جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

واقع الارهاب الالكتروني واليات مكافحته

مذكرة مكملة لنيل شهادة الماستر في الحقوق

تخصص : حوكمة ومكافحة الفساد

إعداد الطالبتين:

- بن مولاي هجيرة
- متيجي هاجر

إشراف الدكتور.

لحاق عيسى

لجنة المناقشة :

د: رزق الله العربي	رئيسا
د: لحاق عيسة	مشرفا ومقررا
د: ناج عطاء الله	مناقشا

السنة الجامعية :2024-2025

مقدمة

مقدمة

مقدمة

تُعتبر الظاهرة الإرهابية قديمة قدم الإنسانية، حيث استُخدمت على مدى عقود كوسيلة لإثبات وجهات النظر وفرضها، وتمرير الأفكار والسياسات والإيديولوجيات، سواءً من خلال إحداث تغييرات أو مقاومتها، أنها آلية متاحة لجميع الأطراف الفاعلة على الصعيدين الداخلي والدولي، رغم اختلاف أساليب توظيفها والتبعات الناتجة عنها، ومع ذلك، لم تتجلى هذه الظاهرة بأكثر صورها عنفًا ودموية إلا مع بداية القرن التاسع عشر، حيث بدأت تُستخدم بشكل مقلق وبأسلوب أكثر راديكالية، مما أسفر عن مآسٍ تركت بصماتها في تاريخ البشرية، وأثارت رعبًا واسع النطاق. وقد وثقت ذاكرة التاريخ وأخبار الرواة وشهادات العيان صورًا مروعة للإرهاب العنصري الذي مارسته القوى النازية في أوروبا الغربية قبل وأثناء الحرب العالمية الثانية، بما في ذلك مجازر الهولوكوست. كما شهدنا بعض هذه الأحداث في أواخر القرن الماضي، مثل هجمات الحادي عشر من سبتمبر 2001، والعنف الدموي الذي عانت منه الجزائر خلال ما يُعرف بالعشرية السوداء.

فالظاهرة الإرهابية هي الهاجس الأكبر الذي يؤرق البشرية جمعاء، إذ انه يمثل التهديد الأكبر للدول في وجودها وبنيتها ومقوماتها واستقرارها وهي من أبرز الظواهر التي تزعزع وتهدد الأفراد في أمنهم المادية والنفسي، وهي في الوقت ذاته خطر داهم يعصف بالعلاقات الدولية والاستقرار والأمن الدوليين، فهي إذا ظاهرة تضع العالم أجمع أمام تحديات حقيقية يتعين عليه رفعها والتعامل معها بقدر كبير من المسؤولية.

يعترف الواقع بأن الثورة الصناعية والتطور التكنولوجي الذي شهدته القرن الثامن عشر، والذي استمر تأثيره حتى اليوم، قد أسهم بشكل كبير في ظهور أشكال متطورة من الظاهرة الإرهابية. وتتميز هذه الأشكال بكونها تشكل تهديدًا خطيرًا للحياة البشرية مقارنة بالصور التقليدية للإرهاب. فقد برزت أنواع جديدة مثل الإرهاب البيولوجي والنووي والإشعاعي والكيماوي، وهي أشكال تحمل مخاطر جسيمة وتأثيرات مدمرة. ومع دخول عصر مجتمع المعلومات وزيادة انشغال الناس بفضاء المعلومات والاتصالات، ظهرت صورة جديدة من الإرهاب لا تقل خطورة عن سابقاتها، وهي الإرهاب الإلكتروني، الذي يُعتبر تهديدًا جديًا للأمن والسلم العالميين.

لقد تكيف الفكر الإرهابي والعناصر التي تتبناه مع التداخل الحاصل بين تكنولوجيا المعلومات وتكنولوجيا الاتصال، مما أوجد فضاءً إلكترونيًا واسعًا يجمع بين حاضر البشرية ومستقبلها. أصبح هذا الفضاء ساحةً للحروب الناعمة والصلبة على حد سواء، وميدانًا للصراعات بين القوى الفاعلة، سواء كانت دولًا أو غير دول، بشكل متساوٍ، يتم ذلك من خلال استخدام مجموعة من الأسلحة الإلكترونية الفتاكة التي قد تترك وراءها دمارًا هائلًا يمكن أن يؤدي إلى انهيار الدول، نظرًا للارتباط الوثيق بين أمنها القومي وهذا الفضاء الحيوي في العديد من المجالات الاستراتيجية.

