جامعة العربي التبسي- تبسة- الجزائر
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر
تخصص: قانون جنائي وعلوم جنائية

بعنوان:

الجهود الدولية في مكافحة الإرهاب الإلكتروني

إعداد الطالب:
شرفي صبري

إشراف الأستاذ(ة):
قحقاح وليد

أعضاء لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة في البحث
بوساحية سايح	أستاذ	رئيسا
قحقاح وليد	أستاذ محاضر –أ-	مشرفا
أحمد بومعزة نبيلة	أستاذة محاضر –أ-	مناقشا

السنة الجامعية 2023-2024

جامعة العربي التبسي- تبسة- الجزائر
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر
تخصص: قانون جنائي وعلوم جنائية

بعنوان:

الجهود الدولية في مكافحة الإرهاب الإلكتروني

إعداد الطالب:
شرفي صبري

إشراف الأستاذ(ة):
قحقاح وليد

أعضاء لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة في البحث
بوساحية سايح	أستاذ	رئيسا
قحقاح وليد	أستاذ محاضر –أ-	مشرفا
أحمد بومعزة نبيلة	أستاذة محاضر –أ-	مناقشا

السنة الجامعية 2023-2024

الكلية لا تتحمل أي مسؤولية على ما يرد
في هذه المذكرة من آراء

قائمة المختصرات:

I.باللغة العربية:

- ج ر: الجريدة الرسمية للجمهورية الجمهورية الجزائرية الديمقراطية الشعبية
- د. ت.ن: دون تاريخ نشر.
- ط: طبعة
- د.ط: دون طبعة.
- ص: الصفحة.
- ص ص: من الصفحة إلى الصفحة
- د.د.ن: دون دار نشر

II.باللغة الفرنسية:

- Ed: Edition.
- N°: Numéro
- P: page

شكر وعرفان

الحمد لله عظيم فضله وكثير عطاءه، وله نسجد سجود الحامدين الشاكرين،

لأن وفقنا لإتمام هذا العمل المتواضع

ولأن حسن السجية يوجب إبداء الشكر والتحية للأستاذ المشرف الدكتور:

قحقاح وليد

الذي لم يبخل علينا بنصائحه وتوجيهاته القيمة والتي ما لبث أن يكون دعما لنا نحي تواضعه وسمو أخلاقه فقد أتاح أن نهلنا من عمله وأن ننهل فله من الله عظيم الجزاء وله منا بالغ الشكر والتقدير

ونشكره على ما قدمه لنا من يد المساعدة والعون لإنجاز هذا العمل عبر تشجيعه لنا من خلال توجيهاته الذي ما فتئ يمدنا بها عبر مختلف مراحل هذا العمل

فخالص شكرنا وعرفاننا لكم

ولا ننسى أن نتقدم بالشكر إلى كل الأساتذة الجامعة وجميع زملاء الدراسة.



إهداء

لى من بث فيا الروح إلى هذا الزمان، إلى من حقاني بنعمه الجليلة وآلاته، ومن رزقني رزقاً طيباً مباركا ... نعم الإيمان الله حسبي.

إلى من كانا سبب في وجودي إلى نور حياتي وضياء دربي إلى من أسعى لبلوغ ..... رضاهما أمي ..... أبي

إلى روح أبي الطاهرة التي طالما انتظرت هذا اليوم ولكن تجري الرياح بما لا تشتهي السفن رحمه الله تبارك وتعالى داعيا من المولى عز وجل أن يسكنه فسيح جناته في جوار نبيه و مصطفاه سيدنا محمد صلى الله عليه وسلم.

إلى من كدت وجدت من أجلي وتحملت مصاعب الحياة لأكون نورا ومشعلا .....رمزا للصبر زوجتي... الوفية، وراعية بيتي ، ومربية أولادي. إلى أولادي الأعزاء : رؤية ، محمد عبد الرحمان ، إسحاق، ملاك، يعقوب.

إلى سندي في الحياة إخوتي وأخواتي الفضلاء حفظهم الله. إلى من تربطني بهم قرابة الدم وذوي رحمي وإلى كل الأهل والأحبة واللذين لم آتي على ذكرهم.

إلى من اعتبرتهم دوما أخوتي وأفراد من عائلتي كل أصدقائي و زملائي إلى من قاسمني ثمرة هذا العمل.

إلى كل من أدركه شفاف قلبي و عجز اللسان عن نطقهم ولم يدركهم قلمي إلى كل من ساندني وشجعني من قريب أو بعيد إلى هؤلاء أهدي ثمرة جهدي وعملي

شرقي صبري

مقدمة

مقدمة:

يعد الإرهاب الإلكتروني ظاهرة إجرامية عابرة للحدود الوطنية، حيث نتجت عن التطور الرهيب في التكنولوجيا التي أصبحت الأكثر اعتمادا في متطلبات الحياة، لاسيما الخدمات النوعية في معظم الدول، فقد يمكن القول بأن العالم أصبح عالم صغير عبر تطور شبكات التوصل الحديثة، حيث نجم عن ذلك مجتمع معلوم يعتمد في نشاطه على تكنولوجيات الإعلام والاتصال كوسائل التواصل الاجتماعي وكذا البريد الإلكتروني وغيرها وسائل التكنولوجيا، فمؤخرا لاحظ العالم بروز الذكاء الاصطناعي، الذي أحدث قفزة نوعية في التكنولوجيات الحديثة، وقبل ظهور الثورة الرقمية كان المجرم الكلاسيكي يعتمد على التخطيط والتنقل لتنفيذ الأعمال الإجرامية، ومن بينها الأعمال الإرهابية بأنواعها، من تفجيرات وقتل للأبرياء واستهداف للممتلكات بغرض تغيير النظام السياسي من جهة، و الإرهاب الإلكتروني من جهة أخرى، وبالفعل ما تقدمه التكنولوجيا أصبح يعتمد الإرهابي على الوسائل الإلكترونية التي تسهل القيام بإجرامه متى أراد، وبسهولة عبر لوحة المفاتيح أو نقر بالماوس.

ويشكل الإرهاب الالكتروني ظاهرة بالغة الأهمية لما ينطوي عليه من تهديدات تمس بأمن جل الدول، حيث يكون الفعل الإجرامي هنا أقرب للجريمة المنظمة، فأصبحت التنظيمات الإرهابية تستغل الفضاء السيبراني، من أجل استقطاب المؤيدين وتجنيدهم بسهولة، مما يستوجب البحث في خصوصية هذه الجريمة، كما يعتبر الإرهاب الإلكتروني أحدث ما توصل إليه العقل الإجرامي.

لثورة التكنولوجية والمعلوماتية، وبالتوافر السهل لشبكة الإنترنت وملحقاتها المادية حيث أصبح العالم دولا وأفرادا يتعرض يوميا لهجمات إرهابية عبر الفضاء الرقمي، وتختلف حدة هذه الهجمات حسب نوعها وهدفها وغايتها.

فقد تصيب المصالح الأساسية للدول وأمنها أو سيادتها القومية، فقد تستهدف سلامة المواطنين وحريتهم. فالإرهاب الإلكتروني هو أحد الجرائم الأكثر سلبية في استغلال التطور الحاصل في تقنية المعلومات.

أهمية الموضوع:

إن أهمية هذه الدراسة تتجلى أولا في خطورة جريمة الإرهاب الإلكتروني المستحدثة على البني التحتية للأنظمة وتقنية المعلومات والاتصالات، وكذا تحديد طبيعة الاختراقات والهجمات المستمرة في شتى المجالات، وهذا ما يميز هذه الجريمة عن غيرها من الجرائم التقليدية الأخرى، وبطريقة عصرية تتمثل في استخدام تقنية المعلومات وكذا الوسائل الالكترونية في جرائم تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الاختفاء، والقدرة على إخفاء أثارها ومحو كل الأدلة الإثباتية لها.

ليس هذا فحسب بل عبر الحدود لتتصف بالعالمية، ولتتعدد ضحاياها بين الأفراد والدول والكيانات الأخرى، فلما أصبحت تثيره هذه الجريمة من مخاوف وقلق لدى المجتمع الدولي والمحلي بسبب تهديدها وتطورها المستمرين، كما تناولنا هذه الدراسة لإبراز الخصائص التي تميز الإرهاب الإلكتروني من تعقيد وصعوبة اكتشافها وملاحقة مرتكبيها وغيرها.

أما غايتنا من هذه الدراسة ليس فقط إبراز مختلف الجهود الدولية والوطنية لمكافحة جريمة الإرهاب الإلكتروني، بل إثراء هذه الجهود، وإيجاد حلول فعالة أخرى من أجل التعاون الدولي لمجابهة هذه الجريمة.

دوافع اختيار الموضوع:

هناك دوافع شخصية تتمثل في الميول الشخصي لدراسة مثل هذا الموضوع، وهذا بسبب سوء استخدام تقنية المعلومات في ظهور العديد من الجرائم الجديدة، بما في ذلك الإرهاب الإلكتروني الذي يعتبر أحد أخطر وأشنع هذه الجرائم، بالإضافة إلى ذلك، فإن له آثار سلبية على الفرد والمجتمع على حد سواء. لذلك كان لدينا اهتمام شخصي بهذا النوع من الموضوعات المستحدثة، وكيفية تعامل مختلف الدول معها لحماية كيانها السياسي والإقتصادي والإجتماعي وأهمهم الأمني، نظرًا للخطر الذي تشكله على أمن هذه الدول.

حيث يمكن ذكر الدوافع الموضوعية لهذه الدراسة بأنها تهدف إلى تسليط الضوء على أهمية هذا الموضوع بحد ذاته، كما تهدف إلى تقييم فعالية الجهود الإقليمية والدولية في مكافحة هذه الجريمة الخطيرة والمتطورة.

أهداف الدراسة.

تهدف هذه الدراسة إلى استعراض الأحكام الموضوعية والإجرائية المتعلقة بالإرهاب الإلكتروني، نظرًا لكونها جريمة حديثة وخطيرة، وكذلك لفهم الجهود الدولية والإقليمية الرامية لمكافحة هذه الجريمة.

وتهدف هذه الدراسة أيضًا إلى تقييم جدوى الجهود الدولية والإقليمية وكذا تحديد النواحي المختلفة التي تعاني من النقص، ومحاولة إيجاد حلول مناسبة من خلال تقديم بعض التوصيات في هذا الصدد.

إشكالية الدراسة:

لقد تركت جريمة الإرهاب الإلكتروني آثارًا مدمرة على المستوى النفسي والاجتماعي وأيضًا على المستويين الاقتصادي والأمني، فلم يقتصر هذا الخطر على نطاق إقليم الدولة الواحدة فقط، بل تجاوزه ليشمل مختلف الدول، وحتى العالم بأسره، حيث أدى ذلك إلى حالة من الاستنفار في معظم دول العالم، حين سارعت إلى اتخاذ العديد من الآليات والإجراءات على الصعيدين الدولي والوطني.

ومن هنا نطرح الإشكال التالي:

– ما مدى فعالية الآليات الدولية الموجهة لتصدي جريمة الإرهاب الإلكتروني؟ وهل حققت النتائج المرجوة منها؟

المنهج المتبع:

وللإجابة على هذه الإشكالية اعتمدنا المنهج الوصفي، وذلك بوصف ظاهرة الإرهاب الإلكتروني كماهي في الواقع من خلال تبيان المفاهيم المتعلقة بهذه الجريمة، وكذا تحديد خصائصها، كما تم أيضا الاعتماد على المنهج التحليلي لتحليل كل الظواهر المؤدية لهذا الفعل الإجرامي "الإرهاب الإلكتروني".

الدراسات السابقة:

حظي هذا الموضوع بالعديد من الدراسات سواء كانت مؤلفات وكتب والتي نذكر من بينها:

– الإرهاب الالكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة" للمؤلف عادل عبد الصادق الذي تطرق فيه إلى دراسة موضوع الإرهاب الالكتروني دراسة تحليلية ومقارنة مع مختلف القوانين محاولا فيها إبراز أهم مفاهيم الإرهاب الالكتروني وأنواعه وكذلك تحديات العلاقات الدولية وتأثيراتها.

ولا نغفل عن اختيار هذا الموضوع ولو اختلفت العناوين في جعله عنوان بحث الرسائل مذكرات عديدة نذكر منها:

– أطروحة الدكتوراه شعنبي صابرة في "الجهود الدولية في مكافحة الإرهاب الالكتروني دراسة مقارنة " ورسالة الماجستير لـ: نجاري علي فايزة كريم في الآليات القانونية لمكافحة الإرهاب الالكتروني .

وأيضا أدرج هذا الموضوع في عدة ندوات وملتقيات وطنية سجل فيها العديد من الأساتذة مداخلاتهم وأرائهم.

صعوبات الدراسة:

لقد واجهتنا العديد من الصعوبات نذكر منها:

- عدم تمكيننا من التطرق إلى كل الجزئيات المهمة في الموضوع التزاما منا بالشكليات المطلوبة في إعداد المذكرة.
- عدم الحصول على المعلومات والتطبيقات الخاصة بجريمة الإرهاب الالكتروني، نظرا للتداول نفس الموضوع، وكذا طرح متشابه الأفكار.
- قلة وجود النصوص القانونية في جرائم الإرهاب الإلكتروني، خاصة في التشريع الجزائري وهذا ما يدل على وجود فراغ وقصور التشريعي في هذا المجال الحديث.
- قلة المراجع المتخصصة في هذا الموضوع.

وفي ظل هذه الصعوبات حاولنا الإلمام بموضوع جريمة الإرهاب الالكتروني، لإزالة كل الغموض واللبس عنه.

التصريح الجزئي بالخطة:

للإجابة على هذا الإشكال المطروح ارتأينا تقسيم موضوع دراستنا إلى فصلين، حيث سنتناول في الفصل الأول الإحكام القانونية في جريمة الإرهاب الالكتروني، والذي ينقسم إلى مبحثين، حيث تطرقنا في المبحث الأول إلى الإطار المفاهيمي لجريمة الإرهاب الالكتروني أما المبحث الثاني فخصصناه لدراسة الأحكام الإجرائية لجريمة الإرهاب الالكتروني.

أما الفصل الثاني المعنون بآليات مكافحة جرائم الإرهاب الالكتروني، والذي ينقسم بدوره إلى مبحثين، حيث تناولنا في المبحث الأول دور الآليات الإقليمية والدولية في مكافحة جريمة الإرهاب الالكتروني، والمبحث الثاني سنتناول فيه التعاون الدولي في مكافحة جريمة الإرهاب الالكتروني.

الفصل الأول

الاحكام القانونية في جريمة الإرهاب الإلكتروني

تمهيد الفصل الأول:

نظرا لأن جريمة الإرهاب الالكتروني تعتبر من الجرائم المستحدثة، والتي انتشرت في العالم بعد التطور التكنولوجي الخطير، حيث أصبح من السهل بما كان الحصول على حاسب آلي وتزويده بشبكة انترنت، فأمام ضعف تأمين البيئة الرقمية في الدول النامية وخاصة العربية، وقلة التكاليف وجدت الجماعات الإرهابية فرصتها في تنفيذ مخططاتها الإجرامية التخريبية دون تحمل تكاليف باهظة، ودون تعريض أنفسهم للخطر.

وعلى ذلك فإن الهدف من وراء العمليات الإرهابية لم يختلف بل بقي كما هو الاختلاف فقط كان في الوسيلة المستخدمة، حيث تغيرت هذه الوسيلة، وتطورت مع التطور العلمي والتكنولوجي، فمن أجل ذلك سوف نحاول من خلال هذا الفصل التعرف على جريمة الإرهاب الالكتروني، والإحاطة بمختلف جوانبها القانونية من خلال التعرض إلى مفهومها وكذلك أساليب ارتكابها، وذلك من خلال مبحثين، المبحث الأول خصص للإطار المفاهيمي لجريمة الإرهاب الالكتروني، أما المبحث الثاني الأحكام الإجرائية لجريمة الإرهاب الإلكتروني.

المبحث الأول: الإطار المفاهيمي لجريمة الإرهاب الإلكتروني.

لقد كان الإرهاب الالكتروني صورة حديثة ومتقدمة لتطور الإرهاب التقليدي كان لزاما علينا أن نتعرض إلى مفهوم الإرهاب الالكتروني بطريقة أفضل وأسهل وبما أن مفهوم الإرهاب كمصطلح تقليدي أصبح واضحا إلى حد ما فان الإرهاب الالكتروني كمفهوم مستحدث لا يزال يعتريه الغموض وذلك لأنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه، وكذا من حيث دور الفاعل فيه وطبيعة سلوكه.

ومن أجل ذلك ومن كل ما سبق سوف نتطرق إلى **مفهوم وأساليب إركاب جريمة الإرهاب الالكتروني** في مطلب أول، وبعدها سوف نتطرق إلى **أركان وصور جريمة الإرهاب الالكتروني** في مطلب ثاني.

المطلب الأول: مفهوم وأساليب ارتكاب جريمة الإرهاب الإلكتروني.

ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب التقليدي، ولا يختلف الإرهاب الإلكتروني عن الإرهاب العام إلا في نوعية الأداة المستخدمة لتحقيق الغرض الإجرامي، فالإرهاب الإلكتروني يعتمد على استغلال الإمكانيات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

الفرع الأول: تعريف جريمة الإرهاب الإلكتروني وخصائصها

أولا: تعريف الإرهاب الإلكتروني

يتألف مصطلح الإرهاب الإلكتروني أو (Cyber terrorisme) من كلمتين، كلمة مألوفة (Cyber) ومتداولة وتعني الإنترنت، والكلمة الأخرى (Terrorisme) وتعني الإرهاب والتي، حتى الآن لم تعرف تعريفاً محدداً [1].

[1] - يوسف حسن يوسف: لجرائم المعلوماتية، المركز القومي لإصدارات القانونية، ط1، القاهرة، 2011، ص 135.

ونسوق بعض التعاريف التي أعطيت للإرهاب الإلكتروني، والتي تتميز في معظمها بتشابه العناصر التأسيسية المكونة له وبوحدة الأهداف التي يسعى لتحقيقها، وكذا الخلفيات التي تحركه، فالإرهاب الإلكتروني:

يعرفه باري كولينز (Barry Collins) بأنه "سوء الاستخدام القصدي لنظام المعلومات الرقمي والشبكات أو مكوناتها لتحقيق هدف يدعم أو يشمل حملة إرهابية أو فعل إرهابي[1].

ويمكن تعريف الإرهاب الإلكتروني كذلك بأنه النشاط غير القانوني الذي يقوم به طرف ما بوساطة التقنية الإلكترونية الرقمية عبر شبكاتها لتحقيق غرض محدد[2].

ويمكن شرح مفهوم "الإرهاب الإلكتروني" بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، باستخدام الموارد المعلوماتية والوسائل الإلكترونية.

ثانيا: تعريف الإرهاب في المعاهدات والتشريعات الوطنية

جاء في مؤتمر "سوفيا" لتوحيد القانون الجزائي المنعقد عام 1930 عرفه بأنه: الاستعمال العمدي لكل وسيلة قادرة على إحداث خطر جماعي، ويعتبر الرعب عنصرا أساسيا في تكوين هذه الجريمة.

1- الاتفاقية العربية لمكافحة الإرهاب التي أبرمت في أفريل سنة 1998

قد عرفته في مادتها الأولى: 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 ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو تعريض احد الموارد الوطنية للخطر[3]."

[1] – يوسف حسن يوسف: المرجع السابق، ص 136.

[2] –مصطفى محمد موسى: الإرهاب الإلكتروني (دراسة قانونية أمنية نفسية إجتماعية)، دار الكتب والوثائق القومية المصرية، ط1، القاهرة، 2009، ص 05.

[3] – الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 والتي اعتمدها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك بالقاهرة يوم 22/04/1998 ودخلت حيز النفاذ بتاريخ 07/05/1999.

2- معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب أسنة 1999

عرفت الإرهاب في الفقرة الثانية من مادتها الأولى بأنه كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو إغراضه يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو أعراضهم أو حريتهم أو أمنهم أو حقوقهم للخطر، أو إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية أو المرافق الدولية للخطر، أو تهديد الاستقرار أو السلامة الإقليمية أو الوحدة السياسية أو سيادة الدول المستقلة[1].

3- مجمع الفقه الإسلامي:

أعطى تعريفا للإرهاب وذلك في الدورة السادسة عشر لرابطة العالم الإسلامي التي عقدت في مكة المكرمة في21 شوال عام 1423هـ الموافق لـ 2002 م وذلك بقوله: العنوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دمه، عقله، ملـه وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصورة الحرابة، وقطع الطريق وكل فعل من أفعال العنف أو التهديد، يقع تنفيذا المشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أقوالهم للخطر ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو تعريض احد الموارد الوطنية أو الطبيعية للخطر[2].

وتجدر الإشارة أنه منذ 1963 إلى غاية 2005 صدرت ثلاثة عشرة اتفاقية وبروتوكولا كلها متعلقة بالإرهاب دخلت جميعها حيز التنفيذ فيما عدا الاتفاقية التي تم اعتمادها في 13 أفريل 2005 بشان الإرهاب النووي بمقتضى قرار الجمعية العامة للأمم المتحدة رقم 59/290 وتم التوقيع عليها اعتبارا من 2005/09/14[3].

---

[1] – مصطفى محمد موسى، الإرهاب الالكتروني- دراسة قانونية – أمنية – نفسية – اجتماعية، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، مطابع الشرطة، دون مكان نشر، 2009، ص 92.

[2] – محمود عبد العزيز محمد، مرجع سابق، ص 23 ،22.

[3] –علاء الدين راشد، الأمم المتحدة والإرهاب قبل وبعد 11 سبتمبر، دار النهضة العربية، القاهرة، 2005، ص 229.

ثانيا: تعريف الإرهاب الإلكتروني في الاتفاقيات الدولية

من أهم النقاط المثارة للنقاش من خلال التعاريف الواردة في الاتفاقيات هو انعدام اتفاق جامع ومانع لمصطلح للإرهاب يعتمد عليه دوليا.

1- في التشريع الدولي

عرفت اتفاقية جنيف لسنة 1937 لقمع الإرهاب على أن" :الأعمال الإرهابية هي الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف، أو يقصد بها خلق حالة من الرعب في أذهان أشخاص معنيين أو مجموعة من الأشخاص، أو عامة الجمهور [1]."حيث نرى من خلال ما ورد في اتفاقية جنيف لتعريفها للإرهاب استعمالها لعبارات عامة، ولم تحدد بدقة الفعل الإجرامي المشكل للإرهاب.

بينما تعرف الاتفاقية العربية لمكافحة الإرهاب الصادرة من مجلس وزراء الداخلية العرب بالقاهرة في سنة 1997 بأنه كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه وأغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر [2].

ثالثا: خصائص جريمة الإرهاب الإلكتروني

إن تعدد خصائص وسمات الإرهاب الالكتروني يرجع إلى تعدد طرق ووسائل هذا الأخير، حيث تمثلت سمات الإرهاب الالكتروني في:

- ✓ أن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.
- ✓ يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود وعابرة للدول والقارات، وغير خاضعة.

[1] – ولد الصديق ميلود، مكافحة الإرهاب بين مشكلة المفهوم واختلاف المعايير، مركز الكتاب الأكاديمي، ج1، ط1، عمان، 2018، ص ص: 17-18.

[2] – عبد القادر الشيخي، طبيعة الإرهاب الإلكتروني، رابط العرب الإسلامي، ط1، السعودية، 2015، ص 05.

- ✓ يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.
- ✓ صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.
- ✓ صعوبة الإثبات في الإرهاب الإلكتروني، نظرا لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.
- ✓ يتميز الإرهاب الإلكتروني بأنه يجري عادة بتعاون أكثر من شخص على ارتكابه.
- ✓ أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسوب والشبكة المعلوماتية.
- ✓ إن الإرهاب الإلكتروني لا يترك أي دليل مادي يعد ارتكاب جرائمه، وهذا ما يصعب عملية التعقب واكتشاف الجريمة أساسا.
- ✓ سهولة إتلاف الأدلة في حال العثور على أي دليل يمكنه إدانة الجاني[1].

الفرع الثاني: أساليب ووسائل ارتكاب جرائم الإرهابية الالكترونية.

أولا: أساليب ارتكاب جرائم الإرهاب الإلكتروني:

تستخدم جماعات المنظمات الإرهابية المختلفة الشبكة المعلوماتية العالمية في الاتصال والتنسيق فيما بينها نظرا لقلة تكاليف الاتصال وتعتبر فرصة ثمينة في التخفي حيث يمكن وضع رسائل مشفرة تأخذ طابعا لا يلفت الانتباه ومن دون أن يظهر الإرهابي للإفصاح عن هويته، كما أنها لا تترك اثرا واضحا يمكن ان يدل عليها.

ويلجأ الإرهابي الإلكتروني، عن طريق الشبكة العالمية، للأساليب التالية:

1- جمع المعلومات الإرهابية: تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيه، كما أنها تعد موسوعة إلكترونية شاملة متعددة الثقافات ومتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها.

[1] – حسن مظفر الرزو، الفضاء المعلوماتي، بيروت، مركز دراسات الوحدة العربية، 2007 ، ط1، ص 214.

3-إنشاء وتصميم مواقع إلكترونية على الشبكة العنكبوتية: وهذا ما يسر على الإرهابيين إستقطاب ذوي العقول الضعيفة والضمائر المهزوزة لحمل مبادئهم وتوجيهاتهم التخريبية[1].

2-التخطيط والتنيسق للعمليات الإرهابية: تحتاج الأعمال الإرهابية إلى التخطيط المحكم و تنسيق شامل و تعد الشبكة العالمية للمعلومات وسيلة الاتصال بالغة الأهمية للجماعات الإرهابية، حيث تتيح لهم الحرية في التخطيط الدقيق والتنسيق الشامل و شن هجمات إرهابية محددة، بعيد عن أعين الناظرين مما يسهل ترتيب تحركاتهم و توقيت هجماتهم[2].

3-الحصول على التمويل: من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم يتم استدراجهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين.

4-التعبئة و تجنيد الإرهابيين. إن استقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الانترنت مع قضاياهم

5-التدريب على تقنيات الإرهاب الالكتروني تسمح الشبكة العنكبوتية من تدريب الإرهابيين بعيدا عن أعين الأمن[3] وتحتاج العمليات الإرهابية الإلكترونية إلى تدريب خاص

ثانيا: وسائل إرتكاب جرائم الإرهاب الإلكتروني:

يعتمد الإرهاب الإلكتروني على "استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم.

[1] – ميلود عبد الرحمن، الإجراءات الإحترازية الدولية في مواجهة خطر الإرهاب الإلكتروني، التجربة الفرنسية نموذجا، ورقة علمية مقدمة إلى المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية الذي نظمته كلية الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، 2015، ص 140.

