ملاحظة الآتى:

١- أنه جاء مطولاً شاملاً لأفعال كثيرة كان من الممكن أن يستغنى عنها ويوضع بدلاً عنها قاعدة عامة لتعريف الإرهاب، تشمل كل ما من شأنه ترويع الآمنيين ولهذا كان النص محل خلاف كبير، فالبعض رآه خطوة مهمة في تحديد مفهوم الإرهاب الذي مازال يشكل مشكلة تحتاج لمزيد من المناقشة، خاصة أن من يبحث بعمق في النص يجده يستبعد الجرائم التي تخلو من استعمال العنف أو القوة أو التهديد أو الترويع مثل تسميم مياة الشرب أو فك براغى السكك الحديدية مثلاً، فضلاً عن أنه قد حدد النتائج المترتبة عن الفعل مما جعل الأمر أكثر دقة وتحديداً.

٢- أن نصوص قانون العقوبات ثابتة نسبياً بينما ظاهرة الإرهاب متغيرة، فأحياناً تزيد وأحياناً تقل حسب يقظة أجهزة الأمن، وبالتالي فإنه يتعين مواجهتها بقوانين مرنة قابلة للتغيير.

٣- استخدام المشرع ألفاظ ذات مدلولات سياسية كتعطيل الدستور أو القوانين أو اللوائح أو الوحدة الوطنية أو السلام الاجتماعى، وهي مدلولات غير متفق أصلاً على تحديد معناها، ومن ثم فهى لا تصلح في مجال التجريم والعقاب الذي يوقع على شخص ارتكب فعلاً محدداً بذاته[١٠٨].

ولعل المشرع أراد بالتوسع في التعريف السابق ألا يفلت من العقاب أي إرهابى من العقاب استناداً إلى فكرة التجريم الوقائى المتمثل في الاحتياط من الإرهاب، بتجريم الأنشطة الإرهابية السابقة على وقوع الحادث الإرهابى، وعليه فقد استحدث المشرع المصرى بالقانون ٩٧ لسنة ١٩٩٢ بعض الصور الخاصة بالنشاط الإرهابى التي درج الفقه على تسميتها بجرائم الإرهاب[١٠٩].

بالإضافة إلى ذلك فقد نص المشرع المصرى على عدد من الجرائم شدد فيها العقوبات المرصودة لها في حالة ارتكابها بغرض الإرهاب من الوسائل التي تستخدم في ارتكابها، وعليه فإن الجرائم الإرهابية في قانون العقوبات المصرى تشمل الجرائم الآتية:

---

[١٠٨] د. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة التجريم وسبل المواجهة، مطبعة العشري، سنة ٢٠٠٦، ص٧-٨.

[١٠٩] د. مدحت رمضان، جرائم الإرهاب في ضوء الأحكام الموضوعية والإجرائية للقانون الجنائى الدولى والداخلى "دراسة مقارنة"، دار النهضة العربية بالقاهرة، سنة ١٩٩٥، ص١٦٨.

أ- الجرائم المستحدثة بموجب القانون ٩٧ لسنة ١٩٩٢.
ب- الجرائم المنصوص عليها سلفاً في قانون العقوبات.

أ- <u>الجرائم المستحدثة: وتشمل هذه الفئة الجرائم التالية:</u>

- جريمة تشكيل جمعية أو هيئة أو منظمة أو جماعة أو عصابة على خلاف أحكام القانون يكون الغرض منها الدعوة إلى تعطيل أحكام الدستور، أو القوانين، أو منع إحدى مؤسسات تادولة من ممارسة أعمالها، أو الاعتداء على الحرية الشخصية للمواطن، أو غيرها من الحريات والحقوق العامة التي كفلها الدستور والقانون، أو الأضرار بالوحدة الوطنية، أو السلام الاجتماعى وهذا طبقاً لنص المادة (٨٦) مكرر الفقرة الأولى.
- جريمة الانضمام إلى إحدى الجمعيات أو التنظيمات الإرهابية أو المشاركة فيها بأية صورة مع العلم بأغراضها وهذا طبقا للمادة (٨٦) مكرر الفقرة الثانية[١١٠].
- جريمة الترويج بالقول، أو بالكتابة، أو بأية طريقة أخرى للأغراض الإرهابية وهذا طبقاً لنص المادة (٨٦) مكرر الفقرة الثالثة.
- جريمة استعمال الإرهاب لإجبار شخص على الانضمام إلى إحدى التنظيمات الإرهابية أو منعه من الانفصال عنها وهذا طبقاً لنص المادة (٨٦) مكرر (ب)[١١١].
- جريمة السعي أو التخابر مع دولة أجنبية، أو لدى جمعية أو منظمة أو جماعة، أو عصابة يكون مقرها خارج البلاد، أو بأحد ممن يعملون لمصلحة أي منها للقيام بأى عمل من أعمال الإرهاب داخل مصر، أو ممتلكاتها، أ، مؤسساتها، أو موظفيها، أو ممثليها الدبلوماسيين، أو مواطنيها أثناء عملهم، أو وجودهم بالخارج وهذا طبقاً لنص المادة (٨٦) مكرر (ج).
- جريمة تعاون المواطن المصرى أو التحاقه بأى جمعية، أو هيئة، أو منظمة، أو جماعة إرهابية يكون مقرها خارج البلاد وتتخذ من الإرهاب أو التدريب العسكرى وسائل لتحقيق أغراضها وهذا طبقاً للمادة (٨٦) مكرر (د)[١١٢].

---

[١١٠] د. محمد محمود سعيد، جرائم الإرهاب "أحكامها الموضوعية وإجراءات ملاحقتها"، دار الفكر العربي، سنة ١٩٩٥، ص٣٢، ص١٠١.

[١١١] د. محمد أبو الفتح الغنام، مواجهة الإرهاب في التشريع المصرى "دراسة مقارنة"، دار النهضة العربية بالقاهرة، سنة ١٩٩٦، ص٦.

(ISSN: 2537 - 0758)

- جريمة اختطاف إحدى وسائل النقل الجوى أو البري أو المائى وهذا طبقاً لنص المادة (٨٨) من قانون العقوبات المصرى.
- جريمة القبض غير المشروع على الأشخاص أو حجزهم أو حبسهم كرهينة، وذلك بقصد التأثير على السلطات العامة في أدائها لأعمالها، أو الحصول منها على منفعة، أو مزية من أي نوع وهذا طبقاً انص المادة (٨٨) مكر من قانون العقوبات.
- جريمة التعدى على أحد القائمين على تنفيذ القانون، أي القائمين على تنفيذ أحكام هذا القسم، وكان ذلك بسبب هذا التنفيذ وهذا طبقاً لنص المادة (٨٨) مكرر (أ).
- جريمة الاشتراك في الأعمال الإرهابية وهي محددة حسب المادة (٤٠) من قانون العقوبات حيث تقرر المادة (٨٨) مكرر (ب) سريان أحكام المواد (٨٢، ٨٣، ٩٥، ٩٦، ٩٧، ٩٨، ٩٨(هـ)) من قانون العقوبات على الجرائم الواردة بالقسم الأول من الكتاب الثانى من قانون العقوبات.
- جريمة القبض غير المشروع على الأشخاص أو حجزهم أو حبسهم كرهينة، وذلك بقصد التأثير على السلطات العامة في أدائها لأعمالها، أو الحصول منها على منفعة، أو مزية من أي نوع وهذا طبقاً انص المادة (٨٨) مكر من قانون العقوبات.
- جريمة التعدى على أحد القائمين على تنفيذ القانون، أي القائمين على تنفيذ أحكام هذا القسم، وكان ذلك بسبب هذا التنفيذ وهذا طبقاً لنص المادة (٨٨) مكرر (أ).
- جريمة الاشتراك في الأعمال الإرهابية وهي محددة حسب المادة (٤٠) من قانون العقوبات حيث تقرر المادة (٨٨) مكرر (ب) سريان أحكام المواد (٨٢، ٨٣، ٩٥، ٩٦، ٩٧، ٩٨، ٩٨(هـ) من قانون العقوبات على الجرائم الواردة بالقسم الأول من الكتاب الثانى من قانون العقوبات[١١٣].

لقد راعى المشرع المصرى في هذه الجرائم أنها ترتكب فى سياق مشروع إرهابى أو تحقيق غاية معينة يستهدفها الجانى من السلوك الصادر منه، ذلك العنف الإرهابى

---

[١١٢] د. محمد محمود سعيد، جرائم الإرهاب "أحكامها الموضوعية وإجراءات ملاحقتها"، المرجع السابق، ص٣٢، ص١٠١.

[١١٣] د. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة التجريم وسبل المواجهة، المرجع السابق، ص٧٤.

يتحرك دائماً انطلاقاً من باعث إيديولوجي يخرج الجانى نحو غاية معينة أو غرض محدد[١١٤].