مقدمة

ومع ظهور الفضاء الإلكتروني، أصبح العالم يواجه واقعًا جديدًا يتمثل في تحولات كبيرة أثرت بشكل عميق وحساس على جميع جوانب الحياة الإنسانية، بما في ذلك السياسة والاقتصاد والتجارة والأعمال والإدارة. وقد أجبرت هذه التغيرات الدول على إعادة تقييم العديد من المفاهيم الأمنية والسياسية والقانونية. وأصبح من الضروري أن تتبنى الدول مفاهيم جديدة، خاصة فيما يتعلق بالتحديات الأمنية الناجمة عن الأنشطة الإرهابية والتخريبية في الفضاء الإلكتروني.

ومن بين هذه المفاهيم الجوهرية التي تمخضت عن هذا الفضاء الإلكتروني، مفهوم الإرهاب الإلكتروني، والذي حاول الباحثون والدارسون الوصول إلى تعريف جامع ومانع له، مستبصرين في ذلك بما يمكن أن يشتمل عليه من خصائص وما يمكن أن يميزه من مميزات، وما قد يكون عاملا منشأ له فكان أن أخذ كل منهم في ذلك مسلكه، فتعددت نحلهم وتوجهاتهم، وتناقضت آراؤهم وأفكارهم، وتضاربت تصوراتهم ومداركهم، وجرى على مفهوم هذا النوع من أنواع الإرهاب ما جرى على الظاهرة الإرهابية بشكل عام من اضطراب في المفهوم.

وتكمن أهمية دراسة هذا الموضوع في كونه موضوع جديد فهو يعبر عن الإرهاب لكن بالطريقة المعاصرة، حيث أنه يرتبط ارتباطا وثيقا بتقنية المعلومات ومن المهم التطرق والتعرف عليه من أجل تحذير الفئات التي يستهدفها وإعلامهم بالمخاطر التي تنجم عنه خاصة أنه يتميز بسرعة الانتشار وعبوره للحدود الإقليمية.

وتهدف هذه الدراسة إلى التعريف بموضوع الإرهاب الالكتروني وتميزه عن الإرهاب العادي وباقي الجرائم الأخرى المشابهة له، وتهدف أيضا إلى التعرف على الاليات الدولية والاقليمية وكذا الوطنية المسخرة من اجل مكافحة الارهاب الالكتروني

وقد دفعنا إلى اختيار هذا الموضوع أسباب شخصية نظرا لكونه من المواضيع الحديثة على الساحة الإجرامية ومن المهم تسليط الضوء عليه أما فيما يخص الأسباب الموضوعية هو الإلمام بجميع الجوانب التي تعرفنا بهذا الموضوع والإحاطة بمختلف الأليات والجهود المبذولة في مكافحة الإرهاب الالكتروني.

ما فيما يخص الصعوبات التي واجهتنا تشعب الموضوع وصعوبة الإلمام بمختلف جوانبه فضلا على اختلاط الأبعاد السياسية مع المقاربات القانونية لتداخله بالقانون الدولي كونه ظاهرة اجرامية عابرة للحدود مما جعلنا نلتزم بالتركيز على الجانب القانوني أكثر منه سياسي وقد انعكس ذلك حتى على مستوى المادة العلمية للبحث، بحيث وجدنا صعوبة كبيرة في إيجاد المراجع التي تتركز على الجوانب القانونية المحصنة.

ومما سبق لنا ذكره توصلنا إلى طرح الإشكالية التالية: إلى أي مدة كرس المجتمع الدولي والمسرع الوطني اليات لمكافحة الارهاب الالكتروني؟

وللإجابة على هذه الإشكالية اتبعنا المنهج الوصفي الذي قمنا من خلاله بوصف جريمة الإرهاب الالكتروني عن طريق التوصل إلى بعض التعريفات الخاصة به وذكر ما يميزه عن المصطلحات المشابهة له كما دعمناه بالمنهج التحليلي وذلك بذكر الاتفاقيات الدولية والاقليمية وكذا الاليات الوطنية من خلال النصوص التي خصصت لهذه الجريمة.