[2] – جميل عبد الباقي الصغير، مداخلة بعنوان: مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الانترنت، حلقة علمية موسومة بـ الأنترنت والإرهاب، نظمتها جامعة نايف العربية للعلوم الأمنية بالقاهرة بالتعاون مع جامعة عين شمس، خلال الفترة الممتدة من 15 – 19 نوفمبر 2008، القاهرة، ص 13.

[3] – نايف بن محمد المرواني، المرجع السابق، ص 20.

1- البريد الالكتروني: يعد البريد الالكتروني من أهم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك "من خلال استخدامه في التواصل وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات و المخططين لها، حيث يتم نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المرسلات الإلكترونية."

2- مواقع الإنترنت: "يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية فقد أنشئت مواقع لتعليم صناعة المتفجرات وكيفية اختراق وتدمير المواقع، وكيفية الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات".

المطلب الثاني: أركان وصور جريمة الإرهاب الإلكتروني.

لكل جريمة من الجرائم بنيان قانوني يميزها عن غيرها من الجرائم، أي لها عناصر معينة حددها المشرع للعقاب و إن أنتفا أحداهما لا تكون أركان جريمة الإرهاب الالكتروني قائمة، فهذه الأركان مستمدة كلها من النظرية العامة للتجريم، وأركان الجريمة هي تقوم بتحديدها وترسم حدودها الفاصلة وتميزها عن غيرها من الجرائم.

الفرع الأول: أركان جريمة الإرهاب الإلكتروني

تعرف أركان الجريمة بأنها: "مجموعة الأجزاء التي تشكل منها الجريمة، أو كل الجوانب التي يتشكل منها بنيان الجريمة أو التي يترتب على وجودها في مجموعها وجود الجريمة، ويترتب على انتفائها أو انتفاء أحدها انتقاء الجريمة. [1]

وقد اختلف الفقهاء حول الأركان العامة للجريمة سواء على الصعيد الوطني أو الدولي فعلى المستوى الوطني ظهرت ثلاث جهات فقهية مختلفة حول أركان الجريمة فيرى الاتجاه الأول أن للجريمة ثلاثة أركان عامة، ركن مادي وركن معنوي وركن شرعي وأما الثاني حسب رأي هذا الاتجاه ركن عدم الشرعية، وهو عدم وجود سبب قانوني لإباحة الفعل، وأما

[1] – محمود صالح العادلي، الجريمة الدولية – دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2004، ص 67.

الاتجاه الثاني فإنه يرى أن هناك ثلاث أركان للجريمة، مادي ومعنوي والثالث شرعي، وأما الاتجاه الثالث فهو الذي يرى أن للجريمة ركنين فقط ركن مادي والآخر معنوي، أما عن الركن الشرعي فينفي عنه أنصار هذا الاتجاه كونه ركن من أركان الجريمة، لأنه من ينشئها (النص القانوني هو الذي يجرم الفعل) ومن المستحيل أن يكون خالق الجريمة على حد تعبيرهم – احد العناصر المكونة لها، وقد امتد هذا الخلاف حول الركن الشرعي إلى الصعيد الدولي.

وقد بينت معظم الدراسات السابقة أن الجرائم الإرهابية تتم بصور وأشكال مختلفة فبعضها محلي والبعض الآخر يكون دولي، فجريمة الإرهاب الدولي تتميز ببعدها الدولي عن الجرائم الأخرى، لذلك سوف نحاول من خلال هذا العنصر ان نتعرض الى الركنين المادي والمعنوي للإرهاب الالكتروني من خلال فرعين كما سوف نعرج على الركن الدولي إذا اشتملت هذه الجريمة على عناصر الجريمة الدولية[1].

أولا: الركن الشرعي:

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبنى على ذلك عدم جواز ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم، كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه[2].

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار او المجرم والعقوبة المقررة لارتكابه[3] .

---

[1] – عبد الله علي عبو سلطان، دور القانون الدولي الجنائي في حماية حقوق الإنسان، أطروحة دكتوراه في القانون العام، كلية الحقوق جامعة الموصل العراق، 2003/2004، ص 72.

[2] – سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج الخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012، ص 33.

[3] – القطاونة مصعب، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني، 2010، الأردن، ص 27.

ويتسم هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون ان يفسره تفسيرا ضيقا، بالإضافة الى منع اللجوء الى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل ورد نص بتجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني للتشابه بين الفعلين.

إن ظهور شبكة الانترنت أدى الى تطور ظاهرة الإجرام بشكل خطير في تفشي الجريمة الإكترونية وازداد هذا الوضع خطورة خاصة حين أصدر المجلس الأوروبي.

ثانيا: الركن المادي.

يعبر الركن المادي على الوجه الظاهر للجريمة، وبه يتحقق اعتداء الفاعل على مصلحة يحميها القانون، وبانعدام الركن المادي تنعدم الجريمة ومعها العقوبة، فالركن المادي ينصب على الفعل والسلوك، فالقانون لا يعاقب على الأفكار والنوايا السيئة ما لم تظهر إلى العالم الخارجي، وتكون هذه النية مجسدة في فعل أو عمل.

وجريمة الإرهاب الالكتروني لا يختلف ركنها المادي عن الجرائم العادية، من حيث توافر سلوك[1] يؤدي إلى نتيجة يعاقب عليها القانون، إلا انه في جريمة الإرهاب يكون السلوك دائما ايجابيا ولا يتصور وجود سلوك سلبي يمثل ركنها المادي[2]، ويشترط في هذا السلوك حتى يحقق النتيجة التي يرجوها الإرهابي أن تربطه بهذه النتيجة علاقة تعرف بالعلاقة السببية.

ومن أجل ذلك وفي سبيل معرفة السلوك المادي والنتيجة الضارة لجريمة الإرهاب الالكتروني بشيء من التفصيل قسمنا هذا العنصر إلى عنصرين الأول ويحمل عنوان السلوك الإجرامي والعنصر الثاني النتيجة الضارة.

1- **السلوك الإجرامي:** عرف السلوك الإجرامي على أنه مجموعة الأفعال الجرمية المكونة للجريمة، فلا جريمة دون سلوك إجرامي[3]."

---

[1]- يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الإستراتيجية السليمانية – العراق، 2007، ص 82

[2]- طارق عبد العزيز حمدي، مرجع سابق، ص 71.

[3]- يوسف كوران، نفس المرجع ، ص 83

فالسلوك الإجرامي في الجريمة الإرهابية ستمثل في الفعل، أو مجموعة من الأفعال فليس هناك شرط محدد في صفة هذا الفعل، سواء أكان عنيفا أم فعل قوة أو تهديد أو ترويع، فلا يشترط مثلا حدا من الجسامة، بل إن هناك مجموعة من الأفعال تتحقق بمجرد نشر أفكار منحرفة (كالإشادة بالإرهاب) فالسلوك الإجرامي يمكن أن يكون قولا أو كتابة أو عملا[1].

ومن اجل ذلك يمكن حصر السلوك الإجرامي فيما يلي:

أ- **العنف:** يمكن القول أن العنف هو فعل مادي أو معنوي يؤدي بالمساس بسلامة الإنسان ويعتبر العنف الصورة البارزة للجريمة الإرهابية، بل وإنها أخذت الحيز الأكبر من اهتمام الفقهاء في هذا الشأن.

ب-التهديد: عرف الفقهاء التهديد بأنه إثارة الخوف لدى الغير من ضرر أو شر يصيبه سواء حدث ذلك بالقول أو الكتابة أو الرسم أو الحركة أو الإشارة، وبذلك لا يشترط أن يحدث التهديد بالفعل فقط.

إلا أن المشرع الجزائري يرى خلاف هذا الرأي ويستنتج من خلال نصوصه القانونية المتعلقة بالجريمة الإرهابية أن السلوك الإجرامي في الجريمة الإرهابية يمكن أن يكون ايجابيا، كما يمكن أن يكون سلبيا كالامتناع عن التبليغ على جماعة إرهابية معلومة النشاط أو مكان اختباء إرهابي أو جماعة من الإرهابيين.

أما بالنسبة للركن المادي لجريمة الإرهاب الالكتروني فان ركنها المادي يشترك مع الجريمة المعلوماتية بشكل عام، فهو عبارة عن سلوك يتضمن وجود بيئة رقمية وجهاز كمبيوتر، وتوافر الاتصال بشبكة الانترنت، وبالتالي فإن السلوك الإجرامي في جريمة الإرهاب الالكتروني يتم من خلال جهاز الكمبيوتر وباستخدام المعالجة الآلية للمعلومات[2].

على ذلك وجب أن تتم مباشرة النشاط التقني المؤدي إلى الجريمة، حيث أن ذلك يؤثر على بناء الأدلة، وإلا فلا يمكن القول بإمكانية توافر الأدلة لاحقا، فلا جريمة من هذا القبيل إذا بنيت على مجرد الاعتراف[3].

---

[1] – يوسف كوران، المرجع السابق، ص 83.

[2] – عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت أطروحة دكتوراه في القانون، كلية الحقوق جامعة عين شمس، القاهرة 2003/2004، ص 256.

[3] – عمر محمد أبو بكر بن يونس، نفس المرجع، ص 256.

ومن الصور المتعددة للركن المادي في جريمة الإرهاب الالكتروني

- ✓الاعتداء على نظام المعالجة الآلية
- ✓الاعتداءات على أنظمة المعالجة للمعطيات.
- ✓الدخول أو البقاء في المشروع في نظام المعالجة الآلية للمعطيات.
- ✓الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.

لم ينص المشرع الجزائري على الاعتداء العمدي على سير النظام بنص خاص واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة داخل النظام ويرجع تفسير هذا الموقف للمشرع الجزائري أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه[1].

وبالرجوع إلى نص المادة 323 في فقرتها الثانية من قانون العقوبات الفرنسي نجدها تنص على هذه الصورة وذلك بقولها:" بمجرد إعاقة أو إفساد اشتغال نظام المعالجة الآلية للمعطيات."

– **التعطيل (العرقلة):** فالمشرع لم يشترط الوسيلة التي يتم بها فعل التعطيل، فقد تكون مادية أو معنوية سواء اقترنت بعنف أم لا ككسر الأجهزة المادية للنظام، أو تحطيم الأسطوانة وتكون معنوية إذا وقعت الكيانات المنطقية للنظام مثل البرامج والمعطيات بإتباع تقنيات إدخال برنامج فيروسي.

– **الإفساد:** وهو كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها

– **الأعمال التحضيرية:** تعتبر هذه المرحلة أولى مراحل تنفيذ الجريمة، حيث يعد فيها الجاني العدة لتنفيذ الجريمة دون أن يرتكب أي عمل من أعمال التنفيذ كأن يحضر أجهزة كمبيوتر ويوصله بشبكة المعلومات، أو أن يجمع معلومات حول مواقع معينة مستهدفة من أجل إيجاد طريقة لاختراقها وقد لا يعاقب القانون على الأعمال التحضيرية في الجرائم البسيطة وفي الحالات العادية، إلا في حالة الجرائم الإرهابية والجرائم ضد أمن الدولة فإن الأمر يختلف، ففي هذه الحالة يمكن للقانون أن يجرم هذه الأعمال ويحدد لها عقوبة[2].

[1] – عمر محمد أبو بكر بن يونس، المرجع السابق، ص 190.

[2] – عمار تيسير بجبوج، المرجع السابق، ص 124.

- **النشاط الإجرامي (الجريمة التامة):** بالوصول إلى هذه المرحلة يكون الجاني قد استنفذ كل المراحل السابقة من تفكير، ورغبة وأعمال تحضيرية، وبدء في التنفيذ إلى غاية إتمام الجريمة وتحقيق النتيجة التي يرجوها.

2- النتيجة الجرمية: يعرف الفقه النتيجة الإجرامية بأنها الأثر اللازم للفعل المجرم وتمس إما الأشياء أو الأشخاص وهي إما تعبر عن حقيقة مادية تحدث في العالم الخارجي كأثر للفعل الإجرامي، أو تعبر عن حقيقة قانونية لأنها لا يترتب عليها ضرر، لكنها تمس قيم المجتمع كالجرائم الشكلية، فالجرائم الشكلية ليس لنتيجتها وجود مادي أو ضرر مجتمعي فهذا النوع من الجرائم يعاقب عليها القانون وأن لم تنتج عليها نتيجة ضارة لأنها تمثل مجموعة مصالح يعاقب عليها القانون، أما النتيجة التي يتناولها المشرع كحقيقة قانونية ويطلق عليها النتائج القانونية، والتي تنقسم إلى جرائم الضرر كالقتل والسرقة والإرهاب وجرائم الخطر المحتمل كجرائم الغش التجاري[1].

وتجدر الإشارة أن بعض الفقه قسم نتائج الفعل الإجرامي إلى[2]:

- ✓ **نتيجة قانونية مجردة:** وتكون في الجرائم الشكلية أو ما يعرف بالجرائم غير ذات النتيجة أنها تقصر على حماية قيم مجتمعية ومصالح وحقوق عامة، فهذه الجرائم ليس لها واقع مادي محسوس وملموس سوى حيازة محل الجريمة الذي نص عليه القانون، وعليه فانه لا يمكن حصول النتيجة الإجرامية في هذه الجرائم الشكلية.
- ✓ **نتيجة مادية ملموسة محسوسة:** وهي تلك النتائج التي لها وجود مادي، وهو ما يعرف بالجرائم ذات النتيجة.

فالنتائج الجرمية لابد أن تمس الحقوق والمصالح التي يحميها القانون والتي تتعلق بالأشخاص الطبيعية أو الاعتبارية سواء في أنفسهم أو في ممتلكاتهم، وكذا فيما يتعلق بالأموال العامة سواء كانت مملوكة على الإطلاق للدولة، أو كانت الدولة شريك فيها[3].

---

[1] – محمود عبد العزيز محمد، المرجع السابق، ص 196.

[2] – محمود عبد العزيز محمد، نفس المرجع ، ص 197.

[3] – المادة 119 قانون العقوبات المصري، المادة 87 مكرر من قانون العقوبات الجزائري.

– **العلاقة السببية:** يقصد بالعلاقة السببية بين الفعل المجرم والنتيجة الأصلية الموجودة بينهما، وتقوم هذه الرابطة السببية في جريمة ما عندما تكون النتيجة الواقعة محتملة الوقوع وفقا للسير العادي للأمور[1].

فللعلاقة السببية أهمية بالغة تكمن في كون الركن المادي في كل جريمة لا يكتمل كون وجود هذه العلاقة السببية، فبهذه العلاقة تتقرر المسؤولية الجنائية للجاني بشأن هذه الجريمة المرتكبة.

ثالثا: الركن المعنوي: الركن المعنوي هو العلاقة التي تربط بين مادية الجريمة وشخصية الجاني وجوهر هذه العلاقة هو الإرادة ومن ثم فهي ذات طبيعة نفسية أي أن المسلك الذهني والنفسي هو الأساس في تكوين الركن المعنوي لجريمة الإرهاب الإلكتروني.[2]

فالركن المعنوي للجريمة بشكل عام يمثل الجانب الشخصي أو النفسي للجريمة فلا تقوم الجريمة بمجرد قيام الواقعة المادية ولا تخضع لسبب من أسباب الإباحة بل يجب أن تصدر هذه الواقعة عن إرادة فاعلها وترتبط بها ارتباطا معنويا حيث يمكن ان يقال بأن الفعل هو نتيجة الإرادة الفاعل وبالتالي قيام هذه الرابطة التي تعطي للواقعة وصفها القانوني وتوصف بالجريمة ويصعب تحديد الركن المعنوي لجريمة الإرهاب الإلكتروني في أن الدوافع الذهنية أو النمطية المرتبطة بنفسية المجرم المعلوماتي هي التي ترسم معالم الركن المعنوي. وبالتالي فان الركن المعنوي لهذه الجريمة يقوم بقصد عام وقصد خاص وسوف نتطرق إليه فيما يلي:

1– القصد الجنائي العام: يعبر القصد الجنائي عن إرادة الجاني في مخالفه المسار القانوني على النحو الصحيح الذي رسمه المشرع لم يتم تعريف القصد الجنائي في قانون العقوبات الجزائري صراحة بل تم الإشارة إليه بشكل ضمني في كثير من مواده، وذلك من خلال اشتراط توافر العمد لدى الجاني عند ارتكابه الجريمة وقد ترك المجال للفقه للقيام بتعريف القصد الجنائي فأعطوه تعريفات عديدة يتمحور مضمونها حول نقطتين تتمثلان في اتجاه

[1] – يوسف كوران، المرجع السابق، ص 89.

[2] – إبراهيم بن محمد محمود الزندان، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني : دراسة مقارنة، جامعة فطاني، ط 1، 2018، ص: 35.

إرادة الجاني إلى ارتكاب الجريمة مع ضرورة العلم بكافة أركانها القانونية، وإذا تحقق العلم والإرادة لدى الجاني قام القصد الجنائي وإذا انتفى أحدهما أو كليهما انتفى قصد الجاني[1].

1-1-تعريف القصد الجنائي العام: اكتفى المشرع الجزائري بالإشارة إليه ضمنيا فقط وذلك من خلال إدراج كلمة العمد في كثير من النصوص القانونية الدالة على قصد ونية الجاني التي تنعكس مباشرة على الجريمة التي يرتكبها الجاني وإرادة تحقيق النتيجة.[2]

للقصد الجنائي مرادفات عديدة، حيث يطلق عليه تسمية الخطأ المقصود أو العمدي كذلك تسمية القصد العمدي، وكل هذه المصطلحات لها نفس معنى القصد الجنائي، وهو يُعرف على أنه علم الجاني علما يقينا بالعناصر المكونة للجريمة مع إرادة تامة بتحقيق الواقعة الإجرامية وقبولها[3].

والاجتهاد الفقهي لم يقصر في إعطاء تعريف للقصد الجنائي حيث يدور حول نقطتين أساسيتين، رغم التعريفات المتعددة التي قدمت وتتمثل هذه النقطتين في علم المجرم بعناصر الجريمة وإرادة متجهة بتحقيق هذه العناصر.[4]

1-2-عناصر القصد الجنائي العام: للقصد الجنائي العام عنصرين جوهريين يتمثلان في العلم والإرادة ولابد من توافرهما لقيام القصد الجنائي لدى المجرم لا يمكن الاستغناء عنهما لا على العلم ولا عن الإرادة[5].

1-2-2 العلم: العلم في قانون العقوبات معناه توافر اليقين لدى الجاني بان سلوكه يؤدي إلى نتيجة إجرامية يعاقب عليها قانونا مع علمه بجميع العناصر القانونية للجريمة[6]، فإذا

---

[1] – عبد الله سليمان، شرح قانون العقوبات الجزائري – الجريمة – القسم العام، ديوان المطبوعات الجامعية 2: ط 1 ، الجزائر، 2005، ص 36.

[2] – خلفي عبد الرحمن، القانون الجنائي العام دراسة مقارنة، المرجع السابق، ص 216.

[3] – عبد القادر عدو، قانون العقوبات الجزائري القسم العام الجريمة – نظرية الجزاء الجنائي، دار هومة للطباعة والنشر، د . ط ، الجزائر، 2010، ص 181.

[4]– بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري – أركان الجريمة، أهمية الإثبات الجنائي طرق الإثبات الجنائي، دار الخلدونية للنشر والتوزيع، د.ط، الجزائر، 2007، ص 119 .

[5] – غازي حنون خلف الدراجي، استظهار القصد الجنائي في جريمة القصد العمد، منشورات الحلبي الحقوقية، ط1، لبنان، 2012 ص23.

[6] – بلعليات إبراهيم، المرجع السابق، ص 120.

انتفى العلم بأحد هذه عناصر انتفى القصد الجنائي لأنها هي التي تمد النشاط الإجرامي الوصف القانوني بالتالي تميزها عن باقي الوقائع الإجرامية الأخرى[1]

1-2-3- الإرادة: الإرادة هي العنصر الثاني للقصد الجنائي بعد العلم وهي قوة نفسية توجه كل أو بعض أعضاء الجسم لتحقيق غرض غير مشروع، وبانتقاء الإرادة ينتفي القصد الجنائي[2].

فالإرادة تنصب على السلوك الإجرامي والنتيجة المعاقب عليها فيجب أن تتجه إرادة الجاني إلى تبني السلوك الإجرامي فهي حلقة الوصل بين الجريمة بوصفها واقعة مادية لها كيانها والفاعل الذي صدر عنه السلوك وأراد تحقيق نتيجته[3]، باستخدام الوسائل الإلكترونية والذي يهدف إلى إثارة الرعب والخوف بين الناس وتعريض سلامة المجتمع للخطر، وإلقاء الرعب ما بين الناس وترويعهم، وتعريض حياتهم للخطر.

ونخلص مما سبق بأن القصد الجنائي العام لجريمة الإرهاب الإلكتروني، هو أن يعلم الجاني بعناصر فعله، وبطبيعة الوسيلة التي يستخدمها بتلك الأفعال، ودورها في إحداث الذعر العام والتخويف، وانصراف إرادته إلى إتيان ذلك الفعل مع علمه بما يحدث إلى ذلك.

2-القصد الجنائي الخاص: تشترط جريمة الإرهاب الالكتروني لقيامها قصدا خاصا إضافة للقصد العام السابق الذكر، ويتمثل القصد الخاص في غاية معينة يتطلبها القانون وان يكون الفعل المادي المكون للجريمة قد ارتكب في سبيلها، فإذا كان لكل فعل غاية فإن اعتداد القانون بغاية محددة أن تتجه إليها إرادة الفاعل يجعل منها قصدا ويتميز القصد في جريمة الإرهاب أن له طابع مميز وهام ويعتبر من خاصية هذا النوع من الجرائم ألا وهو الغرض من ارتكابها [4].

---

[1] – عبد القادر عدو، المرجع السابق، ص 182.

[2] – بلعليات إبراهيم، المرجع السابق، ص: 121.

[3] – أمير فرج يوسف مكافحة جريمة الارهاب الالكتروني، المرجع السابق، ص : 165 .

[4] – يوسف مرين، جريمة الإرهاب في القانون الجزائري، مجلة جامعة القدس المفتوحة للأبحاث والدراسات،عدد42-02،2017، ص314.

ويتمثل هذا القصد بنيه إجرامية خاصة تتعلق أساسا بالنتيجة الإجرامية ويتضح مدلوله من خلال الحالات التطبيقية اعتمادا على كل جريمة بسبب مستقل وهي تتطلب عناصر ذاتيه مجدده تتجاوز القصد العام[1].

وعليه فالقصد الخاص في جريمة الإرهاب الالكتروني هو الغاية او الغرض من ارتكاب السلوكيات السالفة الذكر ونص المشرع على الأفعال الإرهابية في نص المادة 87 مكرر من قانون العقوبات الجزائري

الفرع الثاني: صور جريمة الإرهاب الالكتروني.

يرتبط الإرهاب الالكتروني بتقدم التكنولوجيا في كافة مجالات الحياة وفي العالم بأسره، وبذلك اتخذ أبعاد جديدة وازدادت خطورته على المجتمعات الدولية، حيث تتعدد صوره بحكم نشاطه في العالم الافتراضي المتسم بالسرية والتخفي، واختلافه عن الإرهاب التقليدي الأمر الذي يجعل من الصعب اكتشافه ومتابعته وإثباته حيث يتخذ العديد من الصور مثل التهديد والتجسس إضافة إلى بعض الصور الحديثة المواكبة للتطورات الحاصلة في مجال الانترنت كتدمير واختراق المواقع الإلكترونية، وسوف نحاول إبرازها كما يلي:

أولا: الصور التقليدية للإرهاب الالكتروني

ويقصد بالتقليدية اشتراكها مع صور الإرهاب العادي مع بعض التغييرات الطفيفة ومن أهم هذه الصور:

1-التهديد والتجسس الإلكتروني

1-1- التهديد الإلكتروني: يوجد العديد من الأساليب التي تستخدم في التهديد عبر الشبكة العنكبوتية، وتتنوع تلك الأساليب بين تهديدات باغتيال شخصيات سياسية، تهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل[2].

1-2- التجسس الإلكتروني: يعد التجسس من أقدم وأخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب، ولقد تطور عقب الطفرة التي

[1]- بخاري جميل علي، جريمة الإرهاب الدولي ومشروعية نضال حركات التحرر الوطني إقليم كردستان، المركز العربي للنشر والتوزيع، ط 1، مصر، 2020، ص : 355.

[2] - هشام محمد جرائم الإرهاب المعلوماتية، المركز العربي بالإصدارات القانونية، مصر، 2016، ص 127.

حققتها التكنولوجيا والإعلام واستخدام الحواسب الآلية وشبكات الإنترنت، وأصبح الهاجس الأكبر للدول من أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات.

ثانيا: الحروب الإعلامية وغسيل الأموال

1 – الحروب الإعلامية: الفضاء الإلكتروني له تأثير هائل على الرأي العام العالمي لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتى أنحاء العالم بوسائل مختلفة "الصوت الصورة النص، وبالتالي أي جماعة أو منظمة يمكن لها إنشاء مواقع إلكترونية تروج أفكارها وتنشرها في مختلف أنحاء العالم.

2 – غسيل الأموال: لقد أدى استعمال الوسائل التقنية الحديثة في جريمة غسيل الأموال إلى تسهيل إجراء العديد من العمليات المصرفية وتحويل الأموال في دقائق معدودة مما يصعب رصد حركة هذه الأموال كما ساهمت مواقع الانترنت في تبييض وتسهيل حركة الأموال الغير مشروعة.

ثالثا: الصور الحديثة للإرهاب الالكتروني:

والمقصود بها الصور التي صاحبت التطور التكنولوجي في مجال الانترنت وعالم الكمبيوتر ومن أهمها ما يلي:

1-تدمير واختراق المواقع الإلكترونية

1-1- تدمير المواقع الإلكترونية: ويتمثل فيما تتعرض له المجتمعات المعلوماتية الحديثة والدمار الذي قد يلحقه الهجوم الإرهابي بمنظومة المعلومات التي تتحكم في حياة هذه المجتمعات التي تعتمد على الكمبيوتر والانترنت اعتمادا مطلقا والخسائر التي قد تنجم عن مثل المعلوماتية

1-2- اختراق المواقع الإلكترونية: يتم اختراق المواقع الإلكترونية لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل في الموقع تعلن اختراقه وكأنه بمثابة رفع راية النصر[1].

[1] – محمد معمري، الإرهاب في صورة الحديثة، طلا منشاء المعارف، الإسكندرية، مصر، 2017، ص 71.