وتشمل هذه الفئة الجرائم التي تنفذ لغرض إرهابى وهي كالتالى:

- جريمة التشويش على إقامة الشعائر الدينية وتخريب أو كسر أو إتلاف مبانى معدة لإقامة الشعائر أو انتهاك حرمة القبور أو الجبانات أو دنسها وهذا طبقاً لنص المادة (١٦٠) من قانون العقوبات.
- جريمة التسمى بأسم غير الأسم الحقيقى في تذكرة السفر وهذا طبقاً لنص المادة (٢١٦) من قانون العقوبات.
- جريمة صنع تذكرة مرور أو تذكرة سفر مزورة يعاقب بالحبس وهذا طبقاً لنص المادة (٢١٧) من قانون العقوبات.
- جريمة استعمال تذكرة مرور أو تذكرة سفر ليست له وهذا طبقاً لنص المادة (٢١٨) من قانون العقوبات.
- جريمة تدوين أشخاص بأسماء مزورة في دفاتر الفنادق أو المنازل المخصصة للكراء، وهذا طبقاً لنص المادة (٢١٩) من قانون العقوبات.
- جريمة إعطاء تذكرة سفر أو تذكرة مرور باسم مزور بمعرفة وعلم موظف عمومي وسكون استعمالها لغرض إرهابى وهذا طبقاً لنص المادة (٢٢٠) من قانون العقوبات.
- جريمة الجرح أو الضرب الذي ينشأ عنه مرض أو عجز عن الأشغال الشخصية مدة تزيد على العشرين يوماً وهذا طبقاً لنص المادة (٢٤١) من قانون العقوبات ويكون أرتكابها تنفيذاً لغرض إرهابى[١١٥].
- جريمة الجرح أو الضرب الذي ينتج عنه عاهة مستدسمة يستحيل برؤها وذلك طبقاً لنص المادة (٢٤٠) من قانون العقوبات.

---

[١١٤] المواد (١٦٠، ٢١٦، ٢١٧، ٢١٨، ٢١٩، ٢٤٠، ٢٤١، ٢٤٢، ٢٤٣) من قانون العقوبات.

[١١٥] د. محمد أبو الفتح الغنام، مواجهة الإرهاب في التشريع المصرى "دراسة مقارنة"، دار النهضة العربية بالقاهرة، سنة ١٩٩٦، ص٢١٨.

(ISSN: 2537 - 0758)

- جريمة الضرب أو الجرح في صوره البسيطة وتكون العقوبة مشددة في حالة ما إذا ارتكبت لغرض تنفيذ عمل إرهابى وهذا طبقاً لنص المادة (٢٤٢) من قانون العقوبات.
- جريمة الجرح أو الضرب باستعمال الأسلحة أو عصى أو آلات أخرى وهذا طبقاً للمادة (٢٤٣) من قانون العقوبات.

ومما سبق يتبين أن المشرع المصرى في ظل القانون ٩٧ لسنة ١٩٩٢ لم يعتبر الإرهاب في حد ذاته جوهراً للتجريم، وإنما وضع تعداداً على سبيل الحصر لما يطلق عليه الجرائم الإرهابية، أي الجرائم التي يكون الإرهاب فيها عنصراً من عناصرها أو باعثاً دافعاً لاقترافها أو ظرفاً مشدداً لها[١١٦].

وعلى ذلك يتبين أن المشرع المصرى سلك مواجهة الإرهاب القانون رقم ٩٧ لسنة ١٩٩٢ إتجاهين: **الأول** استحداث نصوص جديدة تشمل صور الجرائم المستحدثة للإرهاب، وذلك في المادة الثانية من القانون المشار إليه حيث أضاف عدداً من المواد إلى القسم الأول من الباب الثانى من الكتاب الثانى من قانون العقوبات، **الاتجاه الثانى** تشديد العقوبة على جرائم منصوص عليها بقانون العقوبات إذا ارتكبت لغرض إرهابى ومن هذه الجرائم[١١٧].

كما أصدرت جمهورية مصر العربية تشريع جنائي خاص فقد صدر القانون رقم ٨٠ لسنة ٢٠٠٢ بشأن مكافحة غسل الأموال، وذلك باعتبار أن غسل الأموال قد يعد مصدراً أساسياً لتمويل الجماعات الإرهابية. وبمقتضى هذا القانون أنشئت بالبنك المركزي وحدة مستقلة ذات طابع خاص لمكافحة غسل الأموال، ومن اختصاص هذه الوحدة القيام بأعمال التحري والفحص وإبلاغ النيابة العامة بما يسفر عنه ذلك، ولها أن تطلب من النيابة العامة اتخاذ التدابير التحفظية التي تكفل تجميد الأموال المشتبه في طبيعتها ومصدرها مما يعد جريمة معاقباً عليها في هذا القانون ومنع الأفراد أو الكيانات التي تملك أو تحول إليها هذه الأموال من التصرف فيها[١١٨].

---

[١١٦] د. أحمد محمد أبو مصطفى، الإرهاب ومواجهته جنائياً "دراسة مقارنة في ضوء المادة (١٧٩) من الدستور"، الفتح للطباعة والنشر بالقاهرة، سنة ٢٠٠٧، ص١٢٨.

[١١٧] د. أحمد محمد أبو مصطفى، الإرهاب ومواجهته جنائياً "دراسة مقارنة في ضوء المادة (١٧٩) من الدستور"، المرجع السابق، ص٢٨٤.

[١١٨] المادة (٥) من القانون رقم (٨٠) لسنة ٢٠٠٢.

وبجانب ما تقدم فقد صدقت مصر على معظم اتفاقيات الأمم المتحدة المعنية بمكافحة الإرهاب، وآخرها اتفاقية قمع تمويل الإرهاب، واتفاقية قمع الهجمات الإرهابية بالقنابل، واتفاقية قمع الإرهاب النووي. كما صدقت على الاتفاقية العربية لمكافحة الإرهاب لسنة ١٩٩٨ واتفاقية منظمة الوحدة الإفريقية لمنع الإرهاب[١١٩].

ثانياً: بعد القانون رقم (٩٤) لسنة ٢٠١٥ لـمكافحة الإرهاب

وأصدر المشرع المصرى القانون رقم (٩٤) لسنة ٢٠١٥ لمكافحة الإرهاب في ١٥ أغسطس سنة ٢٠١٥، وهو قانون شامل للتصدي لجرائم الإرهاب وتمويله من الناحيتين الموضوعية والإجرائية.

ونص في مادته الأولى على أن يعمل بأحكام قانون مكافحة الإرهاب المرافق، وتسري على ما لم يرد في شأنه نص في هذا القانون أحكام قانون العقوبات والإجراءات الجنائية. وقد تضمن قانون مكافحة الإرهاب أحكاماً موضوعية وأخرى إجرائية، وتكفلت الأحكام الموضوعية بتحديد المقصود ببعض الألفاظ والعبارات في تطبيق أحكام هذا القانون، ووضع بعض الأحكام العامة التي يخضع لها هذا القانون، وتحديد الجرائم والعقوبات. أما الأحكام الإجرائية فقد تكلفت أساساً بتحديد سلطات مأمور الضبط القضائي والنيابة العامة وسلطة التحقيق المختصة في تطبيق هذا القانون، وتنظيم القضاء الجنائي المختص[١٢٠].

ويلاحظ أن المشرع في قانون مكافحة الإرهاب الصادر بالقرار بقانون رقم ٩٤ لسنة ٢٠١٥ قد توسع في تحديد الجريمة الإرهابية، فلم يقصره على مدلول العمل الإرهابي، بل اعتمد في هذا التحديد- كما نص عليه في الفقرة (ج) من مادته الأولى- على معايير أخرى هي:

(١) الجرائم التي ينص عليها قانون مكافحة الإرهاب، ولو لم يتوافر فيها النموذج القانوني للعمل الإرهابي، دون إخلال بأحكام قانون العقوبات.

---

[١١٩] د. أحمد فتحى سرور، الجرائم الإرهابية في القانون المصرى وفقاً للمعايير الدولية، الهيئة المصرية العامة للكتاب، سنة ٢٠١٨، ص٣٣.

[١٢٠] د. أحمد فتحى سرور، الجرائم الإرهابية في القانون المصرى وفقاً للمعايير الدولية، المرجع السابق، ص٣٣.

(ISSN: 2537 - 0758)

(٢) كل جناية أو جنحة ترتكب باستخدام إحدى وسائل الإرهاب، أو بقصد تحقيق أو تنفيذ غرض إرهابي. وكما بينا، ينصرف كل من الوسيلة الإرهابية والغرض الإرهابي إلى العمل الإرهابي.

(٣) كل جناية أو أو جنحة تقع بقصد الدعوة إلى ارتكاب أية جريمة إرهابية أو التهديد بها[١٢١].

وبالنسبة للتحريض فقد نص المشرع المصرى على معاقبة المحرض بنفس العقوبة المقررة للفاعل الأصلى فقد نصت المادة (٦) من قانون مكافحة الإرهاب المصري على أنه "يُعاقب على التحريض على ارتكاب أية جريمة إرهابية بذات العقوبة المقرة للجريمة التامة، وذلك سواء كان هذا التحريض موجهاً لشخص محدد أو جماعة معينة، أو كان تحريضاً عاماً علنياً أو غير علني، وأياً كانت الوسيلة المستخدمة فيه، ولو لم يترتب على هذا التحريض أثر"[١٢٢].

كما يُعاقب بذات العقوبة المقررة للجريمة التامة كل من اتفق أو ساعد بأية صورة على ارتكاب الجرائم– المشار إليها بالفقرة الأولى من هذه المادة، ولو لم تقع الجريمة بناءً على ذلك الاتفاق أو تلك المساعدة[١٢٣].