وعليه تم تقسم الدراسة إلى فصلين خصصنا الفصل الاول إلى مفهوم الارهاب الالكتروني، حيث تطرقنا من خلال هذا الفصل إلى تعريف وخصائص الإرهاب الالكتروني في المبحث الاول، ثم اركان جريمة الارهاب الالكتروني في المبحث الثاني.

اما الفصل الثاني فقد كان موضوعه سبل وآليات مكافحة الجريمة الارهابية الالكتًرونية، حيث تطرقنا في المبحث الأول إلى الجهود الدولية لمكافحة الارهاب الالكتروني، ثم الجهود الوطنية لمكافحة الارهاب الالكتروني في المبحث الثاني.

الفصل الأول :

مفهوم الارهاب

الالكتروني

الفصل الاول :مفهوم الارهاب الالكتروني

أدت ثورة المعلومات والاتصالات الحديثة، وما رافقها من تطور علمي وتكنولوجي رهيب إلى ظهور أشكال جديدة من الإجرام، والتي من بينها الإرهاب الالكتروني الذي يعتبر النسخة الالكترونية للإرهاب التقليدي .

حيث استغل المجرمون المزايا التي توفرها البيئة التقنية لتنفيذ شتى العمليات الإرهابية، سواء كان ذلك عن طريق استخدام شبكة الانترنت ووسائل التواصل الاجتماعي لتجنيد الأشخاص وتدريبهم أو إنشاء المواقع الالكترونية التي تثبت الأفكار الضالة والهدامة أو ببث البيانات والتصريحات والأفلام المصورة التي تعلمهم كيفية صناعة الأسلحة والمتفجرات والقيام بالعمليات الانتحارية ، أو من خلال القيام بتدمير البني التحتية للدول والمنظمات، وهذا عن طريق اختراق الشبكات السلكية واللاسلكية، وذلك بنشر الفيروسات والبرامج الخبيثة لتدمير الأنظمة المعلوماتية الخاصة بها أو توقيفها عن العمل، وهذا من أجل بث ونشر الرعب والخوف للإخلال بالوضع الأمني أو الاستقرار السياسي أو الوحدة الوطنية أو إدخال الخوف والفزع بين المواطنين، لتحقيق أغراض سياسية أو عقائدية أو إيديولوجية أو اقتصادية .

وعليه سوف تطرق من خلال هذا الفصل إلى تعريف وخصائص الإرهاب الالكتروني في المبحث الاول، ثم اركان جريمة الارهاب الالكتروني في المبحث الثاني.

المبحث الأول: تعريف وخصائص الإرهاب الالكتروني

إن تحديد المفاهيم يعّد من الاشكاليات التقليدية في الدراسات الانسانية، لاسيما في حقل العلوم السياسية، ولغرض تغطية جوانب الموضوع بشيء من التفصيل، فضلا عن محاولة توضيح راي المختصين حول التأصيل النظري لمفهوم الارهاب الالكتروني، لابد من البحث في مفهوم الارهاب والارهاب الالكتروني في المطلب الاول، ثم خصائص واهداف الارهاب الالكتروني في المطلب الثاني.

المطلب الأول: تعريف الإرهاب الإلكتروني

لقد تعالت مؤشرات الجرائم على مستوى الدولي في القرن الأخير نتيجة ظهور الثورة المعلوماتية، وإفرازها لعديد من الجرائم المستحدثة التي لم يسبق وان عرفها العالم، إذ تعتمد على أساليب متطورة مما أدى إلي تزايد أخطارها وعلى راسها الإرهاب الالكتروني.قبل التعرض إلى تعريف هذا الأخير باعتباره جريمة عصرية توجب علينا أولا التطرق إلي تعريف الجريمة التقليدية للإرهاب، باعتبار الإرهاب الالكتروني امتداد لها.

الفرع الأول: مدلول الظاهرة الإرهابية.

سوف نعرض من خلال هذا الفرع تعريف الارهاب لغة ثم اصطلاحا.