2-تبادل المعلومات وإدارة العمليات عبر الانترنت:

2-1 - تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية: تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظرا لقلة تكاليف الاتصال باستخدام الانترنت، مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها ، وذلك لهدف تقليل المخاطر الناجمة عن القيام باللقاءات المباشرة بين أعضاء الجماعات الإرهابية على ارض الواقع، أو التخفيف من استخدام الاتصالات التقليدية التي يسهل من خلالها تتبع الإرهابيين وإلقاء القبض عليهم.

3-إدارة العمليات الإرهابية عبر شبكة الانترنت: فالجماعات الإرهابية أصبح لها انتشار كبير على الانترنت، لها آلاف الصفحات والمواقع والتي تستخدمها في استقطاب الشباب من مختلف دول العالم، كما تستخدمها في الترويج لأهدافها وللدعاية الخاصة بها، ومن خلال ما أطلق عليه الحضانات الإلكترونية أو الجماعات الإرهابية الإلكترونية.

المبحث الثاني: الأحكام الإجرائية لجريمة الإرهاب الالكتروني.

إذا كانت التكنولوجيا الحديثة ساهمت بتطور أنماط مستحدثة من الجرائم وعرفت بالجرائم الإلكترونية ، فإنها بدورها أثرت على وسائل إثباتها إذ أصبحت الإجراءات التقليدية غير كافية لاستخلاص الدليل الخاص بطبيعة الإجرام المعلوماتي ، مما جعل المشرع الجزائري يعيد النظر في كثير من المسائل الإجرائية ، وجعلها أكثر ملائمة مع طبيعة التقنية للجريمة المعلوماتية المستحدثة.

المطلب الأول: الإجراءات التقليدية لإثبات جريمة الإرهاب الإلكتروني.

فمن ضمن المقومات التشريعية المعدة لمواجهة جريمة الإرهاب الإلكتروني، اعتراض المراسلات والتسرب (الفرع الأول)، ثم من خلال القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في إجراء المراقبة الإلكترونية وحفظ المعطيات بحركة السير (الفرع الثاني)[1].

[1] – بربوش محمد، أمين محمودي محمد، التسرب ودوره في الكشف عن الجرائم، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، ك ح ع س، جامعة العقيد أكلي محند أولحاج البويرة، 2018 ، ص 11.

الفرع الأول: التسرب واعتراض المراسلات في جريمة الإرهاب الإلكتروني

تعتبر جريمة الإرهاب الإلكتروني من الجرائم المستحدثة التي تحمل الطابع المعلوماتي، والتي يمكن فيها اللجوء إلى إجراء التسرب واعتراض المراسلات إذا اقتضت ضرورة التحري والتحقيق بشأنها.

أولا: التسرب: أورد المشرع الجزائري إجراء التسرب في الباب الثاني من الفصل الخامس تحت عنوان "في التسرب" من المواد 65 مكرر 11 إلى مكرر 18 من ق إج ج والذي سوف نتطرق إلى تبيانه كالأتي:

1-تعريف التسرب: بعد التسرب من إجراءات التحري والتحقيق التي اجتاحتها معظم التشريعات الحديثة لمواجهة الجرائم الإلكترونية، ويعرف التسرب على أنه: "تقنية" من تقنيات التحري والتحقيق الخاصة تسمح لضباط الشرطة القضائية أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضباط شرطة قضائية أخرى مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على انه فاعل أو شريك"[1] والمشرع الجزائري بدوره عرف إجراء التسرب في المادة 65 مكرر 12 ق ا ج ج على أنه: "قيام ضابط أو عون الشرطة القضائية ، تحت مسؤولية ضباط الشرطة المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإهامهم أنه فاعل معهم أو شرك لهم أو خاف."[2]

فمن خلال التعريف الوارد في هذه المادة يتبين أن إجراء التلبس معقد وخطير يتطلب من العون أو الضباط الشرطة القضائية المساهمة المباشرة مع الأشخاص المشتبه فيهم في نشاط الخلية الإجرامية التي يتم التسرب إليها والاشتراك معهم في ارتكاب الأفعال غير المشروعة قصد الحصول على معلومات وتفاصيل تفيد في التحقيق.

ومن الأفعال التي أباحها المشرع الجزائري للضباط الشرطة القضائية القيام بها في سبيل إنجاح عملية التسرب والوصول إلى كشف المجرمين تلك الواردة في نص المادة 65 مكرر 14 ق ا ج ج وهي: "يمكن ضباط الشرطة القضائية المرخص لهم بإجراء عملية

[1]- بربوش محمد وأمين محمودي محمد، المرجع السابق، ص. 12.

[2] - المادة 65 مكرر 12 من الأمر 66-155، السابق ذكره.

التسرب والأشخاص الذين يسخرونهم لهذا الغرض دون أن يكون مسؤولين جزائيا القيام بما يأتي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليه من ارتكاب الجرائم أو المستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي أو التخزين أو الإيواء أو الحفظ أو الاتصال"[1]
- وتنفذ عملية التسرب في جريمة الإرهاب الإلكتروني خاصة يتحقق بدخول ضباط الشرطة القضائية أو العون المكلف إلى العالم الافتراضي عبر مواقع التواصل الاجتماعي ومشاركته في محادثاته عبر غرف الدردشة أو حلقات النقاش المباشرة بأسماء وصفات وهمية مستعارة قصد استدراج الجماعات الإرهابية و أهامهم بأنه عضو منهم للحصول على معلومات حول تقنيات اختراق شبكة الاتصال أو بث الفيروسات وغيرها من التفاصيل التي تفيد إجراء التحقيق[2].

2-**الضمانات المقررة للمتسرب:** لقد أحاط المشرع الجزائري المتسرب بالعديد من الضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضاءها ، منها ما ورد في المادة 65 مكرر 16 ق ا ج ج والتي تضمنت السرية والحرص على عدم إظهار الهوية الحقيقية للقائم بعملية التسرب حيث نصت المادة بأنه : "لا يجوز إظهار الهوية الحقيقية الضباط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراء. [3]"

وما تضمنته كذلك المادة 65 مكرر 17 ق ا ج ج: إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب ، وفي حالة عدم تمديدها يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة (65) مكرر (14) أعلاه للوقت الضروري الكافي لتوقيف عملية المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائريا على أن لا يتجاوز ذلك 4 أشهر.[4] "

---

[1]– المادة 65 مكرر 14 من الأمر رقم 66/155، السابق ذكره.

[2] – براهيمي جمال، المرجع السابق، ص 85.

[3] – المادة 65 مكرر 14 من نفس الأمر رقم 66/155.

[4] – نفس المادة 65 مكرر 16 من نفس الأمر رقم 66/155.

3-القواعد التي تحكم عملية التسرب في جريمة الإرهاب الإلكتروني: نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه ، أحاطه المشرع بجملة من الشروط يتعين مراعاتها عندما تقتضي ضرورة التحري والتحقيق اللجوء إليه.

3-1-القواعد الشكلية العملية التسرب: تتلخص الضوابط الشكلية للتسرب الإلكتروني أساسا في الإذن القضائي ، حيث لا يجوز لضباط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسها دون الحصول على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق حسب نص المادة 65 مكرر 11 [1]، ويجب أن يتضمن هذا الإذن مجموعة من الأحكام وتتلخص في:

- أن يكون مكتوبا وإلا وقع تحت طائلة البطلان.
- ذكر هوية الضابط الذي تتم عملية التسرب تحت مسؤوليته.
- أن يصدر الإذن من الأشخاص المخولين بذلك وهم وكيل الجمهورية وقاضي التحقيق بعد إخطار وكيل الجمهورية في الحالة التي يتم فيها فتح التحقيق حول الجريمة المرتكبة.

تحديد مدة التسرب والتي لا يمكن أن تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحريات القائمة، كما يمكن للجهة التي أمرت بهذا الإجراء إيقافه قبل انقضاء المدة المحددة في الإذن حسب المادة 65 مكرر 115.

3-2-**القواعد الموضوعية لعملية التسرب:** إلى جانب القواعد الشكلية أقر المشرع ضوابط أخرى موضوعية لعملية التسرب ويمكن إيجازها في عنصرين **أساسين هما:**

- الأول يشمل في تحديد نوع الجريمة والتي لا يجب أن تخرج عن الجرائم التي حدها على سبيل الحصر في المادة 65 مكرر 5 ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب[2].
- أما الشرط الموضوعي الثاني يجب أن يكون الإذن مسببا، وهي تلك الأسباب التي دعت إلى تقرير هذه العملية وهو الأساس الذي يبرر اللجوء إلى التسرب إلا يعد باطلا[3].

[1] – المادة 65 مكرر 17، من الأمر رقم 66/155، السابق ذكره.

[2] – المادة 65 مكرر نفس الأمر رقم 66/155.

[3] – براهيمي جمال، المرجع السابق، ص 86.

ثانيا: اعتراض المراسلات:

يمكن المشرع الجزائري ضباط الشرطة القضائية في سبيل التحري والتحقيق اختصاصات خطيرة تمس بالحقوق والحريات الفردية وتتمثل في اعتراض المراسلات ، وهو إجراء استحدثه بموجب القانون رقم 06-22 وخصصه في الفصل الرابع من الباب الثاني تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المواد 65 مكرر 5 إلى 65 مكرر 10 ق ا ج ج.

1-تعريف اعتراض المراسلات:

يعتبر إجراء اعتراض المراسلات من إجراءات التحري المستحدثة والذي يقصد به التتبع السري والمتواصل للمراسلات الخاصة بالمشتبه به ودون علمه، ذلك باعتباره إجراء تحقيقي يباشر خلسة وتنتهك فيه سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل مادي للجريمة والتي تستخدمها في مواجهة الإجرام الخطير و تتم عبر وسائل الاتصال السلكية واللاسلكية[1].

ومن خلال نص المادة 65 مكرر 5 ق إ ج ج نجد أن المشرع الجزائري يقصد باعتراض المراسلات: "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للإنتاج أو التوزيع أو الاستقبال أو العرض[2].

فمن خلال هذه المادة نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض، وهي تلك المراسلات التي تتم بواسطة وسائل الاتصالات السلكية واللاسلكية دون أن يحدد طبيعة هذه المراسلة ، مما يفتح المجال لمختلف الرسائل المكتوبة بغض النظر عن شكلها كتابة رموز أشكال (صور) أو الدعامة التي تنصب عليها ورقية أو رقمية، أو الوسيلة المستعملة لإرسالها سلكية كانت كالفاكس . (تليغرام أو لاسلكية البريد الإلكتروني، الهاتف المحمول)[3]

---

[1] – بوشعرة أمينة، موساوي سهام الإطار القانوني للجريمة الإلكترونية دراسة مقارنة، مذكرة لنيل شهادة الماستر في الحقوق ، تخصص القانون الخاص والعلوم الجنائية، ك ح ع س جامعة عبد الرحمان ميرة 2017 / 2018، ص 79.

[2] – خلفي عبد الرحمان، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس للنشر، الجزائر 2015، ص 101.

[3] – براهيمي جمال، المرجع السابق، ص 89.

ومن أهم المراسلات التي تصلح أن تكون محلا لإجراء الاعتراض في جريمة الإرهاب الإلكتروني التي تمثل مصدرا غنيا لأدلة إثبات، المراسلات التي تتم عبر البريد الالكتروني كونها من أكثر التطبيقات الحديثة استخداما عبر الانترنت فهي تتيح فرصة تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة الإلكترونية بين عدة أشخاص حول العالم ، فهو يتميز بسهولة وسرعة أرسالها واستقبالها.[1]

3- الضوابط التي تحكم اعتراض المراسلات في جريمة الإرهاب الإلكتروني:

يعتبر إجراء اعتراض المراسلات السلكية واللاسلكية[2] من أكثر الإجراءات انتهاكا لحرمة الحياة الخاصة للأفراد واعتداء صريح على سرية المراسلات والاتصالات التي كفلتها الدساتير حماية قانونية، إلا أن جدارة هذا الإجراء في إثبات الجرائم الخطيرة كتلك المتعلقة بجريمة الإرهاب الإلكتروني أعطت أغلب التشريعات صلاحية اللجوء إليه فيما تقتضيه ضرورة البحث والتحقيق، ولتحقيق الموازنة بين ضرورة التحقيق التي تفرضها المصلحة العامة واحترام الحياة الخاصة التي تفرضها المصلحة الفردية، وضع المشرع الجزائري مجموعة من الضوابط التي تحكم هذا الإجراء من المواد 65 مكرر 5 إلى 65 مكرر 10 ق ا ج ج وتتمثل فيما يلي:

- لابد أن تنصب عملية اعتراض المراسلات على الجرائم المحددة على سبيل الحصر في المادة 65 مكرر 5 أهمها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب.
- يجب أن يتم هذا الإجراء بمناسبة جريمة في حالة تلبس أو بمناسبة التحقيق الابتدائي حسب المادة 65 مكرر 5 ق ا ج ج : إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي."[3]

[1] – يقصد اعتراض المراسلات السلكية واللاسلكية: "تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل اتصال وهي عبارة عن بيانات قابلة للإنتاج والتوزيع والاستقبال والعرض يمكن يعرف بأنه: "إجراء خاص يقوم على التدخل الوسيطي لتحويل مسار المراسلات في خط مشترك بوسيلة ممغنطة والقيام بتسجيلها ونسخها "أنظر: بو الطمين الهام، المرجع السابق، ص 67.

[2] – بو الطمين الهام، نفس المرجع، ص 90.

[3] – المادة 65 مكرر5 من الأمر رقم 66/155 يتضمن ق إ ج المعدل والمتمم، السابق ذكره.

- لا يجوز لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد الحصول على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق وهو يعد ضمانة جوهرية لمشروعية هذا الإجراء.
- يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر والبيانات التي تسمح بالعرف على الاتصالات والمراسلات المطلوب اعتراضها، والجريمة التي تبرر اللجوء إليها ومدتها.
- يجب أن يكون الإذن محدد لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق[1].
- أن يتم هذا الإجراء في الحدود المحافظة على السر المهني وعدم المساس به (65 مكرر 6/1 ق ا ج (ج) وإذا اكتشفت جرائم أخرى التي لم يرد ذكرها في الإذن فإن ذلك لا يكون سببا لبطلان الإجراءات المادة 65 مكرر 6 ق ا ج ج)[2].
- تسخير أشخاص مؤهلين مكلفين بممارسات السلكية واللاسلكية وبكل الجوانب التقنية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور (طبقا لنص المادة 65 مكرر 8 ق ا ج ج[3].
- تحرير محضر على كل عملية اعتراض وتسجيل المراسلات بذكر كل التفاصيل والبيانات مع ذكر تاريخ وساعة بداية هذه العمليات والانتهاء منها[4].
- على ضابط الشرطة القضائية المأذون له أو المناب بالعملية التي تفيد إظهار الحقيقة، نسخ ووصف العمليات في المحضر الذي يودعه في الملف، وإذا كانت المكالمات باللغة الأجنبية يستعين بمترجم لترجمتها ونسخها[5].

الفرع الثاني: المراقبة الإلكترونية وحفظ البيانات في جريمة الإرهاب الالكتروني.

إلى جانب الإجراءات الواردة في ق إج ج الخاصة بالتحريات والتحقيقات في الجرائم ذات الطبيعة المعلوماتية استحدث المشرع الجزائري بموجب القانون رقم 0409- وسائل

[1] – أنظر: المادة 65 مكرر 7 من الأمر رقم 66/155، السابق ذكره.
[2] – أنظر: المادة 65 مكرر 6 من نفس الأمر.
[3] – أنظر: المادة 65 مكرر 8 من نفس الأمر.
[4] – أنظر: المادة 65 مكرر 9 من نفس الأمر.
[5] – أنظر: المادة 65 مكرر 10 من نفس الأمر.

وتدابير أخرى تدعم فعالية وسرعة التحريات والتحقيقات الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتتمثل أساسا في إجراء المراقبة الإلكترونية وحفظ المعطيات وهي من أكثر التقنيات تلازما معا لطابع الإجرائي الإلكتروني ولاسيما جريمة الإرهاب الإلكتروني التي يكون محلها الحاسب الآلي المتصل بشبكة الانترنت.

أولا: المراقبة الإلكترونية:

أجاز المشرع الجزائري إجراء المراقبة الإلكترونية تبعا لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية في إطار هذا النوع من الجرائم اللجوء إلى وضع تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها وفقا للأشكال المحددة في ق إج وفي القانون رقم 09-04.[1]

1-**تعريف المراقبة الإلكترونية:** لم يتطرق المشرع الجزائري إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية، غير أن الفقه تولى تعريفه على أنه: "إجراء خاص يتم بإشراف قضائي حسب الحالات، وهي تقنية تستخدم لتسجيل البيانات أو المحادثات لجمع معطيات ومعلومات عن المشتبه فيه"، وهي تمثل فائدة أكيدة لفاعلية المتابعة الجزائية في الجرائم الإلكترونية[2].

وينصب هذا الإجراء على الاتصالات الإلكترونية والتي عرفها المشرع في المادة 2 من القانون رقم 09-04: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية[3]."

فمن خلال هذا التعريف فان الاتصالات الالكترونية تشمل كل الاتصالات السلكية أو اللاسلكية كالفاكس البريد الالكتروني، مواقع الدردشة عبر الانترنت وحتى المنتديات المختلفة وساحات الرأي و النقاش التي تسمح بنقل وتبادل الأفكار والمعلومات.

مجالات اللجوء إلى المراقبة الإلكترونية:

[1] – أنظر: المادة 3 من القانون رقم 09-04 ، السابق ذكره.

[2] – أحمد مسعود مريم اليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، مذكرة مقدمة لنيل شهادة الماجستير، تخصص قانون جنائي، ك ح ع س، جامعة قاصدي مرباح، ورقلة، 2012/2013، ص 81.

[3] – أنظر: المادة 2 من القانون رقم 09-04 السابق ذكره.

حدد المشرع الجزائري في نص المادة 4 من القانون رقم 09-04 السالف الذكر حالات اللجوء إلى إجراء مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر وتتمثل في:

- ✓ الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة
- ✓ في حالة توفير معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- ✓ لمقتضيات التحريات والتحقيق القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- ✓ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1]."

ومن خلال نص المادة 4 أعلاه نجد أن المشرع الجزائري لم يقتصر المراقبة الإلكترونية كإجراء تقتضيه التحريات والتحقيقات القضائية فقط مثلما هو في إجراء اعتراض المراسلات الوارد في ق إج ج ، أنما أعطى تصريحا على استعمال هذا الإجراء التقني في إطار الوقاية من الجرائم الإرهابية والتخريبية أو الجرائم التي تشكل خطرا على أمن الدولة[2].

وقد خول مهمة القيام بهذا الإجراء في إطار المراقبة الوقائية الى الهيئة الوطنية تحت سلطة القاضي المختص حسب المادة 4/2 : عندما يتعلق الأمر بالحالة المنصوص عليها في الفقر "أ" من هذه المادة ... بمنح ضباط الشرطة القضائية المنتمين إلى الهيئة المنصوص عليها في المادة 13 أدناه[3]"

لقد نصت على إنشاء الهيئة المادة 13 من القانون 09-04 تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتحدد تشكيلة الهيئة وتنظيمها وكيفيات تسييرها عن طريق التنظيم[4]."

وباستقراء هذه المواد فإن تشكيلة الهيئة[5] تظم مجموعة من الضباط الشرطة القضائية والتي تسمح لهم هذه الصفة تنفيذ المهام الذي أوكلها المشرع لهذه الهيئة.

---

[1] – المادة 4 من القانون رقم 09-04، السابق ذكره.

[2] – براهيمي جمال، المرجع السابق، ص 92.

[3] – المادة 4 من نفس القانون رقم 09-04.

[4] – المادة 13 نفس القانون رقم 09-04.

[5] – تم تنصيب الهيئة الوطنية بموجب المرسوم الرئاسي رقم 26115 المؤرخ في 8_10_2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حيث حددت المادة 6 من هذا المرسوم تشكيلة الهيئة وتنظيمها أما المادة 4 منه حددت مهام هذه الهيئة والتي تقتصر على مهمتين أساسيين هما: -1 الوقاية من الجرائم المتصلة

2- شروط المراقبة الإلكترونية

نصت المادة 4 من القانون 09-04 على القيود القانونية التي تحكم المراقبة الإلكترونية في حالة ما إذا تعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، أما في الحالات الأخرى فهي تخضع للقواعد العامة ل ق إج وتتمثل هذه الشروط في:

- أن يباشر عملية المراقبة ضباط الشرطة القضائية المنتمين إلى الهيئة المنصوص عليها في المادة 13 من القانون 09-04.
- **الحصول على إذن من الجهات القضائية المختصة:** إن عدم الحصول على إذن مسبق يجعل الإجراء غير مشروع ولا ينتج أثاره القانونية ، فلابد قبل البدء بالقيام في المراقبة الإلكترونية الحصول على إذن مكتوب من النائب العام لدى مجلس القضاء الجزائري عندما يتعلق الأمر بجريمة الإرهاب الإلكتروني كاستثناء للأصل لأن الإذن يمنحه إما وكيل الجمهورية أو قاضي التحقيق حسب الحالة وهذا ما أكدته المادة 4 من القانون 09-04 السالف الذكر التي تنص على :" لا يحوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.
- عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية المنصوص عليها في المادة 13 أدناه ويشترط كذلك أن يكون مدة الإذن 6 أشهر قابلة للتجديد[1].
- **تسبيب إجراء المراقبة الإلكترونية:** ويتمثل في ذلك المبرر القانوني الذي يستدعي اللجوء إلى المراقبة الإلكترونية وهي حالة توفر معلومات عن احتمال اعتداء وشيك يهدد أمن واستقرار الدولة، غير أن احتمال وقوع هذا النوع من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال احتمال ضعيف يصعب تحققه لأن الطابع الإجرامي فيها مجرد من مقدمات مادية ولا تكتشف إلا مصادفة ، فاللجوء إلى هذا الإجراء في كل الحالات يشكل

بتكنولوجيا الإعلام والاتصال 2 مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، أنظر: بن سالم إسمان ، المرجع السابق، ص 69.

[1]- المادة 4: من القانون رقم 09/04 السابق ذكره.

انتهاك على سرية المراسلات والاتصالات الخاصة بالأفراد مما جعل المشرع الجزائري يشدد في الفقرة الأخيرة[1] من نص المادة 4 من القانون رقم 09-04 قد نصت على أن تكون التقنية الموضوعة لمراقبة الاتصالات الإلكترونية في هذه الحالة موجهة حصرا لتجميع وتسجيل معطيات تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير[2]

ثانيا: حفظ المعطيات المتعلقة بحركة السير: بعد إجراء حفظ المعطيات المعلوماتية من الإجراءات الحديثة للبحث والتحقيق عن الجرائم ذات الطبيعة الإلكترونية ومن بينها جريمة الإرهاب الإلكتروني، فقد عمدت التشريعات المقارنة إلى إقرار هذا النظام في سبيل الكشف عن الجرائم وضمان عدم إفلات المجرم من العقاب والمشرع الجزائري بدوره قد نظم هذا الإجراء في المادة 10 من القانون رقم 0409 السالف الذكر في الفصل الرابع تحت عنوان :" التزام مقدمي الخدمات مساعدة السلطات والتي تنص: "في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسهيل المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة..."."[3]

وعليه يعد هذا الإجراء بمثابة سلطة قانونية جديدة في سبيل مكافحة الجرائم الإلكترونية الملائمة مع البيئة الافتراضية التي تقع فيه هذا النوع من الجرائم، ومن بينها جريمة الإرهاب الإلكتروني.

1-تعريف حفظ المعطيات المتعلقة بحركة السير

يقصد بهذا الإجراء: توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، وذلك قصد الاستفادة من المعطيات المحفوظة واستعمالها لأغراض التحقي[4].

وقبل تبيان المعطيات الواجب حفظها والتزامات مقدمي الخدمات لا بد من تحديد تعريف مزودي الخدمات وتعريف المعطيات المتعلقة بحركة السير:

---

[1]- براهيمي جمال، المرجع السابق، ص 92.

[2]- أنظر: المادة 4 من القانون رقم 09-04 ، المرجع السابق.

[3]- المادة 10 من نفس القانون رقم 09-04.

[4]- بوالطمين إلهام، المرجع السابق، ص 70.

1-1-تعريف مزودي الخدمات: قد عرفته المادة 2 من القانون رقم 09-04 السالف الذكر على أنه : أي كيان عام أخاص يقدم لمستعملي خدماته ، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها[1]"

من خلال نص المادة أعلاه نلاحظ أن الاتصالات الإلكترونية التي يجريها الأفراد تمر عبر مقدمي الخدمات قبل أن يستقبلها المرسل إليه.

1-2- تعريف المعطيات المتعلقة بحركة السير: قد بين المشرع الجزائري بموجب المادة 2 فقرة هـ من القانون رقم 0409 السالف الذكر المعطيات التي يجب حفظها من قبل مقدمي خدمات الاتصالات الإلكترونية والتي عبر عنها المشرع الجزائري بمعطيات حركة السير" وهي: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال والوجهة المرسلة إليها والطريق الذي يسلكه ووقت وتاريخ وحجم الاتصال ونوع الخدمة[2]"

وقد حصر المشرع الجزائري المعطيات المتعلق بحركة السير في نص المادة 11 من القانون رقم 09-04 السالف الذكر والتي تنص:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليه.
- بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في هذه الفقرة من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.[3]

[1]- المادة 2 فقرة د من القانون رقم 0409، السابق ذكره.

[2]- المادة 2 فقرة هـ من نفس القانون رقم04/09.

[3]- المادة 11، من نفس القانون رقم 04/09.

4- التزامات مقدمي خدمات الاتصالات الالكترونية:

نظرا لما ينطوي عليه إجراء حفظ المعطيات المتعلقة بحركة السير من مساس بحوق الفرد في الخصوصية والسرية قد ألقى المشرع الجزائري على عاتق مزودي الخدمات أعباء عند قيامهم بالتحفظ على البيانات والمعطيات بحث ضبطها المشرع في قانون 09-04 وتتمثل أساسا في:

2-1- التزام مقدمي الخدمات بمدة محددة للتخلص من المعطيات المتحفظ عليها وذلك صونا للحقوق الشخصية وضع المشرع مدة زمنية لمحو و ازالة المعطيات المخزنة من قبل مقدم الخدمات والتي قدرها المشرع هذه المدة بسنة تحسب من تاريخ التسجيل ، باعتبار أن هذا الإجراء مؤقت يلجأ إليه بأمر من الجهات القضائية المختصة ، وعند انتهاء ميعاد الحفظ المعطيات تمحى لضمان عدم الاطلاع على خصوصية الأطراف تحت طائلة العقوبات الجزائية والإدارية، وعند الإخلال كذلك بسير الحسن للتحقيق يعرض مزود الخدمات العقوبات حسب نص المادة 11 من قانون رقم 09-04 السالف الذكر[1].