فقد خرج المشرع المصري في قانون مكافحة الإرهاب على هذه القاعدة العامة في التحريض فيما نصت عليه المادة (٦) من عبارة "سواء كان هذا التحريض موجهاً لشخص محدد أو جماعة معينة، أو كان تحريضاً عاماً علنياً أو غير علني، وأياً كانت الوسيلة المستخدمة فيه، ولو لم يترتب على هذا التحريض أثر" ولم يتطلب وجود علاقة سببية بين التحري وبين تحقق الجريمة الإرهابية حيث تقع الجريمة تامة في جانب المحرض ويعاقب بعقوبتها حتى لو لم يستجب للتحريض من تم تحريضه أو كان قد استجاب ولم يرتكب الجرم، ومؤدى ذلك أن المشرع المصري اعتبر التحريض جريمة مستقلة في مجال الجرائم الإرهابية.

ونصت الفقرة الثانية من المادة (٦) من قانون مكافحة الإرهاب المصري "كما يُعاقب بذات العقوبة المقررة للجريمة التامة كل من اتفق أو ساعد بأية صورة على ارتكاب

---

[١٢١] المادة الأولى الفقرة (ج) من القانون رقم ٩٤ لسنة ٢٠١٥.

[١٢٢] المادة (٦) من قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥.

[١٢٣] المستشار/ بهاء المري، شرح الجرائم الإرهابية المادية والسيبرانية، دار الأهرام للنشر والتوزيع، القاهرة، الطبعة الثانية، ٢٠٢٢، ص ٢٣٠.

الجرائم المشار إليها بالفقرة الأولى من هذه المادة، ولو لم تقع الجريمة بناءً على ذلك الاتفاق أو تلك المساعدة".

حيث أن الاشتراك بطريق الاتفاق إنما يتحقق باتحاد أطرافه على ارتكاب الفعل المتفق عليه وأن هذه النية داخل النفس والتي لا تقع عادة تحت الحس وليس لها أمارات ظاهرة. ويتحقق الاشتراك بالمساعدة بتدخل الشريك مع الفاعل تدخلاً مقصوداً ويتحقق فيه معنى تسهيل ارتكاب الجريمة الذي جعله الشارع مناطاً لعقاب الشريك[١٢٤].

فالاتفاق يتحقق باتحاد أو تلاقى إرادتين أو أكثر على ارتكاب جريمة أي انعقاد عزمها، ولا يقتضي الاتفاق على ارتكاب الجريمة أكثر من تقابل المشتركين فيها فلا يشترط لتوافره مضى وقت معين فمن الجائز عقلاً وقانوناً أن تقع الجريمة بعد الاتفاق عليها مباشرة، والمساعدة تتحقق بكل عون تبعي يقدمه الشخص إلى فاعل الجريمة من أجل ارتكابها أو بأي وسيلة كإمداد فاعل الجريمة بالمعلومات أو بالمعدات، ولإعتبار المتهم شريكاً بالاتفاق أو المساعدة في جريمة ما، يجب أن تقع الجريمة فعلاً بناء على هذا الاتفاق أو تلك المساعدة، فإذا لم تقع لا يعتبر شريكاً، ومن ثم فنص المادة (٦) يعد خروجاً على القواعد العامة ولو عدل الفاعل عن الاتفاق أو لم يستخدم الفاعل وسيلة المساعدة[١٢٥].

والجدير بالذكر أن قانون مكافحة الإرهاب نص على مكافحة الإرهاب الإلكترونى فنصت المادة ٢٩ من قانون مكافحة الإرهاب في فقرتها الأولى على معاقبة 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 في 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.

ونصت المادة ٢٩ المشار إليها في فقرتها الثانية على معاقبة كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية بقصد الحصول

---

[١٢٤] المستشار/ بهاء المري، شرح الجرائم الإرهابية المادية والسيبرانية، المرجع السابق، ص ٢٣١.

[١٢٥] المستشار/ بهاء المري، شرح الجرائم الإرهابية المادية والسيبرانية، المرجع السابق، ص ٢٣٥.

(ISSN: 2537 - 0758)

على البيانات أو المعلومات الموجودة به، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها[١٢٦].

وبعد ذلك صدر القانون رقم (١١) لسنة ٢٠١٧ بتعديل قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥ بشأن تعديل بعض أحكام قوانين الإجراءات الجنائية الصادر بالقانون رقم ١٥٠ لسنة ١٩٥٠ وقانون حالات وإجراءات الطعن أمام محكمة النقض الصصادر بالقانون رقم ٥٧ لسنة ١٩٥٩، وقانون تنظيم قوائم الكيانات الإرهابية والإرهابيين رقم ٨ لسنة ٢٠١٥، قانون مكافحة الإرهاب الصادر بالقانون رقم ٩٤ لسنة ٢٠١٥.

فقد استحدث القانون رقم ١١ لسنة ٢٠١٧ بتعديل قانون الكيانات الإرهابية إجراءاً تحفظياً على أموال الأنشطة الإرهابية الصادرة من أي إرهابي أو كيان إرهابي سواء أكان مدرجاً أم غير مدرج على قوائم الكيانات الإرهابية والإرهابيين[١٢٧].

فقد نصت المادة ٨ مكرر من القانون رقم ١١ لسنة ٢٠١٧ المشار إليه بأن للنائب العام إذا توافرت معلومات أو دلائل جدية على وجود أموال ثابتة أو منقولة متحصلة من أنشطة أي إرهابي أو كيان إرهابي مدرج أو غير مدرج على قوائم الكيانات الإرهابية والإرهابيين أو تستخدم في تمويله بأي صورة كانت في تمويل المنتسبين إليه أو المرتبطين به أن يأمر بالتحفظ على هذه الأموال ومنع مالكيها أو حائزيها من التصرف فيها. ويعرض أمر التحفظ والمنع من التصرف على الدائرة المنصوص عليها في المادة ٣ من القانون رقم ٨ لسنة ٢٠١٥ خلال شهر من تاريخ صدوره للنظر في تأييده أو إلغائه أو تعديله[١٢٨].

وبعد جهود المشرع المصرى السابق بيانها قام بإصدار القانون رقم (٢٢) لسنة ٢٠١٨ بتنظيم إجراءات التحفظ والحصر والإدارة والتصرف في أموال الجماعات الإرهابية والإرهابين، وذلك بتحديد الأموال محل التحفظ والجهة القائمة على التحفظ (هي لجنة ذات تشكيل قضائى من سبعة أعضاء من قضاة محكمة الاستئناف)– المادة الرابعة من القانون، وكيفية التعاون بين هذه اللجنة والجهات والهيئات والبنوك وتمكين أعضاء اللجنة بالاطلاع على المستندات والمعلومات المطلوبة في المواعيد المحددة وتنفيذ القرارات الصادرة عنها،– المادة العاشرة من القانون[١٢٩].

---

[١٢٦] المادة ٢٩ من قانون رقم (٩٤) مكافحة الإرهاب لسنة ٢٠١٥.

[١٢٧] المادة ٨ مكرر من القانون رقم ١١ لسنة ٢٠١٧.

[١٢٨] المادة ٨ مكرر من القانون رقم ١١ لسنة ٢٠١٧.

[١٢٩] القانون رقم (٢٢) لسنة ٢٠١٨.

ثم صدر القانون رقم (١٤) لسنة ٢٠٢٠ بتعديل بعض أحكام القانون رقم ٨ لسنة ٢٠١٥ في شأن تنظيم قوائم الكيانات الإرهابية والإرهابيين، فقد عرف المشرع في المادة الأولى الكيان الإرهابى والنتائج المترتبة على الإدراج ففي القوائم الإرهابية وفى المادة الثانية نص على التعاون الدولى في مجال تجميد الأموال بالنسبة للكيانات الإرهابية[١٣٠].

ثم صدر القانون رقم (١٥) لسنة ٢٠٢٠ بتعديل بعض أحكام القانون رقم ٩٤ لسنة ٢٠١٥، وذلك لتحديد الأموال والأصول محل التجميد وكذلك تحديد المقصود بتمويل الإرهاب[١٣١].

وعلى ذلك يتضح لنا من خلال ما سبق بيانه أن المشرع المصرى لم يدخر جهد في ملاحقة الجرائم الإرهابية والإرهابيين بشتى الطرق من خلال التعديل المستمر لقانون مكافحة الإرهاب ومكافحة هذا النوع من الجرائم من منبعه وذلك من خلال تجريم تمويل الإرهاب والتوسع في التعاون الدولى فى هذا المجال وهذا ما أكده تقرير جمهورية مصر العربية لمجموعة العمل المالى لمنطقة الشرق الأوسط لعام ٢٠٢١ فقد جاء فيه التصرفات التي أجرتها النيابة العامة على قضايا تمويل الإرهاب وذلك على النحو التالى:

السنة	٢٠١٥	٢٠١٦	٢٠١٧	٢٠١٨	٢٠١٩	المجموع
أعداد الأعمال الإرهابية	٦١٧	١٩٩	٥٠	٨	٢	٨٧٦
عدد الأفراد الذين تم التحقيق معهم في قضايا تمويل الإرهاب	٤٣٣	٥٨٣	٤٣٣	٢٣٩٣	١٥٤	٣٩٩٦
عدد القضايا التي تم إحالتها إلى النيابة العامة بشأن تمويل الإرهاب	٢٩٧	٢٥٩	٢٥٥	٢٥٩	٦١	١١٠١
عدد القضايا التي تم إحالتها للمحاكم بشأن تمويل الإرهاب	٢٥٢	٣٠٠	٣٨	٥٦	١	٦٤٧
عدد حالات الإدانة بشأن تمويل الإرهاب	١٥٤	١٣٠	١٥	٤	٤	٣٠٧
حالات الإدانة بشأن تمويل الإرهاب بشكل مستقل	١٩	١٤	١٠	٢	١	٤٢

[١٣٠] القانون رقم (١٤) لسنة ٢٠٢٠.