أولاً: تعريف الإرهاب لغة.

الإرهاب لغة من أرْهَبَ، يُرْهب، وأصله رَهَبَ، يُرهبُ. ويقال: رَهَبتُ الشيء رُهباً أي: خفته[1]

وكما ورد في لسان العرب: رَهَبَ، يَرْهَبُ، رَهْبَة وَرُهْباً، أي خَافَ. ورَهَبَ الشيء رُهْبَاً أي خافه، وأرْهَبَه واسْتَرهَبَهُ أي أفْزَعَه. أما تَرَهبَ الرجل أي صار رَاهباً يخشى الله. والراهبُ المتعبد في الصومعة، ومصدره الرهبة والرهبانية[2]

ولقد وردت كلمة الإرهاب في القران الكريم في قوله تعالى: "يا بني إسرائيل اذكروا نعمتي التي أنعمت عليكم وأوفوا بعهدي وإياي فارهبون"[3]، أي خَافُون.

أما في اللغة الفرنسية فيرجع مصطلح الإرهاب Terrorisme في الثقافة الغربية إلى نوع الحكم الذي لجأت إليه الثورة الفرنسية أثناء الجمهورية الجاكوبية ضد البرجوازيين والملكيين المناهضين للثورة أين كان

---

[1] باخوية دريس، **جرائم الإرهاب في دول المغرب العربي**(تونس، الجزائر، والمغرب أنموذجاً)، مجلة دفاتر السياسة والقانون، المجلد06، العدد 11، 2014، ص100

[2] أحمد أبو الوفا، **ظاهرة الإرهاب على ضوء أحكام القانون الدولي العام**، مجلة البحوث والدراسات العربية، العدد السابع عشر، 1990، ص: 75.

[3] أبو الفضل ابن منظور، **لسان العرب**، المجلد الأول، الطبعة الثالث، مادة (رهب)، بيروت، لبنان، ص: 436.

يطلق عليها(Reign of terrorisme) عندما تم اعتقال ما يزيد عن 200 ألفا وإعدام 18 ألف وموت ما يزيد عن عشرات الآلاف في السجون دون محاكمة[1]

في حين ترى **"موسوعة السياسة "** التي تضمنت شرحا مفصلا مدعوما بأمثلة عن الإرهاب، حيث عرفته على أنه استخدام العنف غير القانوني أو التهديد به بأشكاله المختلفة بغية تحقيق هدف سياسي معين، أو هو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية، كما تشير الموسوعة إلى أن الإرهاب ليس وسيلة متفقا على استخدامها، ولا تقره معظم الحركات السياسية، بحيث تنظر إليه على أنه كفاح شعبي ووسيلة مشروعة وسليمة لمقاومة العدوان وتحقيق مبدأ تقرير المصير الذي أقره القانون الدولي ونص عليه ميثاق الأمم المتحدة[2].

ثانياً: تعريف الارهاب اصطلاحا.

الإرهاب هو محاولة نشر الفزع والذعر لأغراض سياسية عادة[3]

ويراد به: "استعمال العنف غير القانوني أو التهديد به، وبأشكاله المختلفة كالإغتيال والتشويه والتعذيب والتخريب بغية تحقيق هدف سياسي معين".

ولقد ورد في موسوعة علم العلاقات الدولية بأن الإرهاب يتمثل في: "جميع النشاطات التي تقوم بها الدولة أو غير الدولة، ويتم فيها استخدام العنف قصد تحقيق أهداف سياسية محددة"

وانطلاقاً من مجموع المفاهيم المذكورة أعلاه يتبين بأن مفهوم الإرهاب يرتبط بالعنف أو التهديد به والفزع والخوف قصد تحقيق غرض معين غالباً ما يكون سياسياً.

ثالثا: مدلول الظاهرة الإرهابية فقهياً.