التزام مقدم الخدمات بكتمان السر المهني:

يقع على عاتق مزود الخدمات للاتصالات الإلكترونية كذلك إلى وجوب حفظ السر المهني وهم بصدد القيام بالتحفظ على المعطيات الشخصية للأفراد لمقتضيات التحقيق وكذا لتفادي أي طمس وتشويش للأدلة من جهات أخرى تحت طائلة العقاب.

[1]- براهيمي جمال، المرجع السابق، ص 105.

خلاصة الفصل الأول:

تعتبر الجرائم الالكترونية عموما من جرائم القرن و ذلك لارتفاع سب ارتكابها وكثرة أعداد مرتكبيها وأهمية وحساسية أهدافها المتمثلة في إلحاق أضرار بالأشخاص والممتلكات والمساس بالأنظمة المعلوماتية والبنى التحتية الحيوية.

فمما سبق يتبين أن جريمة الإرهاب الالكتروني أصبحت فعلا من أخطر الجرائم التي تهد كيان الدول والمجتمعات على السواء، فعلى الرغم من أن جريمة الإرهاب الالكتروني تتم عن طريق استخدام تقنية المعلومات، كما أن الإجراءات المتبعة في التحري بشأنها وكشفها وملاحقة مرتكبيها هي نفسها الإجراءات المتبعة في إثبات الجرائم المعلوماتية عموما، إلا أن ذا الأمر لا يخرج جريمة الإرهاب الالكتروني أبدا عن طبيعتها كونها جريمة إرهابية ترتكب من أجل تحقيق أغراض وأهداف إرهابية، كما أنها ترتكب بهدف القضاء على أمن واستقرار الدول وزعزعة نظامها السياسي، فالفرق بينها وبين جريمة الإرهاب التقليدي هو أن جريمة الإرهاب الالكتروني تتم بطريقة أكثر دقة واحترافية كما أنها تجنب الإرهابيين التكاليف الباهظة والأخطار الكبيرة لأنها جريمة صعبة الاكتشاف والإثبات ولا تعرف حدود معينة شأنها في ذلك شأن جميع الجرائم المعلوماتية.

كما يمكن أن نستخلص من خلال هذا الفصل أن جريمة الإرهاب الالكتروني من خلال أركانها القانونية تشترك مع الجريمة المعلوماتية في الركن المادي كون الوسيلة المستخدمة في جريمة الإرهاب الالكتروني وسيلة معلوماتية أو الكترونية.

وتشترك مع الجريمة الإرهابية في الركن المعنوي، أي أن القصد الجنائي لمرتكبيها هو تحقيق أعراض إرهابية وتخريبية هذا بالإضافة إلى أن المشرع الجزائري كغيره من معظم مشرعي العالم أدرج جريمة الإرهاب الالكتروني ضمن الجرائم الإرهابية واعتبرها جريمة إرهابية مستحدثة.

الفصل الثاني:

آليات مكافحة جرائم الإرهاب الإلكتروني

تمهيد الفصل الثاني:

مع التقدم الهائل في المجال التكنولوجي وما يشهده هذا العالم من قفزات نوعية في شتى المجالات ما جعل الانترنت تساهم وبشكل كبير في انتشار الجريمة وانتقالها بين الحدود بسرعة كبيرة الأمر الذي يصعب مواجهته نظرا لتداخل القوانين واحتكام كل دولة إلى اختصاصها القانوني، كان لزاما على الدول التكاتف من أجل مكافحة ظاهرة الإرهاب الإلكتروني وذلك بإبرام اتفاقيات ومعاهدات فيما بينها تساعد على مكافحة هذه الظاهرة

تتمثل قوة الإرهاب الإلكتروني في قدرة الإرهابيين الكبيرة على استخدام الانترنت بدرجة عالية من الكفاءة، الأمر الذي أدى بالتشريعات إلى مواكبة التطورات الحديثة وسن قوانين من شأنها مكافحة هذه الظاهرة و حماية الفضاء الإلكتروني من التهديدات الإرهابية في هذا المجال.

وعليه تم تخصيص هذا الفصل للحديث عن الآليات القانونية والأمنية لمكافحة الإرهاب الإلكتروني سواء على الصعيد الدولي أو على الصعيد الوطني من خلال الاتفاقيات الدولية وكذا المنظمات الإقليمية المختصة، وأيضا مدى سعي التشريع الجزائري في مواجهة هذه الظاهرة.

المبحث الأول: دور الآليات الإقليمية و الدولية في مكافحة جريمة الإرهاب الالكتروني

أصبح الإرهاب الإلكتروني أحد أكثر الموضوعات جدلاً على الصعيد الدولي في السنوات الأخيرة بسبب الاختلاف حول تعريف الجرائم الإلكترونية وآليات التعامل معها، فبالرغم من التطور الكبير الذي أحرزه الإرهابيون والمتطرفون في استخدام الإنترنت لنشر الأفكار والمبادئ الإرهابية والدعوة إليها، وتمويل العمليات الإرهابية والتدريب عليها، وتسهيل الاتصالات بين التنظيمات الإرهابية، والاعتداء على الأديان والمعتقدات إلا أن هذا التطور لم يقابله التطور المطلوب في تحديث الأطر المؤسسية والقانونية للاتفاقيات الدولية والإقليمية المتعلقة بمكافحة الإرهاب، ولم يقابله التوسع المأمول في التعاون بين المنظمات الدولية والإقليمية وحكومات الدول من أجل فاعلية أعلى في مواجهة هذا النوع من الإرهاب، الأمر الذي يتطلب تعزيز الإطار القانوني والمؤسسي على جميع المستويات الدولية والإقليمية والمحلية للتغلب على العوامل المؤثرة على جهود تلك المنظمات في مجال مكافحة الإرهاب الإلكتروني.

المطلب الأول: دور المنظمات والاتفاقيات الإقليمية في مكافحة جريمة الإرهاب الإلكتروني.

– الأطر القانونية الدولية والإقليمية لمكافحة الإرهاب الإلكتروني، نظراً لحداثة مفهوم الإرهاب الإلكتروني مقارنة بالمفهوم التقليدي للإرهاب، فقد وضع المجتمع الدولي 19 صكا قانونيا دولًيا لمنع الأعمال الإرهابية التي تمس أمن وسلامة الأشخاص والممتلكات وتعريضها للخطر بما في ذلك أشكال الإرهاب العسكري والنووي والبيولوجي، ووضعت تلك الصكوك تحت رعاية الأمم المتحدة والوكالة الدولية للطاقة الذرية، وهي مفتوحة لمشاركة جميع الدول الأعضاء، في حين كانت الصكوك والمواثيق المتعلقة بتجريم الإرهاب الإلكتروني أقل بكثير، حيث يتمتع العالم في الوقت الحالي بخمس اتفاقيات دولية وإقليمية ملزمة فقط في مجال مكافحة الإرهاب الإلكتروني أو الجرائم الإلكترونية بشكل عام، حيث صادقت أو وقعت 82 دولة حول العالم على واحدة أو أكثر من هذه الاتفاقيات وفقاً لدراسة نشرها مكتب الأمم المتحدة المعني بالمخدرات والجريمة في 2013[1]، وقد ارتفع هذا العدد في الوقت الحالي إلى أكثر من 120 دولة حول العالم.

ويمكن تفصيل هذه الصكوك كما يلي:

[1] - مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، دراسة شاملة عن الجريمة السيبرانية، فيينا، فبراير 2013، ص 133.

– اتفاقية بودابست لمكافحة جرائم الإنترنت كانت اتفاقية بودابست لمكافحة جرائم الإنترنت الموقعة من قبل 30 دولة في العاصمة المجرية بودابست في نوفمبر 2001 أولى الاتفاقيات الدولية المتعلقة بمكافحة جميع الجرائم الإلكترونية بما فيها جرائم الإرهاب.

الفرع الأول: دور الاتفاقيات الاقليمية لمكافحة الإرهاب الإلكتروني.

أولا: اتفاقية بودابست لمكافحة جرائم الإنترنت:

كانت اتفاقية بودابست لمكافحة جرائم الإنترنت الموقعة من قبل 30 دولة في العاصمة المجرية بودابست في نوفمبر 2001 أولى الاتفاقيات الدولية المتعلقة بمكافحة جميع الجرائم الإلكترونية بما فيها جرائم الإرهاب الإلكتروني، ولكن توصيات المجلس الأوروبي الصادرة في سبتمبر 1995 والتي ارتبطت في الأساس بالإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات كانت بمثابة تمهيد لهذه الاتفاقية مثلت اتفاقية بودابست منذ إعلانها الإطار المرجعي للدول في التعامل مع الجرائم الإلكترونية، حيث بلغ عدد الدول الموقعة عليها 68 دولة حتى مايو 2020 ، كما لجأت إليها 153 دولة من الدول الأعضاء في الأمم المتحدة أثناء عملية صنع وإصلاح التشريعات المتعلقة بمكافحة الجرائم الإلكترونية بما فيها الإرهاب والتطرف الإلكتروني.

وقد تناولت هذه الاتفاقية تسعة جرائم فقط كانت تعتبر من أكثر الجرائم شيوعاً على مستوى العالم ارتبط معظمها بالدخول غير المشروع للبيانات والتلاعب بها، والإرهاب الإلكتروني، وتزوير بطاقات الائتمان، واستغلال الأطفال في إنتاج مواد إباحية، كما تطرقت الاتفاقية إلى تحديد الطرق الواجب اتباعها في التحقيق في جرائم الجرائم الإلكترونية. الإنترنت، وركزت على ضرورة التعاون الدولي وتضافر الجهود في مكافح

ثانيا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

تعد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صدرت في ديسمبر 2010 هي الاتفاقية الإقليمية الوحيدة التي تناولت مكافحة الإرهاب الإلكتروني[1] بشكل صريح، حيث تضمنت المادة الخامسة عشر الجرائم الإرهابية المرتكبة بواسطة تكنولوجيا المعلومات، وهي:

– نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

[1] - جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات القاهرة، ديسمبر 2010.

- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

ووقعت 18 دولة على هذه الاتفاقية بهدف تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات ودرء مخاطر هذه الجرائم على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها. وركزت الاتفاقية على تفصيل الجرائم التكنولوجية في 14 مادة من مواد فصلها الثاني مع تخصيص مادة تتعلق بتشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات، إلا أن أبرز ما يميز هذه الاتفاقية عن اتفاقية بودابست أنها خصصت مادة تفصيلية حول الجرائم الإرهابية باستخدام التكنولوجيا بما يمكن الدول الأطراف من تقليل فاعلية عمليات تجنيد الإرهابيين وبث خطاب الكراهية والتطرف عبر المنصات التكنولوجية المختلفة.

الفرع الثاني: دور المنظمات الإقليمية لمكافحة الإرهاب الإلكتروني

أولا: الاتحاد الأوروبي:

شهد التعاون الأوروبي في مكافحة الإرهاب تقدماً ملحوظاً على مدى العقدين الماضيين، الأمر الذي أدى إلى تعزيز قدرة الدول الأعضاء على حماية أمن وسلامة مواطنيها ؛ وقد ساعدت قواعد بيانات الاتحاد الأوروبي في تدعيم التعاون الشرطي والقضائي بين دول الاتحاد والربط بين النقاط الحدودية بشكل يحرم الإرهابيين من السفر لأغراض إرهابية. وفي يوليو 2020 ، توجت جهود التعاون بين دول الاتحاد باعتماد المفوضية الأوروبية استراتيجية جديدة للاتحاد الأمني للاتحاد الأوروبي للفترة من 2020 إلى 2025 تسمح بمنع واكتشاف التهديدات وزيادة مرونة البنية التحتية الحيوية لتعزيز الأمن السيبراني وتعزيز البحث والابتكار[1].

ودخلت الاستراتيجية الجديدة حيز التنفيذ في أبريل 2021، بعد تبني البرلمان الأوروبي حزمة من القيود المشددة التي تفرض إزالة الرسائل والصور ومقاطع الفيديو ذات الطابع الإرهابي خلال ساعة من المنصات الإلكترونية بهدف منع الإرهابيين من استخدام الإنترنت

[1] – المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات استراتيجيات وتشريعات مكافحة الإرهاب داخل الاتحاد الأوروبي، ألمانيا وهولنداء أكتوبر 2021.

للتطرف والتجنيد والتحريض على العنف. كما شجعت المفوضية التوقيع على مدونة الاتحاد الأوروبي لقواعد السلوك بشأن مكافحة خطاب الكراهية عبر الإنترنت في عام 2016، إضافة إلى تقديم مبادرة لتوسيع قائمة الجرائم على مستوى الاتحاد الأوروبي لتشمل جرائم الكراهية[1]

ثانيا: الاتحاد الإفريقي:

على الرغم من اعتماد الاتحاد الإفريقي لاتفاقيته بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي في 2014، إلا أن الاتفاقية لم تدخل حيز التنفيذ إلى الآن بسبب عدم وصول عدد الدول الموقعة عليها للعدد المطلوب، حيث تحتاج الاتفاقية لتوقيع عشر دول إضافية بعد توقيع 19 دولة فقط من أصل 54 دولة؛ وقد يرجع ضعف إقبال الدول الإفريقية على توقيع هذه الاتفاقية إلى عدم الشعور بخطورة الجرائم الإلكترونية في ظل ضعف استخدام الإنترنت في إفريقيا، حيث لم تتجاوز نسبة سكان القارة الأفريقية الذين يستخدمون الإنترنت 28% بنهاية 2019.[2]

ثالثا: جامعة الدول العربية:

اعتمدت جامعة الدول العربية عدداً من الاتفاقيات لمكافحة الإرهاب بشكل عام منذ 1998، والإرهاب الإلكتروني بشكل خاص منذ 2010؛ وبالرغم من اعتماد الاستراتيجية العربية لمكافحة الإرهاب عام 1997، إلا أن التركيز على الإرهاب الإلكتروني بدا جلياً في المراجعة السادسة لها بين عامي 2013-2015، حيث اتفقت الدول العربية على تفعيل دور الرقابة على وسائل الإعلام وعلى شبكة الإنترنت من قبل المكتب العربي للإعلام الأمي، وبذل جهود مكثفة لمنع استغلال مواقع التواصل الاجتماعي من قبل الإرهابيين ومن التشريعات الخاصة بجرائم تقنية المعلومات عند الدول التي لا تمتلك مثل هذا التشريع[3].

---

[1] -European Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, Brussels, December 2020.
Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795&from=EN (14)

[2] – الإنتربول: تقرير للإنتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أي وقت مضى، أغسطس 2020. متاح على:
https://www.interpol.int/ar/1/1/2024/03/12

[3] – ورقة جامعة الدول العربية في الملتقى العلمي أثر الإرهاب على الأمن والسلم العالمي الرباط 14-16 أكتوبر 2014، ص 3.

ولا تقتصر الجهود العربية في مكافحة الإرهاب الإلكتروني على اتفاقية مكافحة جرائم تقنية المعلومات، وإنما امتدت هذه الجهود إلى إنشاء المركز الإقليمي للأمن الإلكتروني للمنطقة العربية الذي أنشئ بموجب الاتفاق مع الاتحاد الدولي للاتصالات في ديسمبر 2012؛ ويتبنى المركز الأجندة العالمية للأمن الإلكتروني التي تنظم التعاملات الإلكترونية وتجرم الاستخدام غير المشروع للتكنولوجيا، وتهدف إلى تدريب وتأهيل وتنمية القدرات وتطويرها في مجال الأمن الإلكتروني[1].

مما سبق، يتضح أن الأمم المتحدة ووكالاتها المتخصصة المختلفة بالإضافة إلى بعض المنظمات الإقليمية ترعى جهود المجتمع الدولي في وضع أطر قانونية وتشريعية ذات صبغة عالمية لمنع الأعمال الإرهابية؛ ولكن إلى الآن لا توجد اتفاقية شاملة للأمم المتحدة بشأن الإرهاب تضم قائمة شاملة لكل أشكال الإرهاب بما فيها الإرهاب الإلكتروني، ولا تخضع الاتفاقيات القائمة الجرائم الإرهابية للقانون الدولي، وإنما تلزم الدول الأطراف في الاتفاقيات بتجريم الفعل المخالف في إطار قانونها الداخلي وتفتح المجال أمام التعاون الدولي بشكل يمكن الدول الأطراف من محاكمة المتهمين أو تسليمهم.

المطلب الثاني: دور المنظمات الدولية والإقليمية وجهودها في مكافحة الإرهاب الإلكتروني

قد يذهب البعض إلى أن التباين الكبير بين الاتفاقيات سالفة الذكر سواء من حيث نشأتها، أو وضعها القانوني أو نطاقها الجغرافي، أو تركيزها الموضوعي، أو الآليات المستخدمة فيها من شأنه أن يؤثر على الجهود الدولية والإقليمية الرامية إلى مواجهة الإرهاب الإلكتروني وتقليل آثاره السلبية على المجتمعات؛ ولكن على مدى خمسة عشر عاماً أو أكثر، بذلت المنظمات الدولية والإقليمية جهوداً حثيثة للتصدي للإرهاب بكافة أشكاله وصوره ولعل أبرز تلك المنظمات التي يمكن أن نركز عليها ما يلي:

الفرع الأول: دور المنظمات الدولية لمكافحة الإرهاب الإلكتروني.

أولا: دور منظمة الأمم المتحدة والهيئات التابعة لها :

يضع ميثاق الأمم المتحدة صون السلم والأمن الدوليين هدفاً رئيسياً للمنظمة الأكبر في العالم، ويلزم الدول باتخاذ التدابير الجماعية المناسبة لمنع كل ما يهدد السلام من جانب

[1] – مجمع البحوث والدراسات بأكاديمية السلطان قابوس العلوم الشرطة الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مسابقة جائزة

وتعزيز حقوق الإنسان والتنمية بكل أبعادها من جانب آخر ؛ ولأن الإرهاب بكل أشكاله التقليدية والإلكترونية يمثل أحد أخطر مهددات السلم والأمن فقد اتخذت الأمم المتحدة والكيانات المرتبطة بها مجموعة من التدابير لمكافحة الإرهاب.

ثانيا: الهيئات المرتبطة بمنظمة الأمم المتحدة.

1- **استراتيجية مكافحة الإرهاب:** تعد هذه الإستراتيجية التي اعتدت بتوافق الآراء في عام 2006 أداة عالمية فريدة لتعزيز الجهود الوطنية والإقليمية والدولية لمكافحة الإرهاب، وقد اتفقت من خلالها جميع الدول الأعضاء في الأمم المتحدة لأول مرة على نهج استراتيجي وتنفيذي مشترك لمكافحة الإرهاب. وترتكز الإستراتيجية على أربعة ركائز أساسية هي: معالجة الظروف المؤدية إلى انتشار الإرهاب؛ وتدابير لمنع الإرهاب ومكافحته؛ وتدابير لبناء قدرة الدول على منع الإرهاب ومكافحته وتعزيز دور منظمة الأمم المتحدة في هذا الشأن؛ واتخاذ تدابير لضمان احترام حقوق الإنسان الواجبة للجميع وسيادة القانون بوصفه الأساس الجوهري لمكافحة الإرهاب[1].

وقد يبدو من ركائز هذه الاستراتيجية أن الإرهاب الإلكتروني قد تم دمجه ضمن المفهوم الواسع للإرهاب دون إشارة صريحة إليه، ولكن المراجعة الدورية للاستراتيجية، والتي تتم كل عامين، أسفرت في نسختها السادسة الصادرة في يونيو 2018 عن إلقاء مزيد من الضوء على قلق الدول الأعضاء إزاء تزايد استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات في ارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها، الأمر الذي دفع مكتب الأمم المتحدة لمكافحة الإرهاب لاتخاذ عدة مبادرات في مجال التكنولوجيات الجديدة من أجل تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع إساءة استعمال الإرهابيين والمتطرفين للتطورات التكنولوجية[2].

2- **مجلس الأمن:** فرض مجلس الأمن مجموعة من التدابير على الدول بهدف التضييق على الإرهاب الإلكتروني بموجب القرار 2161 لسنة 2014 بشأن إنشاء لجان للعمل على الوقاية من التطرف وتقليص أثره على المجتمعات؛ وقد تبع هذا القرار مجموعة من المبادئ

[1] - الجمعية العامة للأمم المتحدة استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب A/RES288/60/، مكتب مكافحة الإرهاب الدورة الستون 2006متاح على:https://undocs.org/ar/A/RES/60/288

[2]- الجمعية العامة للأمم المتحدة: الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب (A/RES) 284/72/، الدورة الثانية والسبعون، مكتب مكافحة الإرهاب، يوليو 2018متاح على:https://undocs.org/ar/A/RES/72/284

التوجيهية التي نصت عليها وثيقة مجلس الأمن رقم 939 لسنة 2015، سميت بمبادئ مدريد التوجيهية لوقف تدفق المقاتلين الإرهابيين الأجانب، وتضمنت مواجهة الإرهاب الإلكتروني في البند السادس والعشرين الذي نص على أن تضطلع الدول الأعضاء ببناء القدرات وتكوين الخبرات في مجالي تكنولوجيا المعلومات والاتصالات وعلم الأدلة الجنائية داخل الأجهزة الوطنية لإنفاذ القوانين وأن تعزز قدرة أجهزة إنفاذ القوانين على رصد محتوى وسائل التواصل الاجتماعي ذي الصلة بالإرهاب من أجل منع تدفق المقاتلين الإرهابيين الأجانب[1] .

3- **الاتحاد الدولي للاتصالات:** وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات وكانت مهمته الرئيسية تتعلق بالاتصالات السلكية واللاسلكية، ويضطلع الاتحاد منذ القمة العالمية لمجتمع المعلومات التي عقدت عام 2010 بدور أساسي يتمثل في بناء الثقة والأمن فيما يتعلق باستعمال تكنولوجيا المعلومات والاتصالات، وقد عُني الاتحاد بالتعاون مع مكتب الأمم المتحدة لمكافحة الإرهاب بوضع سياسات الأمن السيبراني وتحفيز الدول على التعاون من أجل بناء الثقة ورفع درجة الحماية من الإرهاب الإلكتروني، وقد لعب الاتحاد دوراً بارزاً في السنوات الأخيرة في بناء قدرات الدول والمنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني، حيث أطلق برنامج الأمن السيبراني العالمي كإطار للتعاون الدولي لتعزيز الثقة والأمن في مجتمع المعلومات منذ 2007 بالتعاون مع هيئة الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني(IMPACT)"[2].

4-الاتحاد الأوروبي: شهد التعاون الأوروبي في مكافحة الإرهاب تقدماً ملحوظاً على مدى العقدين الماضيين، الأمر الذي أدى إلى تعزيز قدرة الدول الأعضاء على حماية أمن وسلامة مواطنيها؛ وقد ساعدت قواعد بيانات الاتحاد الأوروبي في تدعيم التعاون الشرطي والقضائي بين دول الاتحاد والربط بين النقاط الحدودية بشكل يحرم الإرهابيين من السفر لأغراض إرهابية، وفي يوليو 2020، توجت جهود التعاون بين دول الاتحاد باعتماد المفوضية الأوروبية إستراتيجية جديدة للاتحاد الأمني للاتحاد الأوروبي للفترة من 2020 إلى 2025

[1] - مجلس الأمن مبادئ مدريد التوجيهية لوقف تدفق المقاتلين الإرهابيين الأجانب 939/2024/5، مدريد، ديسمبر 2015. متاح على:https://undocs.org/ar/S/2024/02/03

[2]- لاتحاد الدولي للاتصالات: نشر مقدرات الأمن السيبراني - مركز الإنذار العالمي التابع لهيئةIMPACT ، جنيف، أبريل 2009. متاح على:
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2024-ar.pdf

تسمح بمنع واكتشاف التهديدات وزيادة مرونة البنية التحتية الحيوية لتعزيز الأمن السيبراني وتعزيز البحث والابتكار[1].

الفرع الثاني: دور الاتفاقيات الدولية لمكافحة الإرهاب الإلكتروني

أولا: دور الإتفاقيات

1- اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي

أصدر الاتحاد الإفريقي هذه الاتفاقية في يونيو 2014، وبلغ عدد الدول الموقعة عليها حتى العام الحالي 19 دولة فقط من بين 54 دولة، وقد حاول من خلالها أن يحدد الأهداف والتوجهات الرئيسية لمجتمع المعلومات في إفريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيات المعلومات والاتصالات للدول الأعضاء والمجموعات الاقتصادية الإقليمية، كما تضمنت الاتفاقية قواعد الأمن الضرورية لإنشاء فضاء رقمي موثوق به للمعاملات الإلكترونية وحماية البيانات ذات الطابع الشخصي ومكافحة الجريمة الإلكترونية التي تشكل تهديداً حقيقياً لأمن شبكات المعلومات في إفريقيا. علاوة على ذلك، فقد هدفت الاتفاقية إلى تحديث أدوات قمع الجريمة الإلكترونية من خلال وضع سياسات لاعتماد جرائم جديدة خاصة بتكنولوجيا المعلومات والاتصالات ومواءمة نظام العقوبات الموجود بالفعل في الدول الأعضاء مع مستوى الحداثة الذي تتمتع به بيئة تكنولوجيا المعلومات والاتصالات في الوقت الحالي[2].

بالرغم من أن تركيز الاتفاقية الأكبر كان على تأمين التجارة الإلكترونية بين الدول الأطراف، ولم يرد لفظ الإرهاب أو التطرف الإلكتروني فيها صراحة، إلا أنها تضمنت تعريفاً واضحاً للعنصرية وكراهية الأجانب في تكنولوجيا المعلومات والاتصالات، كما خصصت الفصل الثالث منها لتعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية بجميع أشكالها من

[1] - European Commission: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, Brussels, December 2020.
Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795&from=EN

2African Union: African Union Convention on Cyber Security and Personal Data Protection, Malabo (Equatorial .Guinea), June 2014
:Available at
https://au.int/sites/default/files/treaties/29560-treaty-0048_-

خلال إلزام الدول الأطراف باعتماد تدابير تشريعية لتجريم الأعمال الجنائية المؤثرة على أنظمة تكنولوجيا المعلومات والاتصالات وملاحقة المخالفين.

2- اتفاقية كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية:

وقعت الدول الأعضاء في كومنولث الدول المستقلة هذه الاتفاقية في يونيو 2001 بهدف إنشاء إطار قانوني للتعاون بين هيئات إنفاذ القانون والهيئات القضائية للدول الأعضاء في مكافحة الجرائم المتعلقة بأمن المعلومات الحاسوبية. وتلزم هذه الاتفاقية الدول الموقعة عليها بما يتماشى مع النظام القانوني الوطني والمعاهدات الدولية الأخرى التي يشاركون فيها أن يتعاونوا لتوفير الوقاية الفعالة من الجرائم في مجال المعلومات الحاسوبية وتحديدها وقمعها والكشف عنها والتحقيق فيها، والعمل على التنسيق فيما بينهم لضمان التناسق بين تشريعاتهم الوطنية[1].