[١٣١] القانون رقم (١٥) لسنة ٢٠٢٠.

(ISSN: 2537 - 0758)

يتضح من خلال الإحصائية أن عدد حالات الإدانة بتمويل الإرهاب في تراجع مستمر نتيجة انخفاض العمليات الإرهابية بين ٢٠١٧ و٢٠١٩ بشكل كبير داخل مصر بفضل جهود الدولة من خلال مرفق القضاء فيها[١٣٢].

الفرع الثانى

مكافحة جرائم الإرهاب الإلكترونى في التشريع المصرى

تعد مصر واحدة من أكثر الدول الأفريقية عرضة لخطر الإرهاب الإلكتروني، الترتيب في مصر وجاءت في الترتيب ٢٣ من ١٥٥ دولة فى مؤشر الجاهزية للأمن السيبراني Global Cybersecurity Index GCI الصادر عن "الاتحاد الدولي للاتصالات لعام ٢٠١٨[١٣٣].

لقد تتعدد النصوص القانونية ذات الصلة بمختلف التهديدات السيبرانية بشكل عام والإرهاب الإلكترونى بشكل خاص، وفيما يلي عرض لجهود الدولة المصرية في مكافحة الإرهاب الإلكتروني ومن خلال النصوص التي يمكن الوقوف على أبرزها فيها من خلال النقاط التالية:

- **الدستور المصري:**

تنص المادة ٣١ من الدستور المصري– وفقًا للتعديلات الدستورية التي أُدخلت عليه في ٢٣ أبريل ٢٠١٩–على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"[١٣٤].

كما نصت المادة ٢٣٧ من الدستور ٢٠١٤ المعدل في ٢٠١٩ على أن "تلتزم الدولة بمُواجهة الإرهاب بكافة صورة وأشكاله، وتعقب مصادر تمويله. ويُنظم القانون أحكام وإجراءات مُكافحة الإرهاب والتعويض العادل عن الأضرار الجسيمة عنه وبسببه". وقد تبنَّت الدولة رؤية مُؤداها أن مُكافحة الإرهاب لا يعد إلتزاماً على عاتق الدولة لحماية

---

[١٣٢] تقرير التقييم المتبادل لجمهورية مصر العربية تدابير مكافحة غسيل الأموال وتمويل الإرهاب، مجموعة العمل المالى لمنطقة الشرق الأوسط وشمال أفريقيا، مايو ٢٠٢١، ص٧٠.

[133] Switzerland, 2018, p57 Union، Global Cybersecurity Index GCI.

[١٣٤] المادة ٣١ من دستور جمهورية مصر العربية سنة ٢٠١٤.

أمنها القومي فحسب، وإنما يستهدف أيضاً حماية أحد المبادئ الأساسية لحقوق الإنسان وهو الحق في الحياة، وذلك في إطار مُقاربتها الشاملة[١٣٥].

وإنطلاقاً من الإلتزام الدستوري بمكافحة الإرهاب، فقد وضع المشرع حزمة متكاملة من التشريعات الوطنية التي تتسق مع إلتزامات مصر بموجب قرارات مجلس الأمن والاتفاقات الإقليمية والدولية ذات الصلة بمُكافحة الإرهاب التي إنضمت إليها، وكذلك استراتيجية الأمم المُتحدة العالمية لمُكافحة الإرهاب على نحو يحقق مكافحة فاعلة وشاملة لظاهرة الإرهاب بكافة أبعادها، كما استهدفت التشريعات تعزيز سبل التصدي للطرق المُستحدثة في مجال تمويل الإرهاب ويأتي على رأس هذه التشريعات:

• قانون مكافحة جرائم تقنية المعلومات (القانون رقم ١٧٥ لسنة ٢٠١٨):

يعد صدور قانون مكافحة تقنية المعلومات بمثابة خطوة مهمة، لأنه نص لأول مرة على "تجريم الممارسات السيبرانية غير المشروعة"، مثل: إنشاء المواقع الإلكترونيةالتي تحث على الإرهاب، والتزوير السيبراني، وغير ذلك. ووفقاً له، تتحدد العقوبة وفقًا لحجم وطبيعة الجريمة. ففي حالة جرائم تقنية المعلومات، تُفرض عقوبات كبيرة؛ لما لتلك الجرائم من تداعيات جسيمة على الأمن القومي المصري، علاوة على العقوبات الأخرى المتعلقة بجرائم الاختراق السيبراني، والتزوير، وغير ذلك. ويمكن في هذا الصدد الإشارة إلى مادتين فحسب من ذلك القانون، **وذلك على النحو التالي:**

فقد نصت المادة (٢٠) "يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حساباً خاصاً أو نظاماً معلوماتياً يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها،

[١٣٥] المادة ٢٣٧ من دستور جمهورية مصر العربية سنة ٢٠١٤.

(ISSN: 2537 - 0758)

أو إلغاؤها كلياً أو جزئياً، بأي وسيلة كانت، تكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تتجاوز خمسة ملايين جنيه"[١٣٦].

كما نصت المادة (٢١) على أن "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمدًا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها. ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى العقوبتين. فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تتجاوز مليون جنيه"[١٣٧].

• القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب:

وهو قانون شامل للتصدي لجرائم الإرهاب وتمويله من الناحيتين الموضوعية والإجرائية. وقد تناول المحاور اللازمة للمجابهة القانونية للإرهاب بإجراءات ناجزة وعقوبات رادعة، حيث استُمدت أحكام ذلك القانون من قرارات مجلس الأمن والصكوك والاتفاقات الدولية والإقليمية في مجال مكافحة الإرهاب. وأتى بتعريفات جامعة لكل من: الجماعة الإرهابية، والإرهابي، والجريمة الإرهابية. كما قرر المعاقبة على الشروع في ارتكاب الجريمة الإرهابية أو التحريض عليها بذات العقوبة المقررة للجريمة التامة، ولو لم يترتب على التحريض أثر. ونظَّم المُشَرِّع فيه ضوابط تجميد الأموال والمنع من التصرف فيها، وأوجب القانون تخصيص دوائر لنظر الجنح والجنايات والاستئناف والطعون في قضايا الجرائم الإرهابية.

كما تصدى ذلك القانون لظاهرة الإرهابيين الذين يغادرون أوطانهم للقتال بجوار جماعات الإرهاب، ومد نطاق التجريم لتسهيل التحاق الغير أو تعاونه أو عبوره خارج البلاد بغرض الانضمام إلى الجماعات الإرهابية، إعمالًا لقرار مجلس الأمن رقم ٢١٧٨ لسنة ٢٠١٤. وتصدى المشرع فيه كذلك للترويج لارتكاب الجريمة الإرهابية وللأفكار

---

[١٣٦] المادة (٢٠) القانون رقم ١٧٥ لسنة ٢٠١٨ لمكافحة جرائم تقنية المعلومات،

[١٣٧] المادة (٢١) القانون رقم ١٧٥ لسنة ٢٠١٨ لمكافحة جرائم تقنية المعلومات،

والمعتقدات الداعية لاستخدام العنف بالتجريم، فضلًا عن التصدي صراحة لمشكلة الإرهاب السيبراني تواكباً مع التطورات الحديثة، وهو ما تجلى في المواد التالية:

فقد عرفت المادة (١) الأموال والأصول بجميع الأصول المادية والافتراضية وعائداتها والموارد الاقتصادية، ومنها النفط والموارد الطبيعية الأخرى أو الممتلكات أيًا كان نوعها، سواء كانت مادية أو معنوية، منقولة أو ثابتة، بما في ذلك المستندات والعملات الوطنية أو الأجنبية، والأوراق المالية أو التجارية والصكوك والمحررات المثبتة لكل ما تقدم أيًا كان شكلها، بما في ذلك الشكل الرقمي أو الإلكتروني والائتمان المصرفي والشيكات المصرفية والاعتمادات المستندية، وأي فوائد أو أرباح أو مصادر دخل ترتبت على هذه الأموال أو الأصول أو تولدت عنها، أو أي أصول أخرى أعدت لاستخدامها في الحصول على تمويل أو منتجات أو خدمات وجميع الحقوق المتعلقة بأي منها. كما تشمل الأصول الافتراضية التي لها قيمة رقمية يمكن تداولها أو نقلها أو تحويلها لشكل رقمي وتستخدم كأداة للدفع أو للاستثمار[١٣٨].

وقد عرفت المادة (٣) المقصود بتمويل الإرهاب بقولها "يقصد بتمويل الإرهاب كل جمع أو تلق أو حيازة أو إمداد أو نقل أو توفير أموال أو أصول أخرى أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها لأي نشاط إرهابي فردي أو جماعي منظم أو غير منظم في الداخل أو الخارج، بشكل مباشر أو غير مباشر، أيًا كان مصدره وبأي وسيلة كانت بما فيها الشكل الرقمي أو الإلكتروني، وذلك بقصد استخدامها كلها أو بعضها في ارتكاب جريمة إرهابية أو العلم باستخدامها، سواء وقع الفعل الإرهابي أم لم يقع، أو بتوفير مكان للتدريب أو ملاذ آمن لإرهابي أو أكثر أو تزويده بأسلحة أو مستندات أو غيرها، أو بأي وسيلة مساعدة أخرى من وسائل الدعم أو التمويل أو السفر مع العلم بذلك ولو لم يكن لها صلة مباشرة بالعمل الإرهابي[١٣٩].