إنَّ الإرهاب يختلط في كثير من الأحيان بظاهرة العنف أو التطرف، ويرتبط في أذهان الكثيرين بديانة محددة أو جنسيات معينة على غير الحقيقة. والأكثر أهمية أن تشابكاته قد تجاوزت حدود الدول لتتخذ أبعادها إقليمية ودولية هامة، وتكمن أهمية تحديد المفهوم للظاهرة الإرهابية وتعريفها في أنه: إذا تمَّ تحديدها فإنَّ من السهل بعد ذلك التعرف على الممارسين للإرهاب باعتبار أنهم إذا قاموا بالأعمال الموضحة والُمحددة في التعريف، فإنهم يدخلون ضمن فئة الإرهابيين.

كما أنَّ الواقع يبين أنَّ الظاهرة الإرهابية هي ظاهرة سلبية تهدد السلم والأمن على المستويين الداخلي والخارجي، مما يتعين على الدول نبذ الخلافات والتباينات والانقسامات في الموقف على المستوى

---

[1] عباس شافعة، **الظاهرة الارهابية بين القانون الدولي والمنظور الديني**، اطروحة دكتوراه في علوم القانون، تخصص قانون دولي وعلاقات دولية، جامعة الحاج لخضر، 2010-2011، ص 17

[2] الجهماني ثامر إبراهيم ، **مفهوم الإرهاب في القانون الدولي، دراسة قانونية ناقدة**، ط1 ، دار الكتاب العربي، الجزائر، 2002، ص17

[3] بن أبي بكر الرازي محمد ، **مختار الصحاح**، (مادة رهب)، 1962، ص: 255.

الدولي لإيجاد تعريف واحد له على المستوى العالمي، والتخلُّص من الفوضى المفهوماتية للإرهاب الذي عرفته البشرية، وازداد حِدً في بداية القرن الحالي[1].

لا يوجد إجماع لدى الفقه القانوني بخصوص إعطاء تعريف موحد لظاهرة الإرهاب، نظراً لغموض وتداخل أركان هذه الظاهرة مع ظواهر إجرامية أخرى، لقد ساهم الفقه بطريقة أو بأخرى وبالخصوص فقهاء القانون الدولي من أجل تعريف الإرهاب وتحديد طبيعته، لكن هذه الجهود غير كافية للإلمام بظاهرة الإرهاب من جذورها بسبب التركيز على الجانب القانوني دون الاهتمام بالجوانب الأخرى كالجوانب الاجتماعية، النفسية، الاقتصادية وحتى السياسية والعقائدية.

كما أن الفقهاء تأثروا بطريقة أو بأخرى باتجاهات دولهم في نظرهم للإرهاب، لذلك فسوف أتطرق إلى تعريف الإرهاب عند فقهاء العرب ثم عند فقهاء الغرب.

1. **الإرهاب عند فقهاء العرب:** يرى الدكتور عبد العزيز سرحان بأن الإرهاب يتمثل في: "كل اعتداء على الأرواح أو الممتلكات أو الأموال العامة أو الخاصة، يقع بالمخالفة لأحكام القانون الدولي بمصادره المختلفة، بما في ذلك المادة 38 من النظام الأساسي لمحكمة العدل الدولية"[2]

لذلك فقد اعتبر هذا التعريف الإرهاب جريمة دولية مخالفة للقانون الدولي مهما كان الفاعل فردا أو جماعة أو دولة، كما توسع في مفهوم الإرهاب واعتبر التمييز العنصري جريمة إرهابية.

أ. الدكتور صلاح الدين عامر: عرف الإرهاب بأنه "الاستخدام المنظم للعنف لتحقيق هدف سياسي وبصفة خاصة جميع أعمال العنف (حوادث الاعتداء الفردية أو الجماعية أو التخريب) التي تقوم منظمة سياسية بممارستها على المواطن لخلق جو من اللا أمن وينطوي على طوائف متعددة من الأعمال أظْهرها أخذ الرهائن واختطاف الأشخاص وقتلهم ووضع المتفجرات أو العبوات الناسفة في أماكن تجمع المدنيين أو وسائل النقل العامة وتخريب وتغيير مسار الطائرات بقوة" .

لذلك فقد اعتبر الدكتور صلاح الدين عامر أنَّ أي استخدام منظم للعنف الذي يخلق لدى المواطن جوا من اللا أمن واللا استقراربهدف تحقيق أغراض سياسية يعد عملا إرهابيا مهما كانت المنظمة التي ارتكبته.