وتشابهت هذه الاتفاقية مع اتفاقية بودابست في كونها لم تشتمل على تعريف أو نص صريح بشأن الإرهاب الإلكتروني، ولكنها تضمنت تعريفاً للإرهاب المعلوماتي بأنه استخدام مصادر المعلومات لأغراض إرهابية أو التأثير على المعلومات في الفضاء المعلوماتي لتحقيق أهداف إرهابية.

3- اتفاقية شنغهاي للتعاون في مجال أمن المعلومات الدولي:

تم توقيع هذه الاتفاقية في يونيو 2009 بين الدول الأعضاء في منظمة شنغهاي للتعاون، واعتمدت الاتفاقية في تحديد الإرهاب المعلوماتي على أن مصدر التهديد هو المنظمات الإرهابية والأشخاص المتورطين في الأنشطة الإرهابية وهدفت إلى وضع الأساس القانوني والتنظيمي للتعاون بين الأطراف في مجال أمن المعلومات الدولي، بما في ذلك:

- تنسيق وتنفيذ الإجراءات المشتركة اللازمة في مجال ضمان أمن المعلومات على الصعيد الدولي.
- إنشاء نظام مشترك للمراقبة والاستجابة للتهديدات الناشئة في هذا المجال.

[1]- Commonwealth of Independent States: Agreement on Cooperation in Combating Offences related to Computer Information, Minsk, June 2001.
Available in Russian at:
http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=1180

-وضع تدابير مشتركة لتطوير أحكام القانون الدولي التي تحد من انتشار واستخدام أسلحة المعلومات التي تهدد القدرة الدفاعية والأمن القومي والسلامة العامة[1].

كما حددت الاتفاقية التهديدات الأساسية أمام أمن المعلومات الدولي، وهي تطوير المعلومات واستغلالها كأسلحة في شن حروب معلوماتية، وإرهاب المعلومات والجرائم الإلكترونية، ونشر المعلومات المضللة التي تؤثر على السياقات الاجتماعية والسياسية والاقتصادية للدول الأخرى؛ وهي بذلك أقرب للاتفاقية العربية في تعريف الإرهاب الإلكتروني.

من خلال الاستعراض السابق للاتفاقيات الدولية والإقليمية المرتبطة بالإرهاب الإلكتروني، يتضح أن دول العالم قد انتبهت منذ وقت مبكر لخطر الإرهاب الإلكتروني وأشكاله، واجتمعت المنظمات الدولية والإقليمية على ضرورة مواجهة هذا الخطر بشتى الطرق، وضرورة التوسع في أوجه التعاون الدولي من أجل القضاء عليه، ولكن الاختلاف الملحوظ بين هذه المنظمات يتمثل في عدم اختيار تسمية موحدة لهذه الظاهرة، واستمرار بعضها في الاعتماد على الاتفاقيات التي تركز على ظاهرة الإرهاب بشكله التقليدي دون إفراد مساحة خاصة للإرهاب الإلكتروني.

ثانيا: العوامل المؤثرة على دور المنظمات الدولية والإقليمية في مكافحة الإرهاب الإلكتروني

لم يكن التوافق الدولي حول إطلاق استراتيجية الأمم المتحدة لمكافحة الإرهاب في 2006 كافياً لاعتماد اتفاقية أو استراتيجية مشابهة لمكافحة الإرهاب الإلكتروني، حيث اختلفت السياقات والآليات ومجالات التركيز لكل اتفاقية من الاتفاقيات سالفة الذكر، ولم تتمتع إحداها بالتوافق الدولي الكامل حول بنودها بالرغم من النجاح الجزئي الذي حققته كل اتفاقية منفردة في دفع الدول لوضع وتطوير تشريعات واتخاذ تدابير من شأنها تحجيم الآثار السلبية للإرهاب الإلكتروني، الأمر الذي يؤثر على الجهود الدولية والإقليمية المبذولة في مجال مكافحة الإرهاب الإلكتروني؛ وقد تتمثل بعض العوامل المؤدية لعدم التوافق ذلك فيما يلي:

1- الخصوصية وسيادة الدول:

برغم المرونة التي تتمتع بها اتفاقية بودابست فيما يخص انضمام الدول غير الأوروبية لها، واعتبارها المرجعية الدولية في مكافحة الجرائم الإلكترونية، إلا أن بعض الدول ما تزال

[1]- Shanghai Cooperation Organization: Agreement on Cooperation in the Field of International Information Security between the Member States of the Shanghai Cooperation Organization, Shanghai, June 2009. Available at:
http://eng.sectsco.org/load/207508/

ترفض الانضمام لهذه الاتفاقية حتى وقتنا الحالي؛ ويأتي على رأس قائمة المعارضين لاتفاقية بودابست كل من روسيا والصين والهند، حيث يرون أنها تمنح المحققين القدرة على الوصول إلى البيانات الحاسوبية عبر الحدود وهو أمر ينتهك الخصوصية والسيادة الوطنية للدول، كما أن المادة (32) بـ من الاتفاقية تسمح لأصحاب البيانات بالسيطرة على استخدامها بدلاً من الحكومات، وهو ما يتعارض مع سياسة الدول الثلاث التي ترغب في بسط سيطرة الدولة على البيانات[1].

وقد نجحت روسيا بالفعل بنهاية 2019 في دفع الجمعية العامة للأمم المتحدة لتمرير مشروع قرار يتعلق بضرورة اعتماد اتفاقية جديدة لمكافحة الجرائم الإلكترونية بعنوان مكافحة استخدام تكنولوجيا المعلومات والاتصال لأغراض إجرامية، وقد أقرت الجمعية العامة بالإجماع في مايو 2021 القرار الروسي الهادف للتوصل إلى اتفاقية بحلول عام 2023.

2-المخاوف بشأن حقوق الإنسان:

أبدت العديد من المنظمات الدولية والإقليمية المعنية بحقوق الإنسان قلقها المستمر من القيود التي قد تفرضها الاتفاقيات الدولية والإقليمية والقوانين والتشريعات المحلية المتعلقة بمكافحة الإرهاب على عدد من حقوق الإنسان بما فيها حرية التنقل والتعبير وتكوين الجمعيات والتجمع السلمي، إضافة إلى الحق في الخصوصية والحياة الأسرية؛ وتعد أبرز القوانين المحلية التي واجهت انتقادات واسعة من منظمة العفو الدولية ومكتب الأمم المتحدة لحقوق الإنسان هما: قانون مكافحة الإرهاب في سويسرا، وقانون مكافحة الإرهاب الفرنسي.

علاوة على ذلك، فقد حاربت الولايات المتحدة وعدد من المنظمات غير الحكومية المهتمة بحقوق الإنسان مشروع القرار الروسي بشأن اتفاقية دولية جديدة لمكافحة الجرائم الإلكترونية؛ إذ ترى الولايات المتحدة أن المقترح الروسي ما هو إلا وسيلة للسيطرة على الإنترنت والحد من استخدامه وتقييد حرية التعبير عبر شبكات التواصل الاجتماعي، وهو ما دفعها إلى اقتراح تطوير اتفاقية بودابست الموجودة بالفعل بدلاً من اعتماد اتفاقية جديدة بالكامل.

[1] - مروة نظير :هل المجتمع الدولي بحاجة إلى تشريع جديد بخصوص الجرائم السيبرانية؟، العين الإخبارية، 5 يناير 2023.
متاح على:
https://al-ain.com/article/united-nations-china-russia

3- التأثير السلبي على المهاجرين واللاجئين:

استحدث قرار مجلس الأمن رقم 2178 لسنة 2014 جملة من التدابير لاكتشاف ومنع وتجريم سفر المقاتلين الإرهابيين الأجانب والأنشطة ذات الصلة، وتجريم محاولة السفر للخارج بصفة مقاتل إرهابي أجنبي، حيث فرضت الاتفاقيات الدولية على الدول الأعضاء في الأمم المتحدة منع أي فرد دخول أراضيها، أو عبورها يكون لدى الدولة المعنية معلومات موثوقة تثبت نيته في المشاركة في أفعال إرهابية؛ وقد أدت هذه التدابير إلى زيادة عمليات صد وطرد المهاجرين واللاجئين واستخدام العنف ضدهم على حدود دول الاتحاد الأوروبي وفقاً لما أعلنته المنظمة الدولية للهجرة[1].

عطفاً على ما سبق، لا يمكن اعتبار العوامل الثلاثة سالفة الذكر هي كل ما يؤثر على الجهود الدولية والإقليمية لمكافحة الإرهاب الإلكتروني، ولكن يمكن اختصاص الصراع الدائر بين المعسكرين الأمريكي – الأوروبي من جانب والروسي – الصيني من جانب آخر حول اعتماد اتفاقية دولية شاملة لمكافحة الإرهاب الإلكتروني بأنه العامل الأكثر تأثيراً والسبب الرئيسي وراء عدم التوافق الدولي بشأن توحيد الجهود لتقنين الفضاء الإلكتروني وتحديد ملامح الجرائم الإلكترونية وآليات مكافحة الإرهاب الإلكتروني حتى الآن. إن الأطر القانونية والمؤسسية الحالية قد تكون ملائمة لمكافحة الإرهاب بشكله التقليدي، ولكن خصوصية الدلالة اللفظية للإرهاب الإلكتروني في الاتفاقيات والمواثيق الدولية تفرض بذل المزيد من الجهود لتطوير هذه الأطر أو استحداث أطر جديدة تضفي شكلاً من الفاعلية والحيوية على الجهود الدولية والإقليمية في مكافحة الإرهاب الإلكتروني.

[1] - المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات: المرجع السابق.

المبحث الثاني: التعاون الدولي في مكافحة جريمة الإرهاب الالكتروني

من بين أهم سبل مكافحة جريمة الإرهاب الالكتروني تكاثف الجهود وتحقيق التعاون على المستوى الأمني، ومع تميز هذه الجريمة كونها عابرة للحدود ومرتكبة بتقنية المعلومات فإن مكافحتها لا تتحقق إلا بتعاون دولي على المستوى الإجرائي الجنائي؛ بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وقد تجسد ذلك من خلال إنشاء المنظمة الدولية للشرطة الجنائية تهدف إلى تيسير التعاون الشرطي العابر للحدود ودعم أجهزة الشرطة في العالم وتوفير المعلومات المتعلقة بالجرائم والمجرمين وإيقافهم وتسليمهم .

وعليه وفي هذا الشأن سوف نتناول من خلال هذا المطلب " التعاون الأمني على المستوى الدولي، التعاون الأمني الدولي على المستوى الإقليمي والعربي ممثلا في المنظمة الدولية للشرطة الجنائية" وذلك من خلال فرعين اعتمدناهما تقسيما لهذا الفرع الأول بعنوان " التعاون الأمني الدولي في مكافحة جريمة الإرهاب الالكتروني " وفرع ثاني الثاني بعنوان "التعاون الأمني العربي.[1]

المطلب الأول: التعاون الأمني في مكافحة جريمة الإرهاب الالكتروني

من بين أهم سبل مكافحة جريمة الإرهاب الإلكتروني تكاثف الجهود وتحقيق التعاون على المستوى الأمني ومع تميز هذه الجريمة العابرة للحدود التي ترتكب بتقنيات المعلومات فإن مكافحتها لا تتحقق إلا بالتعاون الدولي على المستوى الإجرائي الجنائي، حيث يسمح بالإتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وقد تجسد ذلك من خلال إنشاء المنظمات الدولية والاقليمية للشرطة الجنائية التي تهدف إلى تسيير التعاون الشرطي في العابر للحدود ودعم أجهزة الشرطة في العالم وتوفير المعلومات المتعلقة بالجرائم والمجرمين وإيقافهم وتسليمهم.

الفرع الأول: التعاون الأمني على المستوى الدولي.

[1]– يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية، ، القاهرة، مصر، ط1، 2011 ، ص: 146

أولا : المنظمة الدولية للشرطة الجنائية الانتربول:

تعد المنظمة الدولية للشرطة الجنائية الانتربول من أقدم صور التعاون الشرطي في مكافحة الجريمة، ففي نهاية سنة 1923 نجح الدكتور "جوهانو سويار" مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية، وذلك في الفترة من 03إلى 07 من شهر سبتمبر عام 1923، ضم مندوبي 19 دولة، وأعلن فيه عنه ولادة اللجنة الدولية للشرطة الجنائية حدد مقرها بفينا، تعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة، والتي أطلق عليها اسم المنظمة الدولية للشرطة الجنائية لانتربول سنة 1956 مقره ا في مدينة ليون الفرنسية[1]، حيث تنقسم شبكة اتصالات الانتربول إلى ثلاثة مستويات هرمية: المكاتب المركزية الوطنية، والمحطات الإقليمية، والمحطة المركزية الموجودة في الأمانة العامة للانتربول.

وتضم المنظمة الدولية للشرطة الجنائية الانتربول حالياً حوالي 195 بلداً عضواً، تستضيف كل دولة مكتبا مركزيا وطني للانتربول، يربط الشرطة الوطنية بشبكة الانتربول العالمية[2].

1- مهام المنظمة الدولية للشرطة الجنائية الانتربول:

للمنظمة الدولية للشرطة الجنائية الانتربول عدة مهام كونها من أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم، فقد وجدت الانتربول لتحقيق عدة أمور منها:

- التعاون الدولي لمواجهة الإجرام الدولي المتزايد باستمرار، تأمين الاتصال الرسمي بين رجال الشرطة في مختلف أرجاء العالم، بغية تبادل الخبرات والأفكار والمناهج وأساليب العمل في مجالات الأمن المختلفة منذ وجدت الدول القومية الوطنية التي تفصل بينها الحدود الجغرافية والصناعية، وارتباط الظاهرة الإجرامية برغبة المجرم للانتقال من مكان إلى آخر، ابتعادا عن مسرح جريمته، واختفائه عن نظر السلطات الأمنية، ولأجل تحقيق أهدافها تقوم الانتربول بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، من مختلف

[1]- أمير فرج يوسف ،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، مكتبة الوفاء القانونية،ط1، الإسكندرية، مصر ،2011 ، ص 427

[2]- المنظمة الدولية للشرطة الجنائية، عرض عام الانتربول 10.30 2024/05/28 https://www.interpol.int/ar/3/10

المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، حيث تقوم المنظمة بعد تجميعها للبيانات والمعلومات بتنظيمها لتكون بها أرشيفا متكاملا يمكن الرجوع إليه عند الحاجة[1].

2- الاختصاصات العامة للمنظمة الانتربول:

بمقتضى ميثاق المنظمة ونظامها الداخلي تتمتع هذه الأخيرة بجملة من الاختصاصات التي تخولها القيام بنشاطات متعددة :

- تجميع وتبادل المعلومات والبيانات المتعلقة بالجريمة والمجرم: حيث تتسلم المنظمة هذه البيانات والمعلومات وتتبادلها مع المكاتب المركزية للشرطة الجنائية في الدول الأعضاء، وتقوم المنظمة بتجميع هذه البيانات وتنظيمها لديها وهذه الوثائق تعتبر وثائق مهمة في مكافحة الجريمة على المستوى الدولي .
- تنسيق الجهود بين الدول الأعضاء خاصة في مسألة هروب المجرمين: حيث تتولى التنسيق مع الدولة العضو من خلال المكاتب المركزية الوطنية التابعة للمنظمة وذلك بتعيين مكان تواجد المجرم والإسراع في اتخاذ إجراءات القبض عليه، وتسليم المجرمين.
- **مكافحة جرائم القانون العام:** مثل جرائم المحذرات و جرائم تبيض الأموال وحتى جرائم الإرهاب، بحيث يمنع على الانتربول التدخل في القضايا ذات الطابع العسكري أو الديني أو العرقي أو السياسي.
- **حماية الأمن الدولي:** وذلك من خلال تحذير الدول من احتمال وقوع جرائم جديدة، إما نظرا لورود معلومات إليها وإما لوجود مجرم خطير في ذلك البلد وبالتالي على سلطات الشرطة في ذلك البلد التحرك واتخاذ لإجراءات الضرورية للقبض عليه[1].

ثانيا: المنظمة الإفريقي الإقليمية للشرطة الجنائية افروبيول:

ترجع فكرة إنشاء آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول " لسنة 2013 بمناسبة انعقاد المؤتمر الإقليمي الإفريقي الـ 22 للإنتربول المنعقد في الفترة الممتدة من 10 إلى 12 سبتمبر بوهران – الجزائر والتي شهدت حضور كافة قادة الشرطة الأفارقة الواحد والأربعين

[1]- شنتير خضرة ،الآليات القانونية لمكافحة الإرهاب الالكتروني-دراسة مقارنة-، أطروحة دكتوراه،القانون الجنائي، كلية الحقوق ،جامعة أحمد د أدرار ،2020-2021، ص 210 .

وبدعوة من الجزائر في شخص السيد اللواء/المدير العام للأمن الوطني عقد المؤتمر الإفريقي للمدراء والمفتشين العامين للشرطة حول الافريبول أيام 10،11 و12 فيفري 2014 والذي تم من خلاله اعتماد إعلان الجزائر بخصوص إنشاء آلية الاتحاد الإفريقي للتعاون ن الشرطي بينما وصفت المادة الثانية من هذا النظام هذه الآلية على أنها مؤسسة تقنية باعتبارها آلية للتعاون الشرطي بين الدول الأعضاء في الاتحاد الإفريقي.

حيث تتخذ هذه الآلية من الجزائر العاصمة مقرا لها بالرجوع لنص المادة 5 من النظام الأساس ي الآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" نجدها قد حددت لنا جملة من المبادئ التي يفترض على هذه الآلية أن تراعيها لدى ممارسة مهامها والمتمثلة في:

- يجب أن تعمل هذه الآلية في إطار احترام سيادة الدول وبهذا فلا يجوز لها بأي شكل من الإشكال أن تتدخل في الشؤون الداخلية لدولة أخرى وقوانينها الوطنية.
- تراعي هذه الآلية لدى ممارسة المهام المنوطة بها احترام أخلاقيات الشرطة.
- يجب على هذه الآلية وهي تباشر مهامها أن تأخذ بعين الاعتبار مبدأ قرينة البراءة.

بالرجوع إلى نص المادة الثالثة من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" نجدها قد سطرت جملة من الأهداف التي ينتظر من هذه الآلية تحقيقها الاعتراف صارحه آلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" بإبرام اتفاقيات مع منظمة الشرطة الجنائية الدولية "أنتربول" وأي منظمات أخرى ذات صلة تعاون، وكذلك إقامة علاقات وتعاون مع المنظمات الحكومية والدولية الممثلة طبعا ف ي إطار سياستها الرامية لمكافحة الجريمة المنظمة العابرة للحدود الوطنية.

ففي هذا الإطار قامت أفريبول بعدة مساعي تصب جلها في إرساء أطر للتعاون مع المنظمات الأخر ى لاسيما من خلال الشروع في أبارم اتفاقات للتعاون مع أجهزة الشرطة الإقليمية والدولية مثل أنتربول وأفريبول. هذه الاتفاقيات هي حاليا قيد الدارسة على مستوى المكتب القانوني الاتحاد الإفريقي تلتزم كل دولة عضو في آلية الافريبول بأن تنشئ وفقا لتشريعاتها الوطنية مكتبا للاتصال الوطني لضمان سلاسة وسير وتنفيذ أنشطة هذه الآلية[1] وقد بلغ عدد هذه المكاتب المنشأة تقريبا أكثر من 30 مكتبا.

[1] https://www.asjp.cerist.dz/en/downArticle/65/11/1/59399 التصفح بتاريخ 2024/04/20 22:00

حيث تجدر الإشارة في هذا الصدد أن المادة 6 من النظام الأساسي المنشئ لآلية الأفريبول قد أناطت باللجنة الفنية المتخصصة للدفاع وال سلامة والأمن" مسؤولية توفير القيادة السياسية والت وجيه فيما يتعلق بشؤون الشرطة في إفريقيا، فضلا عن ذلك أنيط بهذه اللجنة عادة اختصاصات كما سبق الإشارة إليه، ومن أبرزها الوساطة بين الجمع ية العامة وأجهزة صنع السياسة للإتحاد الإفريقي كما يسميها النظام المنشئ لآلية الأفريبول والمساهمة في اعتماد البرنامج السنوي لهذه الأخيرة .

ثالثا: منظمة اليوروبول لمكافحة جريمة الإرهاب الإلكتروني

اليوروبول وكالتين مهمة على المستوى الأوربي في مكافحة الجريمة الخطيرة بصفة عامة، والجريمة الإلكترونية بصفة خاصة، هذه الجريمة التي فرضت نفسها على جميع المستويات الدولية والإقليمية والوطنية.

إن مكتب الشرطة الأوروبية" يوروبول (Europol) "هو وكالة لإنفاذ القانون تابع للاتحاد الأوروبي، يحتل موقعًا مركزيًا ف ي بنية الأم ن الأوروبي، يوظف أفضل محلل ي الجريمة المدربين في أوروبا والذين يستخدمون أدوات فنية متطورة من أجل مساعدة الوكالات الوطنية في تحقيقاتها اليومية.

ولأجل المكافحة الفعالة للجريمة الإلكترونية قام اليوروبول بإنشاء مراكز ووحدات تابعة له، على غرار الفريق العامل المعني بالجريمة الإلكترونية التابع للإتحاد الأوروبي، والذي تم إنشاؤه سنة 2010 بهدف توفير منصة لمديري التحقيقات والملاحقات القضائي ة في مجال الجريمة الإلكترونية، وتطوير وتعزيز نهج منسق داخل الاتحاد الأوروبي لمكافحة الجريمة الإلكترونية، لجعل الفضاء الإلكتروني مكاناً آمن المواطن ي الإتحاد الأوروبي ومؤسساته وحكوماته[1].

ويتألف من رؤساء الوحدات الوطنية لمكافحة الجرائم الإلكترونية لمختلف الدول الأعضاء بالإضافة إلى ممثلين عن المفوضية الأوروبية، وممثلين عن اليوروبول والاوروجيست، كما تم إنشاء المركز الأوربي للجريمة الإلكترونية سنة 2013، والذي قدم مساهمة كبيرة في الجهود

[1] - علي بوعمرة، جريمة الإرهاب الإلكتروني، مذكرة مكملة لنيل شهادة الماستر، تخصص: جريمة وأمن عمومي، جامعة الشهيد الشيخ العربي التبسيي 2020-2021، ص63.

التي تبذلها الدول الأعضاء في الإتحاد الأوربي من أجل حماية المواطنين والشركات والحكومات الأوروبية من هذه الجريمة، هذا المركز الذي ساهم كثيرا في مكافحة الجريمة الإلكترونية من خلال عمليات الدعم العملياتي الفوري، مما سهل في اعتقال المجرمين، إضافة إلى قيامه بتحليل مئات الآلاف من الملفات، والتي في غالبيتها تكون خبيثة أو تحتوي فيروسات إلكترونية، كما يهتم المركز بدارسة التهديدات التي قد يشكلها الإجرام الإلكتروني المنظم وبالأخص الإرهاب الإلكتروني، وكل الجرائم الإلكترونية التي تؤثر على البنية التحتية الحيوية والمعلوماتية للاتحاد الأوروبي، والجرائم الإلكترونية التي تتسبب في أضرار جسيمة لضحاياهم،مثل الاستغلال الجنسي للأطفال عبر الإنترنت[1].

الفرع الثاني: التعاون الأمني على المستوى العربي.

سعت الدول العربية جاهدة وبكل الوسائل المتاحة لها من اجل حد ظاهرة الإرهاب الالكتروني والأخطار التي يخلفها ومن خلال هذا الفرع سنقوم بدراسة بعض الجهود التي قامت بها الدول العربية.

لقد سعت العديد من الدول العربية الأخرى تشريعات وقوانين في إطار تجريم الإرهاب بالوسائل الالكترونية الإرهاب الالكتروني[2]:

أولا: الأجهزة المختصة في مكافحة جريمة الإرهاب الإلكتروني:

1- المملكة العربية السعودية:

تبنت المملكة العربية السعودية مجموعة من المبادرات المختلفة والتي شملت تدابير قضائية ومعايير أخرى استجابة للتطورات الدولية في هذا المجال عن طريق إصدار مؤسسة النقد العربي السعودي قواعد مكافحة غسل الأموال وتمويل الإرهاب فبراير 2012، حيث نصت هذه القواعد في أحدى المواد منها على مكافحة الإرهاب الإلكتروني ومن هذه المواد:

- عند تطبيق أي نظم إلكترونية جديدة لتحويل الأموال والمدفوعات فإنه يجب التأكد من أنها صممت على أن تكون لديها قدرات تسمح بمنع واكتشاف عمليات غسل الأموال وتمويل

[1]- شنتير خضرة، المرجع السابق ص247-248.

[2]- ارئد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية حول: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، ص ص 16-17 .

الإرهاب، فإنه يجب التأكد من أن لا يتم تقديم هذه الخدمات إلا إلى العملاء الذين يملكون حساباً أو علاقة مصرفية أخرى مع البنك أو محل الصرافة [1]

- تشمل العمليات البنكية الإلكترونية تقديم المعلومات والمنتجات والخدمات من خلال وسائل إلكترونية، وتوفر هذه العمليات فرصاً عديدة للبنوك لتقدم مجموعة متنوعة من منتجاتها وخدماتها بطريقة أسرع وأرخص وأكثر راحة.
- الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح
- الامتناع عن إشراك الآخرين في حسابات الاستخدام، أو إطلاعهم على الرقم السري للمستخدم.
- الإلتزام باحت ارم الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليه
- الامتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.
- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دوماً، ويمنع الآخرين من الاستفادة من خدماتها.
- الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للإنترنت والتي تتنافى مع الدين الحنيف والأنظمة.
- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.

وهذا القرار يبين مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطه [2]

2- الجمهورية العربية المصرية:

لقد ظهر في الآونة الأخيرة نوع من الحروب الجديدة التي لا تقتصر على الهجوم المباشر باستخدام القوة العسكرية، وسبب ذلك ظهور الشبكات الإلكترونية التي ساعدت في ظهور ما يسمَّى بالهجمات الإلكترونية التي تستهدف كل المواقع الحيوية بالدولة. وتعد جمهورية مصر العربية واحدة من أكثر الدول الأفريقية التي تكون عرضة لخطر الإرهاب الإلكتروني تعرضت العديد من الدول لسلسلة من الهجمات الإلكترونية بتاريخ 12 مايو

[1]- مؤسسة النقد العربي السعودي، **قواعد مكافحة غسل الأموال وتمويل الإرهاب**، فبراير 2012، المملكة العربية السعودية، ص 47 .

[2]- بوحادة سارة، المرجع السابق، ص:17-20 .