وفى المادة (١٥) نص على عقوبة مشددة حيث نصت على أن "يُعاقب بالسجن المؤبد أو بالسجن المشدد الذي لا تقل مدته عن عشر سنين، كل من قام بأية طريقة مباشرة أو غير مباشرة، وبقصد ارتكاب جريمة إرهابية في الداخل أو الخارج، بإعداد أو تدريب أفراد على صنع أو استعمال الأسلحة التقليدية أو غير التقليدية، أو وسائل

---

[١٣٨] المادة (١) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

[١٣٩] المادة (٣) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

(ISSN: 2537 - 0758)

الاتصال السلكية أو اللاسلكية أو الإلكترونية، أو أية وسيلة تقنية أخرى، أو قام بتعليم فنون حربية أو أساليب قتالية أو تقنية، أو مهارات، أو حيل، أو غيرها من الوسائل، أيًا كان شكلها لاستخدامها في ارتكاب جريمة إرهابية، أو حرض على شيء مما ذكر. ويعاقب بالسجن مدة لا تقل عن سبع سنين كل من تلقى التدريب أو التعليم المنصوص عليه في الفقرة السابقة من هذه المادة، أو وجد في أماكنها بقصد الإعداد أو ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة[١٤٠].

وفى المادة (٢٠) فقد تناولت بعض صور الإرهاب إلكترونحيث نصت على أن "يُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من:

١- أخفى أو تعامل في أشياء استعملت أو أعدت للاستعمال في ارتكاب جريمة إرهابية أو الأموال أو الأصول الأخرى التي تحصلت عنها.

٢- أتلف عمداً أو اختلس أو أخفى مستندًا أو محرراً خطياً أو إلكترونياً من شأنه تسهيل كشف جريمة إرهابية أو إقامة الدليل على مرتكبها أو عقابه.

٣- مكن مرتكب أية جريمة إرهابية من الهرب قبل أو بعد القبض عليه"[١٤١].

وفى المادة (٢٩) تناول أيضاً بعض صور الإرهاب الإلكترونى حيث نصت 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 موقعًا إلكترونيًا تابعًا 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"[١٤٢].

---

[١٤٠] المادة (١٥) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

[١٤١] المادة (٢٠) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

[١٤٢] المادة (٢٩) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

والجدير بالذكر أن المشرع المصرى لم يعرف جريمة الإرهاب الإلكتروني، إلا أنه تناول صور لها في المادة (٢٩) من القانون رقم ٩٤ لسنة ٢٠١٥.

كما نصت المادة (٤٦) على الإجراءات المتبعة من سلطة التحقيق حيث نصت على أن "للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في جريمة إرهابية أن تأذن بأمر مسبب لمدة لا تزيد على ثلاثين يوماً، بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها، وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مددًا أخرى مماثلة"[١٤٣].

وعليه، يمكن القول إن القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب هو قانون شامل للتصدي لجرائم الإرهاب. وقد رُوعي فيه تجريم مختلف الأنشطة الإرهابية وفقاً لاتفاقية قمع تمويل الإرهاب والمعايير الدولية في مجال غسل الأموال وتمويل الإرهاب، فقد عرف الكيان الإرهابي والشخص الإرهابي وسبل تمويل الإرهاب وتجميد الأموال، ووقف على إجراءات النشر وإجراءات الطعن وإدارة الأموال المُتحفظ عليها، ما سمح بإدراج عدد من الجماعات الإرهابية المحلية على قوائم الإرهاب في الداخل المصري.

وإنطلاقاً من رغبة الدولة فى مراعاة الاعتبارت العملية التى كشف عنها تطبيق أحكام قانون مكافحة الارهاب الصادر بالقانون رقم ٩٤ لسنة ٢٠١٥، فقد صدر القانون رقم ١٥ لسنة ٢٠٢٠ بشأن تعديل قانون مكافحة الارهاب المشار إليه متضمناً ما يلي:

- استبدل القانون تعريف الأموال أو الأصول الواردة بالمادة (١- بند "و") حتى يشمل جميع الأصول المادية والافتراضية وعائداتها والموارد الاقتصادية وجميع الحقوق المتعلقة بأياً منها وعدد بعض الأدوات القانونية المُنشئة لتلك الحقوق. وشمل الأصول الافتراضية، وذلك بالإضافة إلى العناصر التى شملها التعريف الوارد بالنص القائم، وقصد من ذلك توافق القانون مع التعديلات التى طرأت على منهجية التقييم عن مجموعة العمل المالي ذات الصلة بالأصول الافتراضية ومقدمي الخدمات.

[١٤٣] المادة (٤٦) القانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب.

(ISSN: 2537 - 0758)

- كما استبدل القانون المقصود بتمويل الإرهاب الوارد بالمادة ٣ ليشمل الأموال والأصول الناتجة عن أي نشاط إرهابي فردي أو جماعي مُنظم أو غير مُنظم فى الداخل أو الخارج بشكل مُباشر أو غير مُباشر. وأضاف الدعم المُتمثل فى توفير مكان للتدريب أو ملاذ آمن لإرهابي أو أكثر أو تزويدهم بأسلحة أو مُستندات أو بأية وسيلة مُساعدة أخرى من وسائل الدعم أو التمويل، أو السفر مع العلم بذلك ولو لم يُكن لها صلة بالعمل الإرهابي، وذلك بالإضافة إلى العناصر التى يشملها التعريف الوارد بالنص القائم، وقصد من ذلك توافق القانون مع المعايير الدولية فى تحديد مدلول تمويل الإرهاب بمعنى يستوعب حالة وقوع الفعل الإرهابي أو عدم وقوعه وأكثر من ذلك ولو لم تكن له صلة مباشرة بالعمل الإرهابي.

كما استبدل القانون أيضاً المادة (١٣) الخاصة بتجريم تمويل الإرهاب بهدف شمول التجريم تمويل الإرهاب بقصد سفر أفراد الدولة غير دولة إقامتهم أو جنسيتهم لإرتكاب العمل الإرهابي أو التخطيط أو الإعداد له أو المشاركة فيه، أو تقديم العون أياً كان شكله كما ساوى فى النشاط بين الجريمة التى تقع بواسطة جماعة إرهابية أو شخص اعتباري، حتى تشمل الأنشطة الإرهابية للأشخاص الاعتباريين أيضاً توسيعاً لنطاق التجريم[١٤٤].

واستبدل في مادته الثانية عبارة (الأموال والأصول الأخرى) محل كلمة الأموال أينما وردت بالقانون رقم ٩٤ لسنة ٢٠١٥[١٤٥].

- وأضافت مادته الثالثة إلى القانون رقم ٩٤ لسنة ٢٠١٥ المشار إليه فقرة ثالثة إلى المادة ٣٩، أوجبت الحكم بغرامة إضافية تُعادل قيمة الأموال والأصول المُبيَّنَة بالفقرة الأولى من هذه المادة التى استخدمت أو خصصت للاستخدام فى العمل الإرهابي، إذا تعَذَّر ضبط الأموال أو تم التصرف فيها للغير حسن النية[١٤٦].

يكمل هذه التشريعات القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم التقنية المعلوماتية والذي جاء ليشدد الحصار على الجرائم الإرهابية من خلال تجريم أي فعل

---

[١٤٤] المادة (١) القانون رقم ١٥ لسنة ٢٠٢٠ بتعديل قانون مكافحة الإرهاب.

[١٤٥] المادة (٢) القانون رقم ١٥ لسنة ٢٠٢٠ بتعديل قانون مكافحة الإرهاب.

[١٤٦] المادة (٣) القانون رقم ١٥ لسنة ٢٠٢٠ بتعديل قانون مكافحة الإرهاب.

اختراق أو اعتداء على الأنظمة المعلوماتية للدولة أو أي فعل آخر باستخدام الوسائل المعلوماتية من أجل تسهيل ارتكاب جرائم إرهابية.

الفرع الثالث

معوقات مواجهة الإرهاب الإلكترونى

مما لا شك فيه أن هناك العديد من الصعوبات والمعوقات التي تعترض سُبل مكافحة جرائم الإرهراب الإلكتروني متعددة، وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلاً عن الجرائم العادية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية، أو خلال تعقب الجناة وكشف جرائمهم وتقديمهم للعدالة، لذلك تثور العديد من المشكلات التي تقف عائقاً أمام مكافحة جريمة الإرهاب الإلكتروني.

وسوف نتناول هذه المعوقات من خلال الآتى:

أولاً: المعوقات المتعلقة باكتشاف الجريمة وإثباتها

ثانياً: المعوقات المتعلقة بالمحكمة المختصة والقانون الواجب التطبيق

أولاً: المعوقات المتعلقة باكتشاف الجريمة وإثباتها

الجرائم الإلكترونية بشكل عام وجرائم الإرهاب الإلكترونى بشكل خاص تطرح إشكالية وصعوبة من نوع خاص وهي صعوبة إكتشاف الجريمة وإثباتها بالدليل، فجريمة الإرهاب الإلكترونى تتم بصورة غير مرئية عبر الحاسب الآلى وشبكة الأنترنت مما يصعب إكتشافها وملاحقة الجناة فيها، وعلى ذلك سوف نتناول تلك المعوقات من خلال الاتى:

أ- عدم إكتشاف الجريمة وصعوبة الوصول لدليل

ب- الصعوبات المتعلقة بجهات التحقيق والتعاون الدولى

أ- عدم إكتشاف الجريمة وصعوبة الوصول لدليل

من أهم وأبرز خصائص جريمة الإرهاب الإلكترونى أنها تقع في بيئة إفتراضية – إلكترونية وهذا يترتب عليه عدة نتائج أهمها صعوبة إكتشاف الجريمة أو إكتشافها بعد

(ISSN: 2537 - 0758)

وقت طويل أو عن طريق المصادفة، كما يصعب من التحقيق فيها وهذا بعكس الجرائم التقليدية[١٤٧].