ب. الدكتور عبد الوهاب حويمد: يرى أن: "الإرهاب مذهب يعتمد للوصول إلى أهدافه على الذعر والإخافة وهذا المذهب ذو شقين: شق اجتماعي يرمي إلى القضاء على نظام الطبقات القائم بمجموعه وتحت مختلف أشكاله، فيكون النظام الاجتماعي بمجموعه هدفا مباشرا له.

وشق سياسي يهدف إلى تغيير أوضاع الحكم رأسا على عقب ولا يتردد في ضرب ممثلي الدول ذاتها"، لذلك فقد اعتبر الدكتور عبد الوهاب حويمد أن كل ما يخلق الخوف والهلع هو إرهاب.

---

[1] عباس شافعة، المرجع السابق، ص 13

[2] باخوية دريس، المرجع السابق، ص 101

كما اعتبر أنَّ الإرهاب له شقّانْ: أحدهما اجتماعي يهدف إلى القضاء على نظام الطبقية بمختلف أشكاله مما يؤدي بالإرهابيين إلى وضع النظام الاجتماعي كهدف أساسي مباشر لتحقيق مآربهم.[1]

وشق سياسي هدفه الإطاحة أو تغيير نظام الحكم في دولة ما وجعل كل من يقف مع النظام هدفا لهم يستوجب القضاء عليه لتحقيق مبتغاهم.[2]

2. الإرهاب عند فقهاء الغرب:وفيما يلي نورد بعض التعريفات لبعض الجهود الفقهية والتي من بينها ما أورده "رولان غوشيه" الذي اعتبر الإرهاب بأنه: "اللجوء إلى أشكال من القتال قليلة الأهمية بالنسبة للأشكال المعتمدة في النزاعات التقليدية، ألا وهي قتل السياسي أو الإعتداء على الممتلكات"[3]

اورد كارلوس مارجيللا تعريف للإرهاب في مضمونه أنه نشاط يجب أن تقوم به العصابات المدنية بأقصى درجة من درجات البرودة والإصرار، ولا يستطيع أي ضابط شرطة أو مشرع أو فيلسوف أن يصف جوهر الإرهاب بشكل أفضل من ذلك، فالهجمات تتم بلا رحمة من حيث طبيعتها، ولكنها تكون محسوبة من حيث تأثيرها على المجتمع كله[4]

الفرع الثاني: مدلول الإرهاب الالكتروني

إذا سلمنا بفكرة مفادها أن مفهوم الإرهاب كمصطلح تقليدي أصبح واضح إلى حد ما، فإن الارهاب الإلكتروني كمفهوم مستحدث يكتنفه الكثير من الغموض، وذلك أنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه ومن حيث دور الفاعل فيه وطبيعة سلوكه.[5]

وان غياب تعريف موحد لإرهاب متعمد إن صح التعبير وذلك بسبب عدم رغبة الدول في تقديم تعريف شامل من اجل سد الثغرات والفراغ القانوني الذي صاحب التطور التكنولوجيا المعلومات السريع، لذلك غالبا ما نجد التعريفات تأتي فضفاضة غير محددة من اجل إمكانية احتوائها لأي فعل من الأفعال الإرهابية الجديدة ممكنة الحدوث، ويستنبط تعريف الإرهاب الالكتروني من التعريفات السابقة للإرهاب العام، حيث نلاحظ أن مبدأ تجريم الإرهاب واحد وهو العنف والتهديد.

أولا: المقصود بالإرهاب الالكتروني:

يعترف الجميع بصعوبة إعطاء مفهوم محدد للإرهاب، نظرا لعدم وجود اتفاق موحد بين المختصين حول هذا المصطلح المعقد ذو الطبيعة المتغيرة، ويرجع ذلك حسب البعض لتداخل مفهوم الإرهاب مع مفاهيم أخرى، كالعنف السياسي أو الجريمة السياسية أو الجريمة المنظمة، كما أنه مفهوم

---

[1] عباس شافعة، المرجع السابق، ص 21

[2] نفس المرجع، ص 22

[3] مجمع اللغة العربية، **المعجم الوسيط**، ج01، دار عمران للطباعة والنشر، القاهرة، ص39.