2017، وقد وقع أكثر 45 ألف هجمة إلكترونية لأكثر من 99 دولة، وذلكوفقاً لخبراء في الأمن المعلوماتي جاءت الدولة المصرية بمجموعة من الجهود.

- **الجهود القانونية:** وتنص المادة 31 من الدستور المصري 2014 على "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون
- **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:** تمت الموافقة على انضمام مصر العربية لإتفاقية مكافحة جرائم تقنية المعلومات من قبل رئيس جمهورية مصر العربية[1]

وقد انضمت مصر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات في سبيل تعزيز التعاون بين الدول العربية لمكافحة جريمة الإرهاب الإلكتروني، علاوة على اقتناعها بضرورة "تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات"

- **قانون مكافحة جرائم تقنية المعلوماتوفقاً للقانون المصرى:**

يعد صدور قانون مكافحة تقنية المعلومات بمثابة خطوة مهمة في ضوء القانون المصري، حيث تضمن القانون المصري لأول مرة "تجريم الممارسات الإلكترونية غير المشروعة"

تتمثل أهم الجهود التنفيذية لجمهورية مصر العربية في وضع الإستراتيجية الوطنية للأمن السيبرياني (2017-2021)، والتي تهدف "لإعداد إستراتيجية وسياسات وبرامج وخطط تأمين البني التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة.

- **وزارة الاتصالات والمعلومات:**

تم إنشاء المركز الوطني "للاستعداد لطوارئ الحاسبات والشبكات"عام 2009، من أجل مواجهة خطر الإرهاب الإلكتروني، ويختص المركز بتقديم الدعم للقطاع الحكومي والمالي، من خلال الدعم التقني والميداني وتقديم التقارير الفنية للجهات المختصة.

- **مؤشر الجاهزية للأمن السيبراني:**

تعد مصر واحدة من أكثر الدول الأفريقية عُرضةً لخطر الإرهاب الإلكتروني، وجاءت مصر في الترتيب 23 ما بين 155 دولة في مؤشر الجاهزية للأمن السيبراني، الصادر عن

[1]- قرار رئيس جمهورية مصر العربية رقم 276 لسنة 2014، الجريدة الرسمية، العدد 46، 13 نوفمبر 2014، ص 3.

"الاتحاد الدولي للاتصالات" لعام 2018، ويقيس المؤشر الجهود والاستعدادات التي قامت بها الدولة من خلال خمسة معايير هي: "المعيار القانوني، والمعيار التقني، والمعيار التنظيمي، ومعيار بناء القدرات، ومعيار التعاون.

3- في القانون الأردني:

تصدى المشرع الأردني لتجريم الأفعال الإرهابية الالكترونية المستخدم فيه الحاسوب والانترنت، وذلك من خلال:

- ✓ وجود برمجيات وبرامج مجانية تخفي هويات المس تخدمين وتجعل من الصعب تعقبهم وكشفهم.
- ✓ توافر المعلومات وسهولة الحصول عليها وإمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية والخبرة في استخدامها من مواقع مجانية عديدة على مواقع الشبكة العالمية
- ✓ الشبكة الخفية، التي تشكل مرتعا خصبا للأعمال غير المشروعة بما في ذلك استئجار أشخاص للقيام بعمليات القتل، وتجارة المخ دارت، والاتجار بالأشخاص، واستغلال الأطفال، الأمر الذي يجعل عملية رصد هذه المواقع ومراقبتها مهمة صعبة، بسبب استخدام التشفير لمنع كشف هوية المستخدمين؛
- ✓ بطئ الإجراءات وتبادل المعلومات في قضايا الجرائم السيبرانية التي تقع في عدة دول، لاسيما بالنظر إلى أن الجريمة السيبرانية تتطلب سرعة الإجراءات والمعالجة؛
- ✓ عدم تجاوب بعض منصات التواصل الاجتماعي وعدم تعاوهنا بخصوص تبادل المعلومات مع أجهزة إنفاذ القانون؛

و- الحاجة إلى بناء القدرات من خلال برنامج تدريبية دولية وتبادل الخبرات مع الدول المتقدمة النمو في مسائل الجريمة السيبرانية [1].

ثانيا: التعاون الامني في التشريعات الداخلية

لقد عمدت الجزائر على غرار باقي الدول إلى السعي في بذل كل الجهود لمكافحة الإرهاب بصفة عامة والإرهاب الالكتروني بصفة خاصة حيث كثفت جهودها لتحقيق مساعيها والسعي لمواكبة الدول المتقدمة في هذا المجال حيث بدأت بالجانب التشريع، لما له

[1] - المركز العربي للبحوث والد ارسات: سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذج اً(acrseg.org) 03/29/2024

من دور فعال في إثبات الجريمة الإلكترونية وسن القوانين الردعية التي تجرم الأفعال الماسة بالأنظمة المعلوماتية، وكذا الإجراءات الجزائية إضافة إلى تجنيد كل الهياكل والمصالحة المتخصصة لمواجهة الإرهاب الإلكتروني الذي أصبح خطرا يهدد الأمن السرياني العالمي والوطني.

- الآليات التشريعية الوطنية:

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة للتصدي للإرهاب الإلكتروني، ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام.

- آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات العامة لقد أخص المشرع الجزائري تنظيم الجرائم الإلكترونية بقوانين عامة وخاصة العامة في:

1- الدستور الجزائري:

كفل دستور 1996 الأساسي والحريات الفردية وذلك عن طريق أهم المبادئ الدستورية في مواده:

- المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.
- المادة 44 حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلفين يحميها القانون .
- لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.
- الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة. [1]

2- قانون العقوبات:

استدرك المشرع الجزائري في السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الجريمة الإلكترونية، وذلك لما أصدر القانون 04-15 المتضمن تعديل قانون العقوبات[1]، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وتضمن ثمانية

[1]- القانون رقم 16-01 المؤرخ في 06 مارس2016، **المتضمن التعديل الدستوري**، المؤرخة في 7 مارس 2016، الجريدة الرسمية عدد: 14.

مواد، إذ تعلقت المادة 394 مكرر بمعاقبة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، أما المادة 394 مكرر1 فنصت على معاقبة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزرار أو عدلا بطريق الغش المعطيات التي يتضمنها، ونصت المادة 394 مكرر2 على معاقبة كل من يقون عمدا عن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن تتركب بها الجرائم المنصوص عليها في القسم الأول.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. أما المادة 394 مكرر3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني، الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد. وفي المادة 394 مكرر4 شدد المشرع على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وجاء في المادة 394 مكرر5 أن كل من شارك في مجموعة أو أتفاق تألف بغرض الإعداد جريمة أو أكثر من الجرائم المنصوص عليها، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها. وأوردت المادة 394 مكرر6 على أنه مع الاحتفاظ بحقوق الغير حسن النية، بحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها. أما المادة 394 مكرر7 فنصت على أنه يعاقب الشروع في ارتكاب الجنح المنصوص عليها بالعقوبات المقررة للجنحة[1] ليصدر في 2009 القانون رقم 09-04،

[1]- بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجازئر: الدور والتحديات كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة، 2017، ص: 432.

المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصالات ومكافحتها[1].

3- قانون الإجراءات الجزائية:

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة. [2]

نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية، ونص على التفتيش في المادة 45 الفقرة 7 من نفس القانون [3] المعدلة حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على «اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر5.[4]

4-القانون المدني الجزائري:

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري«كل عمل أيا كان يرتكبه المرء يسبب ضرار للغير يلزم من كان سببا في حدوثه بالتعويض » وقد جاء هذا النص عاما وشاملا لأي اعتدا ء يقع على أي حق من

---

[1] - شعبان لمياء، الجهود الدولية في مكافحة الإتجار بالبشر عبر الأنترنت، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون العام، تخصص، قانون عام، جامعة الشهيد الشيخ العربي التبسي تبسة، 2020/2019، ص52

[2] - فضيلة عاقلي، الجريمة الإلكترونية ولجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية»، طرابلس، بتاريخ 24- 25 مارس 2017، ص: 130.

[3] - مولود ديدان ، قانون الإجراءات الجزائية، الأمر 11- 02، دار بلقيس،الجزائر، ص: 33.

[4] - توات عبد الحكيم، جريمة الإرهاب الإلكتروني، مذكرة مكملة لنيل شهادة الماستر، تخصص: جريمة وأمن عمومي، جامعة الشهيد الشيخ العربي التبسي 2021، 2022، ص23.

الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهما هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض «فالفعل الضار هو أساس المسؤولية » وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الانترنت، وهو عنصر متحول وصعب التحديد في الإجرام التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدى، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة.[1]

5-آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات الخاصة

- ✓ القانون الخاص بحماية حق المؤلف والحقوق المجاورة.
- ✓ قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ✓ قانون البريد والاتصالات السلكية واللاسلكية.
- ✓ قانون التأمينات.

المطلب الثاني: التعاون القضائي في مكافحة جريمة الإرهاب الإلكتروني.

يعتبر التعاون القضائي الدولي اليوم الآلية الرئيسية في المجال الجنائي لمكافحة الجريمة بشكل عام والجريمة المنظمة بشكل خاص، والتي أصبحت من أكثر الجرائم المهددة للمجتمع الدولي كما أن المساعدة القانونية المتبادلة في المسائل الجنائية – القائمة على التعاون والتنسيق المتبادل بين الدول واللذان يعتبران دعامتان أساسيتان للوقاية من خطر الجريمة والتصدي لها في نفس الوقت أضحت اليوم ضرورة في مواجهة فكرة أن الحدود الدولية لا تعترض الجناة بل القضاة.

[1]- حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر ،29 مارس 2017، ص 121- 122.

هذا وتأخذ المساعدة القانونية المتبادلة أشكالا متعددة منها: الإنابة القضائية الدولية وتنفيذ الأحكام الأجنبية واللذان يدخلان ضمن إستراتيجيات مكافحة الجريمة عموما والجريمة المنظمة خصوصا لهذا حرصت الدول على إرساء قواعد التعاون الدولي في المجال الجنائي من خلال هذه الآليات، كما استحدثت ما يسمى بـ "التحقيق الجنائي عن بعد والذي يمثل أهم الآليات المستحدثة للتعاون الدولي".

وفي هذا الشأن خصصنا هذا المطلب لدراسة "التعاون القضائي في جريمة الإرهاب الالكتروني "**والذي بدوره قسمناه إلى فرعين حيث سنتناول في الفرع الأول**" الآليات التقليدية للتعاون القضائي في مكافحة جريمة الإرهاب الالكتروني "في حين سوف تتناول في الفرع الثاني "الآليات المستحدثة للتعاون القضائي في مكافحة جريمة الإرهاب الالكتروني. [1]

الفرع الأول: الآليات التقليدية للتعاون القضائي في مكافحة جريمة الإرهاب الالكتروني.

لا تستطيع الدولة بمفردها أن تتصدى للإجرام مهما بلغت قوتها فوجود أدوات الجريمة ومرتكبوها على أكثر من إقليم وما يترتب عنه من اندثار الأدلة وضياعها يصعب إكمال مسار التحقيق فيها في الدولة الواحدة، وهكذا تتجسد آليات التعاون القضائي في أشكال مختلفة منها تسليم المجرمين والمساعدة القضائية وتنفيذ الأحكام.

وعليه وفي هذا الشأن سوف تتناول من خلال هذا المطلب "الآليات التقليدية للتعاون القضائي في مكافحة جريمة الإرهاب الالكتروني. وذلك من خلال فرعين اعتمدنا هما تقسيما لهذا المطلب الأول بعنوان قواعد الاختصاص القضائي وتسليم المجرمين " والثاني بعنوان " المساعدة القضائية المتبادلة وتنفيذ الإحكام الأجنبية.

أولا: تسليم المجرمين في جريمة الإرهاب الالكتروني:

إستقر فقه القانون الدولي على إعتبار تسليم المجرمين من أبرز صور التعاون القضائي بين الدول وقد تطور هذا النظام بفضل مجهودات الدول والمنظمات الإقليمية والدولية ليكون أكثر فعالية لتحقيق العرض الذي وجد من أجله، وهو محاكمة الأشخاص المطلوبين أو تنفيذ العقوبة المحكوم بها عليهم، وبالتالي بعد التسليم من أهم الإجراءات العملية

[1]– أشرف محمد لاشين، النظرية العامة للجريمة الدولية – دراسة تحليلية تأصيلية ، 2012، ص700.

التي تكفل القبض على المجرمين وعدم السماح لهم بإيجاد ملجأ أمن بعدما ارتكبوا فعلتهم ولاذوا بالقرار إلى دولة أخرى[1].

وعليه وفي هذا الخصم سوف المتناول " تعريف نظام تسليم المجرمين" و" الأساس القانوني التسليم المجرمين والشروط تسليم المجرمين.

أ- تعريف نظام تسليم المجرمين[2].

يعرف تسليم المجرمين بأنه " إجراء تعاون دولي تقوم بمقتضاه دولة تسمى الدولة الطالبة بتسليم شخص متواجد على إقليمها إلى دولة ثانية تسمى بالدولة المطلوب إليها أو جهة قضائية دولية إما بهدف محاكمته عن جريمة إنهم بأنه إرتكبها، وإما لتنفيذ حكم إدانة صدر بحقه من محاكم فله الدولة أو الجهة القضائية الدولية[3].

ويعرف أيضا بأنه: " الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني حيث تتسلم دولة ما من دولة أخرى شخصا منهما أو مرتكبا لمخالفة جنائية ضد القوانين الخاصة الدولة طالبة التسليم، أو مخالفة للقانون الجنائي الدولي حيث يعاقب على ذلك في الدولة الطالبة[4].

حيث يكفل نظام تسليم المجرمين محاكمة الشخص أمام قاضيه الطبيعي وهو قاضي المكان الذي ارتكب فيه جريمته، وبذلك يؤتي العقاب شماره هذا من ناحية، ومن ناحية أخرى لسهولة جمع أدلة الإثبات وسؤال الشهود في المكان الذي وقعت فيه الجريمة[5].

---

[1]- عمار تيسير بحبوح، التعاون الدولي في مكافحة جرائم الإرهاب، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة القاهرة 2010، ص 296.

[2]- بعد إصطلاح تسليم المجرمين Extradition ذا أصل لاتيني، حيث كان يعبر عن إعادة "Return " الشخص المطلوب تسليمه إلى الدولة ذات السيادة والمختصة لمحاكمته، وقد إستخدم إصطلاح " Extradition" لأول مرة رسميا في المرسوم الفرنسي الصادر 1728 حيث كان يستخدم قبل ذلك إصطلاح " إعادة " Restitution أو " رد Remettion " ولسهر بعد ذلك إصطلاح تسليم Extradition في مجال العلاقات الدولية عند إجراء تسليم المجرمين، أنظر عمار تيسير بجيوج، المرجع نفسه ص 297 .

[3]- سليمان عبد المنعم، الجوانب الإنتقالية في النظام القانوني لتسليم المنجومين دراسة مقاربة، دار الجامعة الجديدة الاستقدرية 2007 ص 32 و 33 .

[4]- زياد محمد جفال، تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي، مقال منشور في مجلة الشارقة للعلوم القانونية، المجلد 16 العدد الأول، 2019 ، ص 513 .

[5]- زياد محمد جمال، المرجع السابق، ص 513.

ب-الأساس القانوني للتسليم المجرمين:

إن مصادر نظام تسليم المجرمين ليست واحدة في كافة التشريعات وإنما تختلف باختلاف الظروف التشريعية لكل دولة، ويمكن ردها إلى ثلاث مصادر أهمها:

الإتفاقيات المبرمة بين الدول والتي قد تكون إتفاقيات ثنائية تتم بين دولتين وفقا للشروط والضوابط المنصوص عنها من طرف الدولتين أو الإتفاقيات المتعددة أو إتفاقيات دولية فتتضمن أحكاما متصلة بتسليم المجرمين من دون أن تكون بحد ذاتها إتفاقيات تسليم[1]، ونظرا لأهمية توحيد أحكام التعاون الدولي في مجال تسليم المجرمين قامت منظمة الأمم المتحدة بوضع اتفاقيات نموذجية تتعلق بهذا الاجراء تصلح أن يسترشد بها في إتفاقيات أو ترتيبات نهائية أو متعددة الأطراف.

كما بعد التشريع الوطني مصدرا العديد من أحكام التسليم، نلجأ إليه الدول التنظيم إجراءات تعليم المجرمين في حالة عدم وجود إتفاقية ترتبط بها هذه الدولة، وقد أثرت العديد من الدول من قوادين وطنية خاصة بتسليم المجرمين[2]، دون الإكتفاء بما قد ترتبط به من إتفاقيات دولية في هذا الخصوص وتكمن أهمية هذه التشريعات في إعتماد الدولة عليها في حالة خلو الاتفاقيات الدولية إن وجدت من حكم ما حيث يتيسر هذا تطبيق الحكم المنصوص عليه في التشريع الوطني.

[1]- تعد الاتفاقيات الدولية المصدر الأساسي لإنشاء القواعد القانونية الدولية وهي تحتل مكانة قانونية هامة في مجال تسليم المحرمين لكونها تعبر عن التزام الدولة بما ورد فيها من نصوص وتتيح الفرصة للدولة المطالبة لإيجاد منقط فرمي يمكن لها أن شهد عليه في طلب التسليم، عادل محمد السيوي، التعاون الدولي في مكافحة جريمتي عسل الأموال وتمويل الإرهاب، طبعة أولى شركة بيضة مصر للطباعة والنشر والتوزيع، القاهرة ،2008، ص 178.

[2]- من أبرز الإتفاقيات التي يعتمدها مؤصر الأمم المتحدة الكلمن لمنع الجريمة ومعاملة المجرمين في - هافانا من 27 إلى 7 سيغير 1990 - المعاهدة النموذجية بشأن تبادل المساعدة في المسائل الجالية والمعاهدة النموذجية يمان نقل الإجراءات، وأمنها الإضافية النموذجية لتسليم المجرمين والتي تعد نمونجا لعقد عليه الدول في ترديداتها التعاقدية وقد نحت في ختام المؤثر على أن " تستدعين الدول الأعضاء في عمليات التسليم بمعاهدات الأمم المتحدة النموذجية المتعلقة بمسائل جنائية .

ج شروط تسليم المجرمين:

توجد شروط عديدة ينبغي توافرها لإجراء تسليم شخص معين إلى الدولة التي تطلبه ويتعلق الأولى بثبوت الاختصاص التشريعي للدولة طالبة التسليم وانتقاء هذا الاختصاص بالنسبة للدولة المطلوب منها التسليم الجريمة سبب التسليم و الشخص المطلوب تسليمه[1].

ثانيا: المساعدة القضائية المتبادلة وتنفيذ الأحكام الأجنبية:

يشكل موضوع المساعدة القانونية المتبادلة محور اهتمام العديد من الاتفاقيات الدولية ذات الصلة بالجرائم العابرة للحدود لاسيما المرتكبة بواسطة تقنية المعلومات والتي تضمنت نصوصا تحدي بضرورة اللجوء إلى المساعدة القضائية المتبادلة بين الدول المتعاقدة من أجل تحقيق الفعالية والسرعة في إجراءات معاقبة وملاحقة مرتكبي الجرائم، وهذه الاتفاقيات منها ما كان خاصا بالجريمة المرتكبة بتقنية المعلومات ومنها كان موضوعه الجريمة العابرة للحدود

في خضم بحثا في ما يخص الآليات التقليدية للتعاون القضائي في جريمة الإرهاب الالكتروني عبر الأنترنت وبعد أن تعرضنا للإختصاص القضائي وتسليم المجرمين في جريمة في مكافحة جريمة الإرهاب الالكتروني في الفرع الأول من هذا المطلب تتعرض في هذا الفرع ببيان"المساعدة القضائية المتبادلة وتنفيذ الأحكام الأجنبية في جريمة الإرهاب الالكتروني" والذي هو عنوان فرعنا الثاني في هذا المطلب، حيث سنتناول" المساعدة القضائية المتبادلة " أولا وتنفيذ الأحكام الجنائية الأجنبية ثانيا.

1- المساعدة القضائية المتبادلة:

تعتبر المساعدة القضائية المتبادلة إحدى وسائل التعاون القضائي الدولي الحديث نسبيا، فقد تكونت بشكل رئيسي منذ الستينيات وإن كانت أصولها ترجع إلى ممارسة قديمة قد كانت تستخدم في القرن الماضي، حيث كانت تسمى بخطابات طلب الحصول على المعلومات وكانت تعني طلب محكمة في دولة ما من محاكم دول أخرى المساعدة القضائية في شكل الحصول على شهادة أو توفير أدلة مادية، وحيث تقوم المحاكم بإرسال الدليل الشفهي أو المادي إلى المحكمة التي تقدمت بالطلب مؤكدة أنه تم الوصول إلى الدليل بوجوب

[1]- نظم المشرع الجزائري موضوع تسليم المجرمين في قانون الإجراءات الجزائية من خلال الفصل الأول في " شروط تسليم المحرمين " من الباب الأول بعنوان " في تسليم المجرمين " من الكتاب السابع " في العلاقات بين السلطات القضائية الأجنبية " بموجب نص المادة (694) إلى المادة (720) من قانون الإجراءات الجزائية الجزائري

الطلبات القانونية للدولة التي طلب منها تقديم المساعدة القضائية وتهدف المساعدة القضائية المتبادلة في المسائل الجنائية بإعتبارها إحدى الآليات الفعالة لمواجهة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة بالتوفيق بين حق الدولة في ممارسة إختصاصها الجنائي داخل حدودها الإقليمية وحقها في توقع العقاب[1].

أ – تعريف المساعدة القضائية المتبادلة:

ذهب جانب من الفقه إلى أن المساعدة القضائية هي كل إجراء قضائي من شأنه مهمة تسهيل ممارسة الإختصاص القضائي في دولة أخرى بصدد جريمة من الجرائم[2] "

وتعرف المساعدة القضائية أيضا بأنها " كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[3].

وتعد إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية – باليرمو 2000 – من أولى الإتفاقيات الدولية التي أدرجت المساعدة القضائية ضمن نصوصها[4]، وهو ما كرسته أيضا المادة (32) من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة (25) من إتفاقية بودابست عندما ألزمت الدول بتبادل المساعدة فيما بينها إلى أقصى حد ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم تقنية المعلومات وجمع الأدلة الإلكترونية في الجرائم

---

[1] --Cherif Bassiouni " the modalities of international cooperation in penal matters in international criminal law 3rd Edition Martinus Nijhoff Publishers 2008 Vol 2 page 3.

[2]– أشرف محمد لاشين، المرجع السابق، ص 711 .

[3]– جميل عبد الباقي الصغير، المرجع السابق، ص 79.

[4]–نصت المادة (15) من إضافية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية – باليرمو 2000 على ما يلي " تقدم الدول الأطراف بعضها البعض أكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية فيما يتصل بالجرائم المضمونة بهذه الإضافية، حسبما قص عليه المادة الثالثة وعد نقل منها الأخرى عبادليا بمساعدة معاشة عندما تكون لدى الدولة الطرف الطالبة دواع معقولة للإشتباه في أن الجرم المشار إليه في الفقرة (1) ألأواب من المادة (3) نو طابع عبر وطني، بما في ذلك أن ضحايا تلك الجرائم أو الشهود عليها أو عائداتها أو الأدوات المستعملة في ارتكابها أو الأدلة عليها توجد في الدولة الطرف مثالية الطلب وأن جماعة إجرامية منظمة صالحة في ارتكاب الجرم.

يجوز أن تطلب المساعدة القانونية المعادلة، التي تقدم وفقا لهذه المادة لأي من الأعراض الثانية : الحصول على أدلة أو أقوال من الأشخاص، جميع المستجدات القضائية، حميد عمليات القديم والضبط والتحميد، فحضر الأشياء والمواقع تقديم المعلومات والأسلة والتقييمات التي يقوم بها الخبراء، تقديم أصول المستجدات والسجلات ذات الصلة بما فيها السحالك الحكومية أو المصرفية أو المالية أو سجلات الشركات أو الأعمال أو نسخ مصدقة عنيا، التعريف على عادات الحركة أو الممتلكات أو الأدوات أو الأحياء الأخرى أو إقضاء أثرها الأعراض الحصول على أملة تيسير مثول الأشخاص طوعية في الدولة الطرف الطالبة، أي نوع آخر من المساعدة لا يتعارض مع القانون الداخلي الدولة التعرف مثالية الكلية

ب – صور المساعدة القضائية المتبادلة تتخذ المساعدة القضائية المتبادلة أشكالا متعددة من بينها :

– تبادل المعلومات.

– نقل الإجراءات الجنائية.

– الإنابة القضائية الدولية.

– مثول الشهود والخبراء في المواد الجنائية.

2– تنفيذ الأحكام الجنائية الأجنبية:

إستنادا القاعدة إقليمية النص الجنائي فالحكم الجنائي الصادر عن محاكم دولة معينة لا يكون له أثر خارج حدود هذه الدولة فهو لا يحوز قوة الأمر المقدسي فيه، وبالتالي لا تكون له حجية خارج حدود دولته ويجوز إذن إعادة محاكمة المتهم عن نفس الفعل الذي ارتكبه في دولة أخرى، وتتأسس القاعدة على فكرة أن تنفيذ الحكم من أعمال السيادة، وعليه يصعب على أي دولة قبول تنفيذ حكم جنائي صدر خارج إقليمها لأنه يعتبر رضوخا لأوامر سلطة دولة أخرى، وهو ما ترفضه اعتبارات السيادة الوطنية يضاف إلى ذلك الرغبة لدى الدولة في تنفيذ الحكم الصادر بحق المجرم من محاكمها حتى لو أرتكب خارج إقليمها.

وفي الوقت الراهن لم يعد يطبق هذا الأصل على عمومه، إذ وجد له استثناءا تمثل في الجواز تنفيذ الحكم الجنائي الأجنبي في دوله أخرى بناء على نص قانوني يجيز ذلك أو إتفاقية دولية بين كلا الدولتين وهذا ما نوهت إليه وحثت عليه كثير من الاتفاقيات الدولية.

أ – تعريف الحكم الجنائي:

يعرف الحكم الأجنبي بأنه: " القرار الصادر من سلطة الحكم في موضوع الدعوى الجنائية أبي الدعوى المرفوعة بشأن جريمة يعاقب عليها قانون العقوبات أو القوانين الجنائية المكملة له"[1].