فأغلب الآثار المتخلفة عن الإرهاب الإلكترونى هي آثار لإلكترونية وهي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة فهى شبه معدومة من الناحية المادية ولا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية حتى تظهر للعيان، وبالإضافة إلى ذلك فهناك صعوبة أخرى تصدم بجهات التحقيق عند التصدي لهذا النوع من الجرائم وهي الاصطدام أحياناً بخصوصية الأفراد مع إتساع مجال البحث عن مرتكب هذه الجرائم حيث يتم البحث بين آلاف بل وملايين الشبكات المنتشرة في العالم للوصول لمرتكب هذه الجرائم[١٤٨].

ولصعوبة استخلاص الدليل في مثل هذه الجرائم يعتبر المختصصين هذا الإثبات تحدياً هائلاً لرجال الأمن، حيث أن رجال الأمن غير متخصصيين في هذا النوع من الجرائم وإنما تنحصر معلوماتهم في الجرائم التقليدية وعلى ذلك لن يكون لديهم القدرة على التعامل مع مثل هذه الجرائم من الناحية التقنية[١٤٩].

لذلك يرى جانب من الفقه أن من متطلبات العدالة أن تتحمل الجهزة الحكومية مسئوليتها نحو إكتشاف هذه الجرائم وضبط الجناة ومحاكمتهم، وهذا يقتضي توفير الإمكانيات التقنية اللازمة للتحقيق في الجرائم المعلوماتية بصفة عامة وجرائم الإرهاب الإلكترونى بصفة خاصة، وللقيام بذلك يجب الإستعانة بالكفاءات المهنية المختصصة في هذا المجال، وتوفير الميزانية اللازمة لتحقيق العدالة ومكافحة هذا النوع من الجرائم[١٥٠].

---

[١٤٧] د. خالد ممدوح إبراهيم، التقاضى الإلكترونى، دار الفكر الجامعى، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص٣٢٣.

[١٤٨] د. جميل عبد الباقى الصغير، أدلة الإثبات الجنائى والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠٠٢، ص١١٥.

[١٤٩] د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية "دراسة مقارنة"، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص٢٣.

[١٥٠] د. منصور فهيد سعيد الحارثى، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، بحث منشور بالمجلة القانونية، كلية الحقوق جامعة القاهرة، المجلد ١٥، العدد ٤، فبراير ٢٠٢٣، ص١٠٥٩.

بالإضافة إلى ما سبق فإن هناك مشكلة أخرى تواجه أجهزة العدالة عند مواجهة الجرائم المعلوماتية أو جرائم الإرهاب الإلكترونى بشكل خاص وهي مشكلة فقدان آثار الجريمة، فهذه الجريمة جريمة غير تقليدية وبالتالي لا تخلف آثار مادية كتلك التي تخلفها الجرائم التقليدية[١٥١].

ومما يزيد من خطورة هذه الجرائم إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل المعلوماتية فيمكن محو الدليل في زمن قصير بحيث لا تتمكن السلطات من الإستمرار في التحقيق بشكل سليم[١٥٢]، وبالتالي تظل جريمة الإرهاب الإلكترونى ومرتكبها مجهولين أما أجهزة العدالة لفقدان الدليل على إرتكبها[١٥٣].

وعلى ذلك يجب رفع المستوى التقنى لرجال الضبط في جرائم الإرهاب الإلكترونى، وذلك للسيطرة على آثار الجريمة عن طريق الحاسب الآلى وضبط أدلتها لضبط مرتكبى هذه الجريمة[١٥٤].

ب- الصعوبات المتعلقة بجهات التحقيق والتعاون الدولى

إن جهات التحقيق القضائى التقليدية تعاني عموماً من ضعف الثقافة القانونية اللازمة للتعرف على جرائم الإرهاب الإلكترونى وتقدير خطورتها، ومثل هذه الإشكالية تتضاعف مع غياب الإطار التشريعى الذي يواجهها، ويزيد من التحدى أن الجناة في هذه الجرائم لهم المفردات الخاصة بهم لدرجة أنهم يطلقون على أنفسهم اسم (النخبة) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلى ولغاته، ويطلقون على رجل الشرطة والنيابة والقضاء صفة (الضعفاء)، وهذا ما يبين مدى القصور في الناحية التقنية لدى رجال السلطة العامة[١٥٥].

---

[١٥١] د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، المجلد الأول، ١٩٩٠، ص٢٨٢.

[١٥٢] د. خالد ممدوح إبراهيم، التقاضى الإلكترونى، دار الفكر الجامعى، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص٣٢٤.

[١٥٣] د. منصور فهيد سعيد الحارثى، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، مرجع سابق، ص١٠٦٧.

[١٥٤] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص٣٥.

[١٥٥] د. عبد الفتاح بيومى حجازى، مبادئ الإجراءات الجنائية في جرائم الكمبيور والأنترنت، مرجع سابق، ص١٢٤.

(ISSN: 2537 - 0758)

وهذا القصور الفني والمعرفى يتطلب معالجته من عدة نواحى أهمها التدريب التخصصي لجهات التحقيق لزيادة مهارتهم على أن يتم إختيار المتدربين على أعلى مستوى من ناحية المؤهلات والقدرات الذهنية والنفسية لتلقى هذا النوع من التدريب[١٥٦].

هذا من ناحية جهات التحقيق، ومن ناحية التعاون الدولى فهناك ضعف في التعاون والتنسيق بين الدول في مكافحة جريمة الإرهاب الإلكترونى، ورغم المناداة بضرورة التعاون الدولى في مكافحة الإرهاب الإلكترونى ألا أن هناك عوائق تحول دون ذلك[١٥٧]، **وأهم هذه العوائق:**

١- <u>إختلاف النظم القانونية بين الدول</u>

فالأنظمة القانونية في الكثير من الدول لمواجهة الإرهاب الإلكترونى لا يوجد فيها إتفاق عام مشترك حول نماذج هذه الجريمة فقد تكون الأفعال المكونة للجريمة مباحة في دولة ومجرمة في دولة أخرى، وبسبب هذا الإختلاف نجد أن طرق التحرى والتحقيق والمحاكمة التي ثبت فاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى ومن ذلك المراقبة المعلوماتية، والتسليم المراقب وغيرها من الإجراءات التى تساعد في ضبط هذه الجريمة، وبالتالي فالدولة التي تستخدم هذه الأساليب سوف تشعر بخيبة أمل تجاه الدول الأخرى التي لا تستخدم هذه الأساليب لمكافحة لهذه الجريمة[١٥٨].

٢- <u>عدم وجود معاهدات ثنائية أو جماعية بين الدول</u>

برغم من وجود معاهدات تعاون ثنائية بين الدول في مجال مكافحة جريمة الإرهاب الإلكترونى، وكذلك وجود بعض المعاهدات الجماعية التي تنظم الجرائم المعلوماتية بشكل عام ألآ أنها قاصرة عن تحقيق المطلوب في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الأنترنت، ومن ثم تطور الجريمة المعلوماتية والإرهاب الإلكترونى بذات

---

[١٥٦] د. عمر محمد بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٨٠٩.

[١٥٧] د. حاتم عبد الرحمن منصور، الإجرام المعلوماتى، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠٢، ص١٥٣.

[١٥٨] د. جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دارالنهضة العربية، القاهرة، ٢٠٠٢، ص٧٢.

السرعة على نحو يؤدى إلى إرباك المشرع وسلطات الأمن في الدول مما يخل بالتعاون فيما بينها[١٥٩].

٣- مشكلة الإختصاص القضائى

من أهم خصائص جريمة الإرهاب الإلكترونى أنها عابرة للحدود، وعلى ذلك تثور مشكلة الإختصاص على المستوى الدولى بسبب إختلاف التشريعات والنظم القانونية التي ينجم عنها تنازع في الإختصاص بين الدول بالنسبة لجرائم الإرهاب الإلكترونى، بإعتبارها جريمة دولية[١٦٠].

وهذا التنازع يستلزم مزيد من التعاون بين الدول من خلال عقد معاهدات ثنائية وجماعية في إطار الأمم المتحدة لفض تنازع الإختصاص بين الدول عند تناول جرائم الإرهاب الإلكترونى، مع التأكيد على التطوير المستمر لهذه المعاهدات ومراجعتها بصورة دورية لملاحقة التطور التكنولوجى والتقنى في مجال الجرائم المعلوماتية بشكل عام وجرائم الإرهاب الإلكترونى بشكل خاص.

ثانياً: المعوقات المتعلقة بالمحكمة المختصة والقانون الواجب التطبيق

ان تحديد المحكمة المختصة والقانون الواجب التطبيق من أهم المشكلات التي تعوق مواجهة جرائم الإرهاب الإلكترونى وقد حاول المشرع المصرى التغلب على هذه الإشكالية من خلال النص في المادة (٣) في قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، بتحديد نطاق تطبيق القانون من حيث المكان " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني، وذلك في أي من الأحوال الآتية:

---

[١٥٩] د. محمود صالح العادلى، الجريمة الدولية "دراسة مقارنة"، مرجع سابق، ص٤١.