فالحكم الجنائي الأجنبي لا يختلف في جوهره عن الحكم الجنائي الوطني إذ أنه يعبر عن القرار الصادر من سلطة الحكم في موضوع الدعوي الجمالية، إلا أن الإختلاف الجوهري بينهما بالنظر إلى السلطة التي أصدرت هذا الحكم، حيث يصدر الحكم الأجنبي عن سلطة

[1]– عادل يحي، وسائل التعاون الدولي في عايد الاحتدام الحالية الأجنبية، الطبعة الأولى، دار البيضة العربية، القاهرة، 2004، ص 24

أجنبية مجير وطنية وعلى ذلك يمكن تعريف الحكم الجنائي الأجنبي بأنه " القرار الصادر في موضوع الدعوى الجنائية من سلطة لها ولاية الفصل في هذا الموضوع بإسم سيادة دولة أجنبية[1]. و يعني تنفيذ الأحكام الجنائية الأجنبية أنه إذا صدر حكم قضائي في إحدى المسائل الجنائية في دولة ما هيمكن تنفيذه في الدولة الأخرى كما لوكان صادرا في الدولة ذاتها المطلوب منها التنفيذ[2].

وأمام تطور الإجرام الدولي المنظم العابر للحدود واستفحال خطره الذي أضحى يهدد العالم أدى إلى ضرورة الإعتراف بحجية الحكم الجنائي الصادر عن محاكم دولة أخرى داخل إقليم الدولة إذ لا مفر لملاحقة هذه الأنشطة على نحو فعال من أن تعترف كل دولة في حدود وضوابط معينة بالقوة التنفيذية للحكم الأجنبي الصادر من محاكم دولة أخرى، وبالتالي وجب تجاوز فكرة عدم قابلية الحكم الأجنبي للتنفيذ لأنه من غير المقبول أن يشكل انتقال شخص من دولة صدر فيها حكم جدائي ضده إلى دولة أخرى حائلا دون تنفيذ هذا الحكم.

ب – أثار الحكم الجنائي:

تعبر الأحكام الجنائية عن سلطات الدولة التي تصدر فيها فهي كالقوانين التي تستند إليها ولها صفة أمرة تتجلى فيها سيادة الدولة بأقوى مظاهرها، ويتمتع الحكم الجنائي في إقليم الدولة التي يصدر فيها بحجية ذات شقين، شق إيجابي يتمثل في القوة التنفيذية التي يتمتع بها هذا الحكم، والشق السلبي الذي يقصد به إكتاب الحكم الجنائي ما يسمى بقوة الشيئ المحكوم فيه بحيث يصبح الحكم عدوانا للحقيقة تقضي به الدعوى العمومية، وإذا كان التسليم بالحجية التي يتمتع بها الحكم الجنائي في إقليم الدولة التي يصدر فيها لا يثير صعوبة إذ بعد ذلك تطبيقا مباشرا لمبدأ إقليمية قانون العقوبات فالتساؤل الذي ينور حول مدى إمكانية التسليم بهذه الحجية للأحكام الجنائية على الصعيد الدولي أي الإقرار بآثار الحكم الجنائي في غير إقليم الدولة التي صدر فيها[3].

[1]– عمار تيسير بجنوح، المرجع السابق ص 545.

[2]– أشرف محمد الأمين، النظرية العامة الجريمة الدولية، – دراسة الحسينية تأصيية، سنة 2012، ص 716.

[3]– عادل يحي، المرجع السابق، ص 20.

الفرع الثاني: الآليات المستحدثة للتعاون القضائي في مكافحة جريمة الارهاب الالكتروني.

إتجه مرفق العدالة الجنائية في الآونة الأخيرة إلى إرساء قواعد قانونية جديدة تواجه المشكلات التي أسفر عنها التطور التكنولوجي والمعرفي الكبير، وذلك من خلال الأخذ بمعطيات التكنولوجيا الحديثة في الكشف عن الجرائم وملاحقة مرتكبيها ومحاكمتهم، دون الإخلال في الوقت ذاته بحقوق المتهم أو غيره من أطراف الخصومة الجنائية، وتجلى ذلك بشكل واضح في مجال التحقيق من خلال استخدام تقنية الإتصال المرئي المسموع أو المحاكمة الجنائية عن بعد، حيث تبنت العديد من دول العالم استخدام هذه التقنية نظرا للمزايا والفوائد الكبيرة التي يمكن أن تحققها. وذلك من خلال عنصرين إعتمداهما تقسيما لهذا **أولا:** بعنوان " ماهية تقنية التحقيق الجنائي عن بعد أو تقنية الإتصال المرئي المسموع **ثانيا:** بعنوان الإطار القانوني لتقنية التحقيق الجنائي عن بعد الفيديو كونفرنس.

أولا: ماهية تقنية التحقيق الجنائي عن بعد[1].

هي وسيلة أو آلية حديثة للتحقيق أو المحاكمة الجنائية عن بعد يتم الإستعادة بها في بعض الحالات السماع شهادة الشهود والمتعاونين مع العدالة لكشف غموض الجرائم الخطيرة لاسيما المنظمة منها، بل وكذلك محاكمة المتهمين رغم تواجدهم داخل المؤسسة العقابية أمام محكمة قد تبتعد عن هذه المؤسسة أو تلك المؤسسات مئات الأميال[2].

وعليه وفي هذا الخصم سوف ترصد هذا الفرع الدراسة ماهية تقنية التحقيق الجنائي عن بعد أو تقنية الاتصال المرئي المسموع حيث تتناول تعريف تقنية التحقيق الجنائي عن بعد أولا وأساليب استخدام تقنية الاتصال عن بعد تاليا وإيجابيات تقنية التحقيق عن بعد ثالث.

---

[1]– ومصطلح الفيديو كونفرس ليس مصطفتها عربيا ، وانما يتكون هذا المصطلح من تكلمتين أصليها بالغة الانصيرية رياح بالأولى video البوشي، وبالثانية "conterence بنتها ان و اصفح مجمعا الاجتماع التحرش أمن بالسعة الفرنسية بالمصطلح يقصد به مالك المصرى Video–conference في الاجتماع أو الموتر الكيريوني والاجتماع بالمعنى العربي بدون من هذه أحد من يعترف فيه أمرين أن يشدد الأشخاص وأشخاص آخرون يسمعونيد ويته عالي الطرفين مع تعظيم البعض من خلال أستة وأخرية ويتغالب الأطراف السيف عامر يدين التعليق والحالة الثانية عن بعد برسة الحبيبية تأصيبية التعلمية (Video Conference) دار الشيصة العربية القاهرة، 2006، ص 22.

[2]– تيسير بجبوج، المرجع السابق، ص 272

1- تعريف تقنية التحقيق الجنائي عن بعد:

عرف جان من الفقه الجنائي هذه التقنية بأنها وسيلة للإتصال المرئي المسموع الإجتماع شخصين أو عدة أشخاص في أماكن مختلفة سواء في داخل دولة واحدة أو بين عدة أشخاص في أماكن مختلفة، سواء في داخل دولة واحدة أو بين عدة دول يستطيعون المشاركة في اجتماع بالمناقشة بصورة إيجابية وفعالة، تمكن جميع الأطراف من رؤية الآخرين وسماعهم والحديث معهم في الوقت سواء تعلق الأمر بطلبات التحكيم الدولية أو إجراءات الدار قصة ويمكن في إطار الإجراءات المنقبة سماع أقوال الشهود والخبراء وفي بعض الأسنان العليم عن هذه التقنية[1].

وباللجوء إلى استخدام هدية الفيديو كونفرس في مجال التحقق الجمالي أصبح من الممكن إمداد النطاق الإقليمي لجلسة التحقيق أو المحاكمة بحيث يعمل عدد أماكن السنة داخل الدولة الواحدة أو أماكن إقليمية في دول متعددة، وبحيث تكون سلطة التحقيق في دولة والمتهم الذين يتم التحقيق معه يكون في دولة أخرى وقد يكون الدهود في دولة ثالثة.

2-أساليب استخدام تقنية الاتصال عن بعد

استعرض في ما يلي أساليب استخدام الحية الاتصال عن بعد والتي التماثل في

- ✓ نظام الإتصال من مكان واحد محمد القاعة الجلسة.
- ✓ الإتصال الفردي بين أكثر من مكان وقاعة الجلسة.
- ✓ الإتصال الثابت الجماعي بين أكثر من مكان وقاعة الجلسة.
- ✓ الإتصال المستمر المتقدم بين قاعة المحكمة ومكانين فقط.

ويرى رواد الفقه الجنائي أن النمط الأخير من تقنية الفيديو كونفرس عن بعد من أفضل الأنماط لتحقيق فكرة الحضور الإعتباري[2] في ضوء ما يحققه في حال جودة الاتصال بدون فترات القطاع من ضمان الرؤية والسماع المتبادل بين الأطراف المشاركة في المحاكمة

[1]- رامي متولي القاضي، الوضيف التكنولوجيا المعلومات في مجال الإجراءات العمالية مقال منشور في مودي العلوم والتكولوجيا المعاد من 9 إلى 11 ديسمبر 2017 الكلية الحقوق جامعة عين شمس، ص 10 و 11

[2] -Sossin, Lome and Yetnikoff, Zimura, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources (August5. 2007). Windsor Yearbook of Access to Justice, 2007, p257

الجنائية عن بعد وبصورة مترامية وواضحة وفعالة، بما يمكن التقرير معه بإمكان القول ولو مجازا بأن الأقوال أبديت شفهيا بقاعة المحكمة.

3- إيجابيات تقنية التحقيق عن بعد

استعرض فيما يلي إيجابيات تقدية التحقيق عن بعد والتي تمثل في:

أ - سرعة إنجاز القضايا:

يؤدي استخدام تقنية الفيديو كونفرس إلى تبسيط وتسريع إجراءات التحقيق والمحاكمة الجنائية فإذا ما قورنت مع إجراءات الإنابات القضائية بجد إن الإنابة القضائية تتسم بالبطء والتعقيد، حيث يتم إرسالها عبر الطرق الدبلوماسية في الدولة المطلوبة فيها التنفيذ ومن ثم إلى وزارة العدل فالمحكمة المختصة، حتى تصل إلى الجهة القضائية في الدولة الطالبة[1] وهذا كله يتصف بطول الإجراءات وزيادة التكاليف مما فاللجوء إلى التحقيق عن بعد قد يحول دون طول هذه الإجراءات ومن ثم تجنب الإفراج عن المتهمين لإنتهاء المدة الواجبة في الحبس الاحتياطي فضلا عن أن نقل المتهمين من أماكن الاحتجاز إلى الأماكن التي تنعقد فيها جلسات التحقيق أو المحاكمة تؤدي إلى زيادة النفقات التي تترتب على ذلك.

ب - حماية الشهود والمجني عليهم

تتجلى أهمية تقنية ال video conference باعتباره إحدى الوسائل الفعالة التي تضمن حماية أطراف النزاع أو الدعوى القضائية كالشهود والمجني عليهم وأي شخص آخر من الأشخاص المتعاونين مع العدالة، حيث يرى البعض ضرورة استخدام هذه التقنية في سماع الشهود والمتهمين التاثيين المتعاونين مع العدالة لكي يتم الحصول على إفاداتهم المتعلقة بالعصابات الإجرامية المنظمة حول مخططاتهم الإجرامية المستقبلية وغيرها من المعلومات التي تفيد العدالة الجنائية في القبض عليهم[2].

---

[1]- رامي متولي القاضي، توطين التكنولوجيا المعلومات في مجال الإجراءات الجنائية، المرجع السابق، ص 24

[2]- قامت وزارة العدل السعودية بصفين برنامج للمحاكمة عن بعد بهدف قليل عند التقاضي واختصار الوقت والجيد مع تحقيق كافة الصمامات القضائية للمتهمين والسجناء أثناء المحاكمة، وتخفيف العباء والتكاليف المصاحبة العملية عقل المحبوسين والتوفير الجهد والمال على إدارات السجون، حيث تم تجهيز حرف مزودة بتقنيات نقل صورة وصوت عالية الجودة في السجون مرتبطة بالمكاتب القضائية، حيث يتم التحقق من هوية السجين عن طريق نظام البصمة المرقط بمركز المعلومات الوطني، ويستفاد من هذه الخدمة في القضايا المطورة من قاصي فردي والتي تمثل سنة الكبيرة من القضايا المقطورة أمام المحاكم، حيث بدأ تطبيق هذا البرنامج في المحكمة الجزائية بالرياض، وجاري التوسع في تطيقه ليعمل الكافة المحاكم التي لديها نسبة قضايا مرجعة أنظر الموقع الالكتروني لصحيفة

هذه التقنية لعدم كشف هذه الجماعات الإجرامية الأماكن تواجد الشهود وتحركاتهم وذلك حماية لهم من الانتقام الذي قد يتعرضون له

ت تعزيز الوسائل المتبعة في التعاون الدولي لمكافحة الجريمة

تقنية الفيديو كونفرس تعد وسيلة مستحدثة وإضافية من وسائل التعاون الدولي في مكافحة الجرائم والمساعدات القضائية المتبادلة بين الدول، ولا سيما في مجال إستجواب المتهمين وسماع الشهود عندما يكونون مقيمين في إقليم دولة غير تلك الدولة التي تقوم بالتحقيق أو المحاكمة، حيث يكفل اللجوء إلى هذه التقنية الوصول إلى حل توافقي للمشكلات الناتجة عن إختلاف النظام الإجرائي للدولتين الطالبة والمطلوب منها التنفيذ على إعتبار أنه سوف يكون هناك قانون واحد واجب التطبيق هو قانون الدولة الطالبة التي تباشر الإجراءات وفقا لما هو منصوص عليها في قانونها.

ثانيا : الإطار القانوني لتقنية التحقيق الجنائي عن بعد (فيديو كونفرنس):

شكل إستخدام تقنية الفيديو كونفرس مرحلة جديدة من مراحل تطور الإجراءات الجنائية بشكل يعكس الرغبة في الاستفادة من المعطيات التكنولوجية الحديثة في مجالات تطوير مرافق العدالة الجنائية، وقد أرست العديد من الإتفاقيات الدولية والتشريعات الوطنية تقنية التحقيق عن بعد. وعليه وفي هذا الخضم سوف ترصد هذا الفرع الدراسة الإطار القانوني لتقنية التحقيق الجنائي عن بعد (فيديو كونفرنس حيث سيتناول التنظيم التشريعي لتقنية الفيديو كونفرنس في التشريعات المقارنة أولا والإطار القانوني الدولي الإتفاقيات الدولية – ثانيا . أولا : التنظيم التشريعي لتقنية الفيديو كونفرنس في التشريعات المقارنة ناول عدد ليس بقليل من التشريعات المقاربة تقنية الفيديو كونفرس في تشريعاتها الإجرائية

ومن أبرز هذه التشريعات ما يلي:

- ✓ التشريع الفرنسي:
- ✓ التشريع الإماراتي:
- ✓ التشريع البحريني
- ✓ التشريع الجزائري:

المدينة السعودية تاريخ الزيارة http://www.al-madina.com/article/473756 في 16/04/2024 على الموقع الكتروني 6.00 04/03/2024 ساعة الزيارة ، أنظر: أيضا تيسير بحلول ، المرجع السابق ، ص 276.

ج التشريع الجزائري:

أجاز التشريع الجزائري سماع الشهود والخبراء عبر تقنية الفيديو كونفرس حيث أشارت المادة (65) مكرر 127[1] من قانون الإجراءات الجزائية الجزائري إلى جواز سماع شهادة الشهود والخبراء باستخدام تقنيات حديثة لا تسمح بمعرفة صورته وصوته أو شمع بسماع شهادته عن بعد ويكون ذلك إما من محكمة الموضوع من تلقاء نفسها أو يطلب من الأطراف، حيث نصت المادة المذكورة على أنه يجوز لجهة الحكم تلقائيا أو بطلب من الأطراف سماع الشاهد مخفي الهوية عن طريق وضع وسائل تقنية تسمح بكتمان هويته بما في ذلك السماع عن طريق المحادثة المرئية عن بعد واستعمال الأساليب التي لا تسمح بمعرفة صورة الشخص وصوته

1- الإطار القانوني الدولي لتقنية " الفيديو كونفرنس:"

من خلال هذا الجزء من دراستنا سوف تعالج الإطار القانوني الدولي – الإتفاقيات الدولية التقنية التحقيق الجنائي عن بعد (فيديو كونفرس)، حيث سنتطرق للإتفاقية العربية لمكافحة الجريمة المنظمة ثم للبروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية، وكذا إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

أ – الإتفاقية العربية لمكافحة الجريمة المنظمة

لم تغفل الإتفاقيات العربية الإشارة إلى جواز الاستعادة بتقدية الفيديو كونفوس في مجال سماع شهادة الأشخاص المتعاونين مع العدالة من شهود وخبراء ومبلغين ومجني عليهم، حيث أشارت المادة (36) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية إلى توفير الحماية للشهود والخبراء بالنص على أن تلتزم كل دولة طرف أن تتخذ ما يلزم من تدابير لتوفير الحماية من أتي إنتقام أو ترهيب محتمل للشهود والخبراء الذين يوافقون على الإدلاء بأقوالهم بخصوص إحدى الجرائم المشمولة بهذه الاتفاقية وكذلك لأقاربهم وسائر الأشخاص مع إتاحة الإدلاء بالشهادة على نحو يكفل سلامة الشهود والخبراء والضحايا، ويجوز استخدام التقنيات الحديثة في هذا المجال[2].

[1] ـ نص المادة (65) كرر 27 من الأمر رقم 15-2- المؤرخ في 23/07/2015 المعدل بالقانون الإجراءات العراقية.

[2] - شعنبي صابرة، الجهود الدولية في مكافحة الغرهاب الإلكتروني، أطروحة مقدمة لنيل شهادة العلوم في الحقوقن تخصص: قانون جنائي، جامعة الشهيد الشيخ العربي التبسي- تبسة، 2019، ص 68.

ب-البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية

تعد مواثيق الاتحاد الأوروبي من أبرز الإتفاقيات الإقليمية والدولية التي عملت على تنظيم إجراءات وشروط اللجوء إلى تقنية الفيديو كونفرس، ومن أبرز هذه المواثيق البروتوكول الثاني الإضافي للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية. أجاز الإتحاد الأوروبي في الإتفاقية الأوروبية الجديدة للمساعدة القضائية في المسائل الجنائية التي أقرها المجلس الأوروبي في 30/11/2000 استخدام تقنية الفيديو كونفرس كوسيلة للتحقيق الجنائي عن بعد في سماع إفادات الشهود والخبراء بين الدول المتعاقدة وفي إطار الحرص على تفعيل التعاون الدولي في المسائل الجنائية وبصفة خاصة المساعدة القضائية[1]، لذلك حرصت دول القارة الأوروبية على تضمين البروتوكول الإضافي الثاني للإتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجنائية، والذي تم التوقيع عليه في ستراسبورج في 08/11/2001 توسعا في آليات ووسائل التعاون الدولي القضائي من خلال الإستفادة من الوسائل التقدية الحديثة في مجال القانون الجنائي ومنها إستعمال تقنية الفيديو كونفرس، على إعتبار أن هذه النقدية تكفل سرعة أكبر ومرونة وفاعلية أشد لهذا التعاون على ألا يتعارض ذلك مع حقوق الإنسان وسيادة القانون[2] بهدف ضمان مواجهة قانونية وقضائية فعالة وسريعة للجرائم الخطيرة التي باتت تهدد الدول الأوروبية وقد تضمنت المادتان التاسعة والعاشرة من البروتوكول بيانا تفصيليا لكيفية إستخدام هذه التقنية، وهو ما سوف تتناوله على النحو التالي:

2-شروط تطبيق تقنية الفيديو كونفرنس في أحكام البروتوكول:

حددت المادة التاسعة (09) من البروتوكول الشروط التي يتوجب على الدول الأوروبية العقيد بها عند استخدام تقنية الفيديو كونفرس في الإجراءات الجنائية، حيث إستلزمت عدم تعارض إستخدام هذه التقنية مع المبادئ الأساسية لقانون الدولة المتقدة، كما توجب توفير الإمكانيات الفنية التي تمكن الدولة المنفذة من استخدام هذه التقنية، على أن يقتصر استخدامها في مجال سماع الشهود والخبراء وذلك على النحو التالي:

[1]- صفوان محمد الصديقات التحقيق والمحاكمة الجزائية عن بعد عبر غنية Video-conference ، مجلة علوم الشريعة والقانون المجلد 42 العدد الأول، جامعة العلوم الإسلامية، الأردن 2015 من 356.

[2] - رامي متولي القاضي، توظيف تكنولوجيا المعلومات في مجال الإجراءات الجنائية، المرجع السابق ص30

- عدم تعارض تقنية الفيديو كونفرنس مع قانون الدولة المطلوب فيها التنفيذ[1].
- توافر الوسائل والإمكانيات التي تمكن الدولة المنفذة من إستخدام هذه التقنية[2].
- قصر استخدام هذه التقنية على سماع الشهود والخبراء[3] .
- إجراءات اللجوء لتقنية الفيديو كونفرنس في أحكام البروتوكول.
- تقديم طلب للدولة التي يتواجد فيها الأشخاص المطلوب سماعهم.
- مباشرة الإجراء المطلوب تنفيذه
- إجراءات السلطة القضائية في الدولة المطلوب عليها التنفيذ[4].
- إخطار الشخص المطلوب بهذا الطلب.
- حضور ممثل للدولة المنفذة خلال مباشرة الإجراء.

3- إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية:

تطالب المادة (18 هـ / 18) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة الدول الأطراف بإستخدام تشريعات داخلية تسمح بعقد جلسات استماع عن طريق الفيديو أو من خلال استخدام وسائل تكنولوجية أخرى، كالأجهزة والبرمجيات الخاصة بتمويه الصورة والصوت لمنع كشف هوية الشاهد للمتهم والجمهور، حيث نصت الفقرة المذكورة على أنه: " عندما يتعين سماع أقول شخص موجود في إقليم دولة طرف بصفة شاهد أو خبير أمام السلطات القضائية لدولة طرف أخرى و يكون ذلك ممكنا ومتفقا مع المبادئ الأساسية للقانون الداخلي، يجوز للدولة الطرف الأولى أن تسمح، بناء على طلب الدولة الأخرى، بعقد جلسة إستماع عن طريق الفيديو إذا لم يكن ممكنا أو مستصوبا مثول الشخص المعني بنفسه في إقليم الدولة الطرف الطالبة.

ويجوز للدول الأطراف أن يتفق على أن تتولى إدارة جلسة الإستماع سلطة قضائية تابعة للدولة الطرف الطالبة وأن تحضرها سلطة قضائية تابعة للدولة الطرف متلقية الطلب."

---

[1] -Art 9-1..... and on condition that it has the technical means to carry out the hearing. If the requested Party has no access to the technical means for video conferencing, such means may be made available to it by the requesting Party by mutual agreement

[2] –شريف محمد محمد عمر، آليات التعاون القصائي الدولي في مجال مكافحة الجريمة (كندية التحقيق الجنائي عن بعد تقنية الفيديو كونفرانس نموذجا) أعمال المؤصر القانون والتكنولوجياء الجزء الثاني، ديسمبر، 2017 المرجع السابق.

[3] - صفوان الصديقات، المرجع السابق، ص 357،

[4] - فريد محمد محمد عمر، المرجع السبق، ص 40.

كما نصت المادة (24) من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والمعنونة بحمية الشهود على أنه – تتخذ كل دولة طرف تدابير ملائمة في حدود إمكانياتها التوفير حماية فعالة للشهود الذين يدلون في الإجراءات الحداثية بالشهادة بخصوص الجرائم المشمولة بهذه الاتفاقية، وكذلك لأقاربهم وسائر الأشخاص الوثيقي الصلة بهم حسب الاقتضاء، من أي انتقام أو ترهيب محتمل.

خلاصة الفصل الثاني:

يعاني المجتمع الدولي في كل شبر من أرجائه في هذا العصر من جرائم مستحدثة التي غطت على الجرائم التقليدية، حيث بات الإرهاب الالكتروني وما يفرزه من مشاكل وتهديدات الشغل الشاغل للمجتمع الدولي، وفي ظل زيادة خطورة هذا الإرهاب الجديد وانتشاره الرهيب أصبحت محاربته ضرورة حتمية تستوجب على دول تكثيف جهودها بسن تشريعات وإبرام الاتفاقيات وإنشاء منظمات الدولية والإقليمية لمكافحة هذا الوحش الذي أضحى من أكبر التحديات التي تواجهها الدول.

وان خطورة هذا الإرهاب فرضت على الحكومات تطوير وسائلها وقدراتها لتصدي لتهديداته المختلفة بتوفير التقنيات اللازمة للحماية وتقنين قواعد وتشريعات على مستوى الإقليمي والدولي. وان الطابع العالمي لهذه الظاهرة ازدها تعقيد في شان مكافحتها دوليا، خاصة مع عدم وجود إطار قانوني دولي واضح يتناول هذه الظاهرة المستحدثة، ولقد حضي الإرهاب الالكتروني باهتمام كبير على كافة الأصعدة سواء الدولي أو الإقليمي إذ عقدت في شانه العديد من الاتفاقيات وندوات مختلفة وتسابقت جل الدول الكبرى إلى سن تشريعات بهدف الحد منه.

الخاتمة

الخاتمة:

في ختام هذه الدراسة نصل إلى خلاصة مفادها أن الإرهاب الإلكتروني هو تلك الأعمال الواقعة عبر الأجهزة الإلكترونية الموصولة بشبكة الإنترنت، بحيث تنطوي هذه الأعمال على التخويف والتهديد، أو نشر أفكار ومعتقدات متطرفة وعصرية، أو إختراق النظم وكذا بيانات الشخص بذاته أو شركة أو دولة معينة.

وعليه نستخلص من خلال هذه الدراسة النتائج التالية:

- أصبح الإرهاب الإلكتروني واقعا معاشا ذو أبعاد خطيرة لا يمكن التنبؤ بها، خاصة مع إرتفاع عدد المستخدمين للإنترنت والنمو السريع لتقنيات الحاسوب، مما عقد سبل مكافحته وجعلها صعبة.
- الإرهاب الإلكتروني من الجرائم غير المنتهية والمستمرة والعابرة للحدود، ذلك لأن مرتكب الفعل الإجرامي الإلكتروني "الإرهابي الإلكتروني" لا يمكن ردعه ومحاسبته عن جرائمه دون تفعيل وتحيين النصوص القانونية وفق حداثة الفعل الإجرامي، ولذلك وجب على المشرع مواكبة التطور التكنولوجي في نص النصوص القانونية.
- إن مختلف الجهود لمكافحة الإرهاب الإلكتروني لم تكن في مستوى خطورة الفعل الإجرامي، فمنظمة الأمم المتحدة لم تكن مساعيها في هذا المجال واضحة وثابتة مما يبرر عدم عقد اتفاقية دولية خاصة بمكافحة الإرهاب الإلكتروني، وإن كانت اتفاقية بودابست لمكافحة جرائم الحاسب الآلي تناولت في محتواها مكافحة الأعمال الإرهابية عن طريق الإنترنت، فهذا لا يكفي خاصة مع التطور والتهديد المستمرين لمرتكبي جرائم الإرهاب الإلكتروني.
- إن الجهود الدولية لا تقل عن جهود مختلف الحكومات في مكافحة الجرم الإلكتروني،فهناك من الدول من سنت قوانين وتشريعات خاصة لمكافحة الإرهاب الإلكتروني، وفي المقابل هناك دول لم تستحدث تشريعاتها في هذا المجال، خاصة دول العالم الثالث إلا في بعض جوانب هذه الجريمة كإختراق الأنظمة مثلا.

- إن جل ما تقوم به الدول المسيطرة دوليا من أعمال عدائية إلكترونية اتجاه غيرها من الدول لا يختلف عما تقوم به الجماعات الإرهاب الإلكتروني من خلال استعمالها للمعلوماتية، وبذلك فيمكن أن يكون مرتكب الجرم الإلكتروني إما فردا أو جماعة أو دولة.
- ضعف الجهود الدولية والإقليمية خاصة العربية والجزائرية منها في مكافحة الإرهاب الإلكتروني، وذلك راجع إلى الأزمات المتعددة وكذا المتنوعة التي مر ويمر بها العالم، وكذا الوطن العربي خاصة الجزائر منها.
- نلاحظ من خلال دراستنا هذه محدودية الآليات الدولية وكذا الوطنية التي سنت لمواجهة وتصدي جريمة الإرهاب الإلكتروني، لذا لم تحقق النتائج الردعية المرجوة منها.

نوصي من خلال هذه الدراسة بمايلي:

- ✓ على المشرع الجزائري وضع نصوص قانونية ردعية لمنع العود والتخطيط لنفس الأفعال الإجرامية الإلكترونية وغيرها، وذلك لتسهيل عملية إكتشاف هوية مرتكب الجريمة الإلكترونية والقبض عليه.
- ✓ يجب وضع آليات وقائية قبل وضع الآليات الردعية لمكافحة جريمة الإرهاب الإلكتروني وذلك من خلال نوعية النصوص القانونية والاتفاقيات الدولية التي تضيق على مرتكب الفعل الإجرامي المجال الجرمي.
- ✓ توعية المجتمعات خاصة منها مجتمعات العالم الثالث والدول النائية، والتي تعاني من الجهل والمشاكل الاجتماعية المزرية، وذلك من خلال تنظيم ندوات، وكذا لقاءات تحسيسية في المجال الإلكتروني خاصة، وهذا ما يحد أو يقلل من هذا النوع من الجريمة.
- ✓ إعادة النظر في البرامج الدراسية وفق التطورات التكنولوجية في جميع مراحله، وذلك لترسيخ التوعية المعلوماتية، وهذا ما يعتبر من الآليات الوقائية قبل مكافحة الفعل الإجرامي في المجال الإلكتروني، وهذا ما يمكن إعتباره من الوسائل الفعالة في التربية الإلكترونية.
- ✓ مراقبة الأطفال من طرف الأولياء خاصة وأن هذه الفئة من المجتمع تعتبر الأكثر استعمالا للإنترنت كمواقع التواصل الاجتماعي وغيرها من المواقع، والتي عن طريقها تقوم الجماعات الإرهابية بالتواصل مع الأفراد والتعريف بتنظيمها الإرهابي.

- ✓ يجب تفعيل دور الجمعيات الوطنية والمنظمات الدولية خاصة منها منظمة الأمم المتحدة من أجل مكافحة فعالة للإرهاب الإلكتروني.
- ✓ يجب على الدول مجتمعة أن تتكاتف في جهودها للتعاون من أجل مكافحة تشريعية ومؤسساتية دولية للإرهاب الإلكتروني، وذلك من خلال عقد اتفاقيات دولية، وإنشاء قضاء دولي مختص في مجال الجرائم الإلكترونة العابرة للحدود. ووضع إستراتيجية دولية شاملة وفعالة لمكافحة الإرهاب الإلكتروني.
- ✓ يجب أن يحدد التجريم ليس فقط للأعمال الإرهابية الإلكترونية، بل عليه أن يشمل أيضا مجموعة من السلوكيات المادية التي تتضمنها الحروب الإلكترونية، والتي تقوم بها بعض الدول، كاختراق دولة ما لأنظمة جيش دولة أخرى، أو إصابة أنظمتها الأمنية المعلوماتية بفيروس حتى تبقيها تحت السيطرة.
- ✓ على حكومات الدول تكوين القضاة في مجال المعلوماتية، وفق ما عصرنة تشريعاتها، لأن في عصر الرقمية يجب استحداث مؤسسات قضائية مختصة في المجال القضاء الرقمي الإلكتروني، مستعينة في ذلك بخبراء ومختصين في هذا المجال الإلكتروني.
- ✓ يجب تأمين البيانات والمعلومات المهمة بصفة مستمرة سواء تعت هذه المعلومات بالفرد أو الدول أو الشركات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر

I-الدستور الجزائري 1996

1-المادة 119 قانون العقوبات المصري، المادة 87 مكرر من قانون العقوبات الجزائري.
2-القانون رقم 16-01 المؤرخ في 06 مارس2016، المتضمن التعديل الدستوري، المؤرخة في 7 مارس 2016، الجريدة الرسمية عدد: 14.

أ-الإتفاقيات:

1. النظام الأساسي للمنظمة الدولية للشرطة الجنائية 13 تموز 1956.
2. اتفاقية الجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية، الموقعة في نيويورك عام 1973.
3. اتفاقية مناهضة أخذ الرهائن الموقعة في 18/12/1979 في نيويورك، وقد اعتمدت هذه الاتفاقية قبل صدور القرار 34/1461 من قبل الجمعية العامة للأمم المتحدة، وبحلول نهاية عام 1980 كان قد تم التوقيع عليها من قبل 39 دولة ودخلت حيز التنفيذ في 3 يونيو 1983 بعد أن صدقت عليها 22 دولة، واعتبارا من ديسمبر 2014 فإن اتفاقية أصبحت الضم 174 دولة.
4. اتفاقية الرياض للتعاون القضائي بين الدول العربية المصدقة بالقانون رقم 14 بتاريخ 10/10/1983، وقد وافق على هذه الاتفاقية مجلس وزراء العدل العرب بموجب قراره رقم 01 المؤرخ 06/04/1983 في دورة انعقاده الأولى في الرياض ودخلت الاتفاقية حيز النفاذ ابتداءا من تاريخ 30/10/1985
5. اتفاقية ماسترخت سنة 1992 التي دخلت حيز التنفيذ سنة 1993، وتم الاتفاق عليها من قبل المجلس الأوروبي في مدينة ماسترخت الهولندية في ديسمبر 1991، ودخلت هذه المعاهدة، التي تم توقيعها في 7 فبراير 1992 في ماسترخت، حيز التنفيذ في الأول من نوفمبر 1993.

6. الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 والتي اعتمدها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك بالقاهرة يوم 22/04/1998 ودخلت
7. اتفاقية المعافية على تمويل الإرهاب لسنة 1996، والتي اعتمدت وعرضت التوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 54109 المؤرخ في 9 كانون الأول / ديسمبر 1999. 8 اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، التي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم (25) في الدورة الخامسة والخمسون بتاريخ 15/11/2000 منشورات الجمعية العامة للأمم المتحدة 08/01/2001.
8. اتفاقية بودابست لسنة 2001 ، حيث تم اعتماد الاتفاقية وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة في 08/11/2001 وفتح باب التوقيع عليها في 23/11/2001 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.
9. الاتفاقية العربية لمكافحة تقنية نظم المعلومات التي وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المتعقد بالقاهرة بتاريخ 51432/01/1 هـ الموافق لـ 21/12/2010، وقد وقعت عليها الجزائر في 2010/12/21.

ج القرارات الدولية:

1. قرار مجلس الأمن رقم 883 المؤرخ في 11 نوفمبر 1993 المتعلق بقضية لوكربي الليبية.
2. قرار مجلس الأمن رقم 1044، الصادر في الجلسة رقم 3627 المنعقدة في 21 1996جانفي
3. قرار مجلس الأمن رقم 1373 الصادر بتاريخ 28 سبتمبر 2001
4. قرار مجلس الأمن رقم 2322 لسنة 2016.

د القوانين الوطنية:

1. 1966 الأمر 66-156 المؤرخ في 18 صفر 1386 الموافق لـ ك يونيو المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

الكتب:

1. إبراهيم بن محمد محمود الزندان، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني : دراسة مقارنة، جامعة فطاني، ط 1، 2018.
2. أشرف محمد الأمين، النظرية العامة الجريمة الدولية، – دراسة الحسينية تأصيية، سنة 2012.
3. أشرف محمد لاشين، النظرية العامة للجريمة الدولية – دراسة تحليلية تأصيلية ، 2012.
4. أمير فرج يوسف ،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر، مكتبة الوفاء القانونية،ط1، الإسكندرية، مصر ،2011 .
5. بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجازئر: الدور والتحديات كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة، 2017.
6. بخاري جميل علي، جريمة الإرهاب الدولي ومشروعية نضال حركات التحرر الوطني إقليم كردستان، المركز العربي للنشر والتوزيع، ط 1، مصر، 2020.
7. بلعليات إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري – أركان الجريمة، أهمية الإثبات الجنائي طرق الإثبات الجنائي، دار الخلدونية للنشر والتوزيع، د.ط، الجزائر، 2007.
8. حسن مظفر الرزو، الفضاء المعلوماتي، بيروت، مركز دراسات الوحدة العربية، 2007 ، ط1.
9. خلفي عبد الرحمان، الإجراءات الجزائية في التشريع الجزائري والمقارن، دار بلقيس للنشر، الجزائر 2015.
10. رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية حول: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب.

11. شريف محمد محمد عمر، آليات التعاون القضائي الدولي في مجال مكافحة الجريمة (كندية التحقيق الجنائي عن بعد تقنية الفيديو كونفرانس نموذجا) أعمال المؤصر القانون والتكنولوجيا الجزء الثاني، ديسمبر، 2017 .
12. عادل يحي، وسائل التعاون الدولي في عايد الاحتدام الحالية الأجنبية، الطبعة الأولى، دار البيضة العربية، القاهرة، 2004.
13. عبد القادر الشيخي، طبيعة الإرهاب الإلكتروني، رابط العرب الإسلامي، ط1، السعودية، 2015.
14. عبد القادر عدو، قانون العقوبات الجزائري القسم العام الجريمة – نظرية الجزاء الجنائي، دار هومة للطباعة والنشر، د ط ، الجزائر، 2010.
15. عبد الله سليمان، شرح قانون العقوبات الجزائري – الجريمة – القسم العام، ديوان المطبوعات الجامعية 2: ط 1 ، الجزائر، 2005.
16. علاء الدين راشد، الأمم المتحدة والإرهاب قبل وبعد 11 سبتمبر، دار النهضة العربية، القاهرة، 2005.
17. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية»، طرابلس، بتاريخ 24– 25 مارس 2017.
18. القطاونة مصعب، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني، الأردن، 2010.
19. محمد معمري، الإرهاب في صورة الحديثة، طلا منشاء المعارف، الإسكندرية، مصر، 2017.
20. محمود صالح العادلي، الجريمة الدولية – دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2004.
21. مصطفى محمد موسى: الإرهاب الإلكتروني (دراسة قانونية أمنية نفسية إجتماعية)، دار الكتب والوثائق القومية المصرية، ط1، القاهرة، 2009.

22. مصطفى محمد موسى، الإرهاب الالكتروني- دراسة قانونية – أمنية – نفسية – اجتماعية، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، مطابع الشرطة، دون مكان نشر، 2009.
23. هشام محمد جرائم الإرهاب المعلوماتية، المركز العربي بالإصدارات القانونية، مصر، 2016.
24. ولد الصديق ميلود، مكافحة الإرهاب بين مشكلة المفهوم واختلاف المعايير، مركز الكتاب الأكاديمي، ج1، ط1، عمان، 2018.
25. يوسف حسن يوسف: لجرائم المعلوماتية، المركز القومي لإصدارات القانونية، ط1، القاهرة، 2011.
26. يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية،ط1، القاهرة، مصر ،2011.
27. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الإستراتيجية السليمانية – العراق، 2007.
28. سليمان عبد المنعم، الجوانب الإنتقالية في النظام القانوني لتسليم المنجومين دراسة مقاربة، دار الجامعة الجديدة الاستقدرية، 2007 .

المذكـــــرات:

أ-الأطروحات:

1. شعبان لمياء، الجهود الدولية في مكافحة الإتجار بالبشر عبر الأنترنت، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون العام، تخصص، قانون عام، جامعة الشهيد الشيخ العربي التبسي تبسة، 2020/2019.
2. شعنبي صابرة، الجهود الدولية في مكافحة الغرهاب الإلكتروني، أطروحة مقدمة لنيل شهادة العلوم في الحقوق، تخصص: قانون جنائي، جامعة الشهيد الشيخ العربي التبسي- تبسة، 2019.
3. شنتير خضرة ،الآليات القانونية لمكافحة الإرهاب الالكتروني-دراسة مقارنة-)أطروحة دكتوراه،القانون الجنائي،كلية الحقوق ،جامعة أحمد د أدرار ،2020-2021 .

4. عمار تيسير بحبوح، التعاون الدولي في مكافحة جرائم الإرهاب، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق جامعة القاهرة 2010.
5. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت أطروحة دكتوراه في القانون، كلية الحقوق جامعة عين شمس، القاهرة 2003/2004.

المذكرات:

1. أحمد مسعود مريم اليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 09-04، مذكرة مقدمة لنيل شهادة الماجستير ، تخصص قانون جنائي ، ك ح ع س، جامعة قاصدي مرباح، ورقلة 2012/2013.
2. بربوش محمد، أمين محمودي محمد، التسرب ودوره في الكشف عن الجرائم، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، ك ح ع س، جامعة العقيد أكلي محند أولحاج البويرة، 2018.
3. بوشعرة أمينة، موساوي سهام الإطار القانوني للجريمة الإلكترونية دراسة مقارنة، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، ك ح ع س جامعة عبد الرحمان ميرة 2018/2017.
4. توات عبد الحكيم، جريمة الإرهاب الإلكتروني، مذكرة مكملة لنيل شهادة الماستر، تخصص، جريمة وأمن عمومي، جامعة الشهيد الشيخ العربي التبسيي 2021، 2022.
5. سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج الخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012.
6. علي بوعمرة، جريمة الإرهاب الإلكتروني، مذكرة مكملة لنيل شهادة الماستر، تخصص: جريمة وأمن عمومي، جامعة الشهيد الشيخ العربي التبسيي 2020-2021.

المجلات:

1. صفوان محمد الصديقات التحقيق والمحاكمة الجزائية عن بعد عبر غنية Vidéoconférence، مجلة علوم الشريعة والقانون المجلد 42 العدد الأول، جامعة العلوم الإسلامية، الأردن 2015 .
2. يوسف مرين، جريمة الإرهاب في القانون الجزائري،(مجلة جامعة القدس المفتوحة للابحاث والدراسات،عدد42-،2017.

المؤتمرات والمداخلات:

1. جميل عبد الباقي الصغير، مداخلة بعنوان: مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الإرهاب عبر الانترنت، حلقة علمية موسومة بـ الإنترنت والإرهاب، نظمتها جامعة نايف العربية للعلوم الأمنية بالقاهرة بالتعاون مع جامعة عين شمس، خلال الفترة الممتدة من 15 – 19 نوفمبر 2008، القاهرة.
2. حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني"آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.
3. رامي متولي القاضي، الوظيف التكنولوجيا المعلومات في مجال الإجراءات العمالية مقال منشور في مودي العلوم والتكنولوجيا المعاد من 9 إلى 11 ديسمبر 2017 الكلية الحقوق جامعة عين شمس.
4. زياد محمد جفال، تسليم المجرمين كأحد آليات جامعة الدول العربية لمكافحة الإرهاب وموقف المشرع الإماراتي، مقال منشور في مجلة الشارقة للعلوم القانونية، المجلد 16 العدد الأول، 2019 .
5. عبد الله علي عبو سلطان، دور القانون الدولي الجنائي في حماية حقوق الإنسان، أطروحة دكتوراه في القانون العام، كلية الحقوق جامعة الموصل العراق، 2003/2004.
6. غازي حنون خلف الدراجي، استظهار القصد الجنائي في جريمة القصد العمد، منشورات الحلبي الحقوقية، ط1، لبنان، 2012.

7. ميلود عبد الرحمن، الإجراءات الإحترازية الدولية في مواجهة خطر الإرهاب الإلكتروني، التجربة الفرنسية نموذجا، ورقة علمية مقدمة إلى المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية الذي نظمته كلية الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية، 2015.

المراجع باللغة الأجنبية:

1. Cherif Bassiouni " the modalities of international cooperation in penal matters in international criminal law 3rd Edition Martinus Nijhoff Publishers 2008 Vol 2 .
2. Sossin, Lome and Yetnikoff, Zimura, I Can See Clearly Now: Videoconference Hearings and the Legal Limit on How Tribunals Allocate Resources (August5. 2007). Windsor Yearbook of Access to Justice, 2007.

المواقع الإلكترونية:

1. الإنتربول: تقرير للإنتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أي وقت مضى، أغسطس 2020. متاح على:
https://www.interpol.int/ar/1/1/2024/03/12

2. لاتحاد الدولي للاتصالات: نشر مقدرات الأمن السيبراني – مركز الإنذار العالمي التابع لهيئة IMPACT، جنيف، أبريل 2009. متاح على:
Shanghai Cooperation Organization: Agreement on Cooperation in the Field of International Information Security between the Member States of the Shanghai Cooperation Organization, Shanghai, June 2009.
Available at:
http://eng.sectsco.org/load/207508/

3. مروة نظير :هل المجتمع الدولي بحاجة إلى تشريع جديد بخصوص الجرائم السيبرانية؟، العين الإخبارية، 5 يناير 2023.
متاح على :https://al-ain.com/article/united-nations-china-russia

4. المنظمة الدولية للشرطة الجنائية، عرض عام الانتربول 10.30 2024/05/28
https://www.interpol.int/ar/3/10

https://www.asjp.cerist.dz/en/downArticle/65/11/1/59399 التصفح بتاريخ 22:00
https://undocs.org/ar/S/2024/02/03متاح على: 2024/04/20

5. الجمعية العامة للأمم المتحدة استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب A/RES288/60/، مكتب مكافحة الإرهاب الدورة الستون 2006متاح على https://undocs.org/ar/A/RES/60/288:

6. مجلس الأمن مبادئ مدريد التوجيهية لوقف تدفق المقاتلين الإرهابيين الأجانب 939/2024/5، مدريد، ديسمبر 2015.

فهرس المحتويات

فهرس المحتويات	الصفحة
شكر وعرفان	/
إهداء	/
مقدمة	1-5
الفصل الأول: الإطار المفاهيمي لجريمة الإرهاب الإلكتروني	
تمهيد:	**7**
المبحث الأول: الإطار المفاهيمي لجريمة الإرهاب الإلكتروني	**8**
المطلب الأول: مفهوم وأساليب ارتكاب جريمة الإرهاب الإلكتروني	**8**
الفرع الأول: تعريف جريمة الإرهاب الإلكتروني وخصائصها	**8**
أولا: تعريف الإرهاب الإلكتروني	**8**
ثانيا: تعريف الإرهاب في المعاهدات والتشريعات الوطنية	**8**
ثالثا: خصائص جريمة الإرهاب الإلكتروني	**11**
الفرع الثاني: أساليب ووسائل ارتكاب جرائم الإرهابية الالكترونية	**12**
أولا: أساليب إرتكاب جرائم الإرهاب الإلكتروني	**12**
ثانيا: وسائل إرتكاب جرائم الإرهاب الإلكتروني	**14**
المطلب الثاني: أركان وصور جريمة الإرهاب الإلكتروني	**14**
الفرع الأول: أركان جريمة الإرهاب الإلكتروني	**14**
أولا: الركن الشرعي	**15**
ثانيا: الركن المادي	**16**
ثالثا: الركن المعنوي	**20**
الفرع الثاني: صور جريمة الإرهاب الالكتروني	**23**
أولا: الصور التقليدية للإرهاب الالكتروني	**23**
ثالثا: الحروب الإعلامية وغسيل الأموال	**24**
ثالثا: الصور الحديثة للإرهاب الالكتروني	**24**
المبحث الثاني: الأحكام الإجرائية لجريمة الإرهاب الالكتروني	**25**
المطلب الأول: الإجراءات التقليدية لإثبات جريمة الإرهاب الإلكتروني	**25**
الفرع الأول: التسرب واعتراض المراسلات في جريمة الإرهاب الإلكتروني	**26**
أولا: التسرب	**26**

ثانيا: اعتراض المراسلات	**29**
الفرع الثاني: المراقبة الإلكترونية وحفظ البيانات في جريمة الارهاب الالكتروني	**31**
أولا: المراقبة الإلكترونية	**32**
ثانيا: حفظ المعطيات المتعلقة بحركة السير	**35**
خلاصة	**38**
الفصل الثاني:آليات مكافحة جرائم الإرهاب الإلكتروني	
تمهيد	**40**
المبحث الأول: دور الآليات الإقليمية والدولية في مكافحة جريمة الإرهاب الإلكتروني	**41**
المطلب الأول: دور المنظمات والإتفاقيات في مكافحة الإرهاب الإلكتروني	**41**
الفرع الأول: دور الإتفاقيات الإقليمية لمكانة الإرهاب الإلكتروني	**42**
أولا: اتفاقية بودابست لمكافحة جرائم الإنترنت	**42**
ثانيا:الاتفاقية العربية لمكافحة جرائم تقنية المعلومات	**42**
الفرع الثاني: دور المنظمات الإقليمية لمكافحة الإرهاب الإلكتروني	**43**
أولا: الاتحاد الأوروبي:	**43**
ثالثا: جامعة الدول العربية	**44**
المطلب الثاني: دور المنظمات الدولية والإقليمية وجهودها في مكافحة الإرهاب الإلكتروني	**45**
الفرع الأول : دور المنظمات الدولية لمكافحة الإرهاب الإلكتروني	**46**
أولا: دور منظمة الأمم المتحدة والهيئات التابعة لها	**46**
ثانيا: الهيئات المرتبطة بمنظمة الأمم المتحدة.	**46**
الفرع الثاني: دور الاتفاقيات الدولية لمكافحة الإرهاب الإلكتروني	**48**
أولا: دور الإتفاقيات	**48**
ثانيا: العوامل المؤثرة على دور المنظمات الدولية والإقليمية في مكافحة الإرهاب الإلكتروني	**51**
المبحث الثاني: التعاون الدولي في مكافحة جريمة الإرهاب الالكتروني	**54**
المطلب الأول: التعاون الأمني في مكافحة جريمة الإرهاب الالكتروني	**54**
الفرع الأول: التعاون الأمني على المستوى الدولي	**55**
أولا: المنظمة الدولية للشرطة الجنائية الانتربول	**55**
ثانيا: المنظمة الإفريقي الإقليمية للشرطة الجنائية افروبيول:	**56**
ثالثا: منظمة اليوروبول لمكافحة جريمة الإرهاب الإلكتروني	**58**
الفرع الثاني: التعاون الأمني على المستوى العربي	**59**

أولا: الأجهزة المختصة في مكافحة جريمة الإرهاب الإلكتروني	**59**
ثانيا: التعاون الامني في التشريعات الداخلية	**62**
المطلب الثاني: التعاون القضائي في مكافحة جريمة الإرهاب الإلكتروني	**66**
الفرع الأول: الآليات التقليدية للتعاون القضائي في مكافحة جريمة الإرهاب الالكتروني	**67**
أولا: تسليم المجرمين في جريمة الإرهاب الالكتروني	**67**
ثانيا: المساعدة القضائية المتبادلة وتنفيذ الأحكام الأجنبية	**70**
الفرع الثاني: الآليات المستحدثة للتعاون القضائي في مكافحة جريمة الارهاب الالكتروني	**73**
أولا: ماهية تقنية التحقيق الجنائي عن بعد	**74**
ثانيا : الإطار القانوني لتقنية التحقيق الجنائي عن بعد (فيديو كونفرنس)	**77**
خلاصة الفصل الثاني	**82**
خاتمة	**84**
قائمة المصادر والمراجع	/
ملخص	/

ملخص

تهدف هذه الدراسة إلى تبيان مختلف الجهود المبذولة الوقائية منها والردعية لمكافحة جرائم الإرهاب الإلكتروني، حيث تتميز هذه الجهود بين الطابع الدولي والوطني، والتي من خلالها كان الاهتمام بمكافحة هذا النوع من الأفعال الإجرامية الخطيرة والمستحدث على المستويين الدولي والوطني، ولهذه الدراسة أهمية كبيرة تتمثل في أن الإرهاب الإلكتروني هو خطر يهدد على حد سواء سلامة الكيان الطبيعي والكيان المعنوي، فجريمة الإرهاب الالكتروني تستفيد بشكل سلبي من تطور تقنية المعلومات والشبكات العنكبوتية التي هي المورد الهام والأساسي في ارتكاب الجريمة الإرهابية والرقم–ية، مما حتم على الدول مجتمعة ومنفردة إعادة النظر في آلياتها الوقائية وكذا الردعية لمكافحة هذا النوع الخطير من الإجرام العابر للحدود بمختلف الأساليب والطرق.

فقد خلصنا إلى أن هذه الجهود والآليات تلعب دورا هاما وفعال في مجابهة الإرهاب الإلكتروني، إلا أنه وبالرغم من ذلك لا تزال هذه الظاهرة الإجرامية قائمة وتعاني منها جل الدول وكذا الأفراد على حد سواء، مما يستوجب إيجاد وسائل تكون أكثر وقائية.

الكلمات المفتاحية: الإرهاب الإلكتروني، الجريمة الإلكترونية، مكافحة الإرهاب الإلكتروني.

Abstract:

This study aims to elucidate the various preventive and deterrent efforts undertaken to combat cyber terrorism. These efforts are characterized by both international and national dimensions, underscoring the significant attention given to combating this type of serious and novel criminal activity at both levels. The importance of this study lies in the fact that cyber terrorism poses a threat to both physical and intangible entities. Cyber terrorism crimes exploit the advancements in information technology and the internet, which serve as crucial resources for committing such terrorist and digital crimes. Consequently, it has become imperative for states, collectively and individually, to reassess their preventive and deterrent mechanisms to combat this dangerous form of transnational crime through various means and methods.

We conclude that these efforts and mechanisms play an essential and effective role in confronting cyber terrorism. However, despite these efforts, this criminal phenomenon persists, affecting most countries and individuals alike, necessitating the development of more preventive measures.

Keywords: cyber terrorism, cyber crime, combating cyber terrorism