[١٦٠] د. نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتى، منشأة المعارف الإسكندرية، ٢٠٠٨، ص١٢٣.

(ISSN: 2537 - 0758)

١- إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.
٢- إذا كان المجني عليهم أو أحدهم مصرياً.
٣- إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية.
٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية.
٥- إذا كان من شأن الجريمة إلحاق ضرر بأي من موطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها في الداخل أو الخارج.
٦- إذا وُجد مرتكب جريمة في جمهورية مصر العربية بعد ارتكابها ولم يتم تسليمه[١٦١].

وعلى ذلك فقد تبنى المشرع المصرى معيار دقيق يتماشى مع طبيعة هذه الجرائم فالمادة (٣) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، قامت بالجمع بين العديد من المعايير في تحديد القانون الواجب التطبيق فقد تبني مبدأ الإقليمية ويتبين ذلك في الفقرة الأولى، كما تبني مبدأ الشخصية ويقصد ذلك بتطبيق القانون المصري على كل من يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها، أو كان المجني عليه مصرياً، ولو كان الجاني أجنبياً وارتكب الجريمة خارج إقليم الدولة، كذلك تبني مبدأ العينية بأن القانون المصري يطبق على الجرائم التي ترتكب بالخارج بغض النظر عن جنسية مرتكبها، ويتبين ذلك في الفقرة (٥) إذا كان من شأن الجريمة إلحاق ضر بأي من موطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج.

وعلى ذلك يمكن القول رغم مسلك المشرع المصرى بشأن القانون الواجب التطبيق وهو مسلك محمود لمواجهة هذا النوع من الجرائم ألا أنه يجب أن يتم في إطار تعاون إقليمى ودولى حتى لا يتصدم مبدأ السيادة القضائية للدول التي يجب تطبيق القانن المصرى على أراضيها وحتى يتم تطبيق القانون صورة صحيحة.

[١٦١] المادة (٣) في قانون رقم ١٧٥ لسنة ٢٠١٨

الخاتمة

من خلال عرضه في هذه البحث يتضح لنا أنه مما لا شك فيه أن الإرهاب الإلكتروني هو أحد أشكال الإرهاب عموماً، ولكنه من أخطر أشكال الإرهاب وخاصة بعد اعتماد المجتمعات على التكنولوجيا عسكرياً واقتصادياً، أصبح هو الشكل الأكثررعباً الذي يواجهه العالم، فهو عابر للحدود، وقليل التكلفة، ويصعب إكتشاف مرتكبيه، كما أن هناك بعض الدول لم تجرم الأفعال المكونة لهذا النوع من الجرائم حتى الآن.

ولذلك، سعت الدول بشكل فردي وجماعي في إطار المنظمات الدولية إلى تبني سياسات واستراتيجيات لمكافحة الإرهاب الإلكترونى، فعمدت إلى خلق هياكل تنظيمية لذلك، كما قامت بدعم التكنولوجيا لسد الثغرات الأمنية التي يمكن أن يفلت منها الإرهابيون فى الفضاء الإلكتروني، كما سعت أيضاً إلى بناء منظومة قانونية لتجري صور الإرهاب الإلكتروني وعمدت أيضاً إلى تعزيز التعاون القضائي الدولي لتحقيق هذا الغرض.

غير أن معظم السياسات التي تم وضعها في هذا المجال إلى الآن لا تزال قاصرة على التأمين الكافى للدول من هجمات الإرهاب الإلكترونى، فهو يتخطى كل الحدود ويتجاوز كل السيادات ولا يمكن مواجهته إلا بوضع سياسات أمنية داخلية في إطار سياسة دولية عامة، حيث أن مشكلة الإرهاب الإلكترونى ليست مشكلة محلية فهى من أخطر أنواع الجرائم المنظمة، ولذلك ومن الضرورى العمل على تنسيق الجهود الدولية لمواجهتها ومكافحتها.

فمكافحة الإرهاب الإلكتروني في الوضع الراهن ليست بالفعالية التي يمكن بها أن تتصدي لظاهرة كظاهرة الإرهاب الإلكتروني، فإذا أخذنا المواجهة التقنية وجدناها هشة أمام أبسط الهجمات الإرهابية، فضلاً من أن الإرهابيين يطورون قدراتهم الفنية في التعامل مع تلك التقنيات المستعملة، كما يمكني أيضاً الاستعانة بالهاكرز الذين يملكون معرفة مستفيضة في مجال تقنيات ونظم المعلومات، مما يجعل الوقوف في وجه نشاطاتهم أمر بالغ الصعوبة.

(ISSN: 2537 - 0758)

ومن خلال البحث وجدنا أن الدولة المصرية بذلت الكثير من الجهد في مجال مكافحة الإرهاب في صورته التقليدية ونجحت في مواجهته، ألا أنها تعاني من بعض القصور التشريعى في مجال الإرهاب الإلكترونى وهو ما يجب مواجهته ووضع الحلول المناسبة له من خلال سن تشريعات تواجه هذا النوع المستحدث من الجرائم في ضوء الإتفاقات الدولية والتنسيق الدولى إقليمياً ودولياً فى إطار الأمم المتحدة.

ومن خلال البحث توصلنا إلى عدة نتائج وتوصيات وهي كالآتى:

أولاً: النتائج

١- يعد الإرهاب الإلكتروني هو الشكل الأحدث للإرهاب حيث يهدد السلم والأمن الداخلى والدولى.

٢- الإرهاب الإلكترونى من أخطر أشكال الإرهاب على الإطلاق بسبب تعدد أشكاله تنوع أساليبه وإتساع الأهداف التى يمكن الوصول إليها.

٣- يفوق تأثير الإرهاب الإلكترونى الإرهاب التقليدي حيث يكون موجه لكل الأفراد التذين يستخدمون شبكة الأنترنت وهو عدد غير محدود، بعكس الإرهاب التقليدى حيث ينحطر نطاقه في منطقة محددة وعلى فئة معينة من الأفراد.

٤- يتطور الإرهاب الإلكترونى بتطور أنظمة الحاسب الآلى وهو ما يصعب أمر ملاحقة الإرهابين ورصدهم. فكل تطور جديد يطرأ على الساحة التقنية يقابلها ظهور أشكال جديدة من الإرهاب.

٥- الإرهاب الالكتروني غير محصور بزمان ومكان معين لذلك يتطلب من الدولة متابعته باستمرار.

٦- عدم وجود تشريعات قانونية صريحة تحد من جريمة الإرهاب الالكتروني رغم وجود قوانين لمكافحة الإرهاب التقليدي وأثبتت فعاليتها في هذا المجال.

ثانياً: التوصيات

١- يجب توفير البرامج والأنظمة اللازمة لحماية الفضاء الإلكتروني والكشف المبكر من الهجمات الإرهابية المحتملة.

٢- يجب سن قوانين على المستوى الداخلى والدولى لمكافحة الإرهاب الإلكترونى مع ضرورة مراجعتها باستمرار لملاحقة التطور الحاصل في هذا المجال.
٣- يجب التنسيق بين الجهات المختلفة تشريعية وقضائية وتنفيذية من اجل سد الثغرات والنقص التشريعى لمواجهة الإرهاب الإلكترونى.
٤- يجب التعاون بين الدول لعقد إتفاقيات ثنائية ومتعددة الأطراف للتعاون في مجال تسليم المجرمين.
٥- عمل وحدات لمراقبة شبكات الأنترنت داخلياً ودولياً لرصد الإرهابين وملاحقاتهم.
٦- إنشاء وتدريب جهاز شرطة متخصص لمكافحة الإرهاب الالكتروني مزود بكافة الإمكانيات المادية والنظم المعلوماتية والتكنولوجية.
٧- إنشاء جهاز قضائي متخصص، يفوت على الإرهابى الالكتروني فرصة الإفلات من العدالة.
٨- توظيف وسائل الإعلام للتوعية الأمنية وتوضيح مخاطر الإرهاب الالكتروني ونشرها في المجلات الدورية والصحف والفضائيات لضبط الجناة وذوي النزعة الإرهابية.
٩- ضرورة التعاون والتنسيق بين الدول في مجال مكافحة تلك الجرائم ووضع الأحكام القانونية لضبط المعاملات الإلكترونية والتفتيش والرقابة عليها.

(ISSN: 2537 - 0758)

قائمة المراجع

المراجع العربية

أولاً: الكتب

- د. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة التجريم وسبل المواجهة، مطبعة العشري، سنة ٢٠٠٦.
- د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، ٢٠٠٦.
- د. أحمد فتحي سرور:

١- حكم القانون في مواجهة الإرهاب، الدار الجامعية، ٢٠٠٥.

٢- المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠٨.

٣- الجرائم الإرهابية في القانون المصرى وفقاً للمعايير الدولية، الهيئة المصرية العامة للكتاب، سنة ٢٠١٨.

- د. أحمد محمد أبو مصطفى، الإرهاب ومواجهته جنائياً "دراسة مقارنة في ضوء المادة (١٧٩) من الدستور"، الفتح للطباعة والنشر بالقاهرة، سنة ٢٠٠٧.
- د. أحمد يوسف جمعة، الإرهاب السيبراني والعملات الافتراضية والتجسس الإلكتروني، دار الأهرام للنشر والتوزيع، المنصورة، ٢٠٢١.
- د. أمير فرج يوسف:

١- الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، دار الوفاء القانونية، القاهرة، ٢٠١١

٢- مكافحة جريمة الإرهاب الإلكترونى، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٦.

- د. أميرة عبد العزيز العربي، جذور الإرهاب وآليات المواجهة، أطلس للنشر والإنتاج الإعلامي، مصر، ٢٠١٩.
- د. جميل عبد الباقى الصغير:

١- أدلة الإثبات الجنائى والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠٠٢

٢- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دارالنهضة العربية، القاهرة، ٢٠٠٢

- د. حاتم عبد الرحمن منصور، الإجرام المعلوماتى، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠٢
- د. حسنين المحمدى بوادى، تجربة مواجهة الإرهاب، دار الفكر الجامعى بالإسكندرية، الطبعة الأولى، سنة ٢٠٠٤
- د. حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، التسريبات، التجسس، الإرهاب الإلكتروني، دار الفكروالفن، مدينة السادس من أكتوبر، ٢٠١٤
- د. حمد عبد المنعم عبد الخالق، الجرائم الدولية د راسة تأصيلية للجرائم ضد الإنسرانية والسلام والحرب، الطبعة الأولى، دار النهضة المصرية، القاهرة، ١٩٨٩
- د. خالد ممدوح إبراهيم، التقاضى الإلكترونى، دار الفكر الجامعى، الإسكندرية، الطبعة الأولى، ٢٠٠٧
- د. دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢
- د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠١٢
- د. عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩
- المستشار/ عبد الفتاح بيومى حجازى:

١- مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦

٢- مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧

- د. عبد الله نور شعت، التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، ٢٠١٧
- د. علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، منشأة المعارف، الإسكندرية، ٢٠٠٦
- د. عماد مجدي عبد الملك، د. عماد مجدي عبد الله، جرائم الكمبيرتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١١

(ISSN: 2537 - 0758)

- د. عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، المجلد الأول، ١٩٩٠
- د. عمر محمد بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٤
- د. كامل السعيد، شرح الأحكام العامة في قانون العقوبات، الدار العلمية للنشر والتوزيع، ٢٠٠١
- د. محمد أبو الفتح الغنام، مواجهة الإرهاب في التشريع المصرى "دراسة مقارنة"، دار النهضة العربية بالقاهرة، سنة ١٩٩٦
- د. محمد عبد الحميد عرفه، د. أمين مصطفى محمد، علم الإجرام والعقاب، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٦
- د. محمد عبد اللطيف عبدالعال، جريمة الإرهاب، دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٤
- د. محمد عبد الله، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦
- د. محمد على سويلم، الأحكام الموضوعية والإجرائية للجريمة المنظمة، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٩
- د. محمد محمود سعيد، جرائم الإرهاب "أحكامها الموضوعية وإجراءات ملاحقتها"، دار الفكر العربي، سنة ١٩٩٥
- د. محمود شريف بسيونى، الجرائم ضد الإنسانية في القانون الجنائى الدولى، الطبعة الثانية، ١٩٩٩
- د. محمود صالح العدلى، الجريمة الدولية، دار الفكر الجامعى، الإسكندرية، ٢٠٠٤
- د. مدحت رمضان، جرائم الإرهاب في ضوء الأحكام الموضوعية والإجرائية للقانون الجنائى الدولى والداخلى "دراسة مقارنة"، دار النهضة العربية بالقاهرة، سنة ١٩٩٥
- د. مصطفى أحمد فؤاد، أصول القانون الدولي العام، منشأة المعارف، الإسكندرية، ٢٠٠٨

- د.مصطفى محمد موسى، الإرهاب الإلكتروني "دراسة قانونية–أمنية–نفسية–إجتماعية"، دار الكتب والوثائق القومية المصرية، الطبعة الأولى، القاهرة، الطبعة الأولى، ٢٠٠٩
- د. منير محمد الجهيني، د. ممدوح محمد الجهيني، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي، ط ١، الاسكندرية، ٢٠٠٤
- د. نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتى، منشأة المعارف الإسكندرية، ٢٠٠٨
- د. هشام محمد فريد رستم:

١– الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤

٢– الإرهاب الدولي، دار النهضة العربية، القاهرة، ٢٠٠٣

- د. هلالي عبد اللاه أحمد:

١– جرائم المعلوماتية وأساليب المواجهة وفقاً لاتفاقية بودابست، دار النهضة، ط ١، القاهرة، ٢٠٠٧

٢– اتفاقية بودابست لمكافحة الجرائم المعلوماتية "معلقاً عليها"، دار النهضة العربية، القاهرة، ٢٠١١

- د. يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، ٢٠١١

ثانياً: الرسائل العلمية

- د. غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق بالجامعة الإسلامية في لبنان، ٢٠٠٤.

ثالثاً: الأبحاث القانونية والمؤتمرات الدولية

- د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته، محاضرة ألقيت بملتقى دولى بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، أيام ٢–٢٠١٤/٩/٤.

(ISSN: 2537 - 0758)

- د. جمال علي دهشان، الإرهاب في العصر الرقمى (الإرهاب الإلكترونى) "صوره، مخاصره، آليات مواجهته"، بحث منشور في مركز المعرفة الدولى، المجلد (١)، العدد (٣)، ٢٠١٨.
- د. حسن سعد محمد عيسى سند، جرائم الإرهاب الإلكترونى من منظور القانون الدولى العام، بحث منشورمجلة كلية الحقوق، جامعة المنيا، المجلد الخامس، العدد الثانى، ديسمبر ٢٠٢٢.
- د. شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية العدد١، المجلد ١٧ كلية القانون الامارات يونيو ٢٠٢٠.
- د. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، ٢-٣ يونيو ٢٠٠٨.
- د. محمد أبو المجد محمد سليم، بحث بعنوان المساهمة والتحريض على الإرهاب الإلكتروني عبر وسائل التواصل الإلكتروني، مجلة البحوث القانونية والإقتصادية (المنصورة)، ٢٠٢١.
- د. محمد محي عوض، مشكلات السياسة الجنائية المعاصرة جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣.
- د. منصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، بحث منشور بالمجلة القانونية، كلية الحقوق جامعة القاهرة، المجلد ١٥، العدد ٤، فبراير ٢٠٢٣.
- د. هشام بشير، "الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي"، آفاق سياسية، العدد ٤، القاهرة: المركز العربي للبحوث والدراسات، يونية ٢٠١٤.
- د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ٢٠٠٠.

رابعاً: القوانين والمعاهدات الدولية

أ- القوانين والدساتير

- الدستور المصرى لسنة ٢٠١٤.
- القانون رقم ٩٧ لسنة ١٩٩٢ بتعديل بعض نصوص قانون العقوبات والإجراءات الجنائية وإنشاء محاكم أمن الدولة.
- القانون رقم ٨٠ لسنة ٢٠٠٢ بشأن مكافحة غسل الأموال والمعدل بالقرار بقانون رقم ٣٦ لسنة ٢٠١٤.
- القانون رقم (٩٤) لسنة ٢٠١٥ لمكافحة الإرهاب وتعديله بالقانون رقم (١١) لسنة ٢٠١٧.
- القانون رقم ١٧٥ لسنة ٢٠١٨ لمكافحة جرائم تقنية المعلومات.
- القانون رقم ١٥ لسنة ٢٠٢٠ بتعديل قانون مكافحة الإرهاب.

ب- المعاهدات الدولية

- ميثاق الأمم المتحدة.
- الملحقان البروتوكولان الإضافيان إلى اتفاقيات جنيف المعقودة في ١٢أغسطس١٩٤٩.
- نظام روما الأساسي للمحكمة الجنائية الدولية المعتمد في روما في ١٧ يولية ١٩٩٨.
- الإتفاقية العربية لمكافحة الإرهاب ١٩٩٨.
- اتفاقية بودابست لمكافحة جريمة الإرهاب الالكتروني ٢٠٠١.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢٠١٠/١٢/٢١.

ج- التقارير والمنشورات الدولية

- التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية الصادر في ٢٣ نوفمبر ٢٠٠١.
- تقرير لجنة منع الجريمة والعدالة الجنائية عن أعمال دورتها السادسة عشرة، فيينا، ٢٨ أبريل ٢٠٠٦، ٢٣-٢٧ أبريل ٢٠٠٧.
- منشور اللجنة الدولية للصليب الأحمر بعنوان "القانون الدولي الإنسانى إجابات على أسئلتك، جنيف سويسرا، ٢٠١٥.
- تقرير التقييم المتبادل لجمهورية مصر العربية تدابير مكافحة غسيل الأموال وتمويل الإرهاب، مجموعة العمل المالى لمنطقة الشرق الأوسط وشمال أفريقيا، مايو ٢٠٢١.

(ISSN: 2537 - 0758)

المراجع الأجنبية

- Eugen Walter: Terror and Resistance A Study of Political Violence with case studies of some Primitive African communities OXFORD University New, 1999 .
- Alix DESFORGES “Cyberterrorisme: quel périmètre?” Fiche de l’Irsem n° 11 décembre 2011.
- DOROTHY E. DENNING” Cyber terrorism” Global Dialogue Autumn 2000 .
- John Arquilla David Ronfeld: Networks and Netwars: The Future of Terror Crime and Militancy. USA Rand publication 2001.
- Ushie Henry Ekpe: The Impact of Terrorism (Including Cyber Terrorism) and Threats of Terrorism on International Business (or Nation Sate). Journal of the International Relations and Affairs Group Volume 3 Issue 1 2013.
- Haut-Commissariat des Nations Unies aux droits de l’homme Fiche d’information n° 32 chap. III sect. H.