[4] عباس شافعة، المرجع السابق،ص 23

[5] المناعسة أسامة احمد، الزعبي جلال محمد، **جرائم التقنية نظم المعلومات الالكترونية، دراسة مقارنة**، ط2 ، دار الثقافة لنشر والتوزيع، عمان، الأردن،2014، ص321

ديناميكي متطور تختلف أشكاله ودوافعه، باختلاف الأماكن والفترات الزمنية، لذا تعددت وتباينت مفاهيم الإرهاب، تبعا لتفاوت منطلقات الباحثين في الموضوع، إلا أن العامل المشترك بينها جميعا هو أن العمل الإرهابي ضرب من أعمال العنف التي تستهدف كيان المجتمع.[1]

مع أن الارهاب الالكتروني أصبح شائعا في السنوات الأخيرة، وبات خطرا كبيرا على الصعيد الدولي ولاسيما مع التطور السريع لتقنيات الاتصال واعتماد المتزايد للبشر على الانترنت، إلا انه لا يوجد لحد الآن تعريف عالمي متفق عليه لهذه الظاهرة، فقد تعددت التعريفات التي تناولته.

يتألف مصطلح الإرهاب الالكتروني من كلمتين كلمة(cyberterrorisem) وتعني الإرهاب ،ولقد ظهر هذا المصطلح (terrorisem) تعني الانترنت و(cyber) عقب التطورات الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسب الآلية والانترنت في الإدارة معظم شؤون الحياة .حيث نجد أن الغرب أول من تفطن لهذا الإرهاب الرقمي أو ما يسمى سيبراني أو المعلوماتي أو الشبكي حيث تعددت تسمياته، في فترة الثمانينات واقر "Barry Collin " فأول من استخدام كلمة الارهاب الالكتروني هو بصعوبة إعطاء تعريف شامل للإرهاب التكنولوجي وعرفه انه" هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو إيدلوجية وان الهجمة يجب أن تكون ذات أثر مدمرو تخريبي مكافئ للأفعال المادية للإرهاب"

وفي بداية التسعينات صدر تقرير عن الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر جاء فيه " :نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر، حيث غدا بإمكان الإرهابيين إحداث تدمير كبير بالاعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربر الكتروني جديد[2]

ولقد ظهر الإرهاب الالكتروني بشكل علني في الولايات المتحدة الأمريكية عندما قام الرئيس بيل كلينتون سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية، التي توصلت إلى أن مصادر الطاقة والاتصالات وكذا شبكات الكمبيوتر ستكون هدف الأول للهجمات الإرهابية، ولكن هذه الأخيرة لم تعرفه اكتفت بدراسة الظاهرة ومحاولة فهم سياسة تفكير الإرهاب الالكتروني والطرق التي يتخذها في تنفيذ عماليته بحيث تظهر الدراسة شغف، الإرهابيين في استخدام شبكة الانترنت في عملياتهم الإرهابية، مظهرين بذلك براعتهم في التفوق على أي تقنية مستخدمة[3].

---

[1] بن عمروش فريدة، **الإرهاب الالكتروني :دراسة في إشكالات المفهوم والأبعاد**، المجلة الجزائرية للعلوم الاجتماعية والإنسانية، المجلد08 ، العدد02، 2022، ص 218

[2] عبد الصادق عادل، **استخدام الإرهاب الالكتروني في الصراع الدولي**، دار الكتاب الحديث، القاهرة،2015 ، ص104

[3] نجاري بن حاج علي فايزة، **الاليات القانونية للإرهاب الالكتروني**، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2016 ، ص24

وفي هذا الصدد قامت وكالة المخابرات المركزية الأمريكية بتعريف الإرهاب الالكتروني على انه "أي هجوم تحضيري ذو دوافع سياسية موجهة ضد نظم المعلومات والتي تنتج عن العنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين".[1]

في حين عرفه مركز الحماية البنية التحتية القومية الأمريكية" انه عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية ولا السلكية ينتج عنه تدمير وتعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو ايدلوجية[2] ."

كما نلاحظ أيضا أن الاتحاد الأوربي بدوره يقر بجرائم الإرهاب الالكتروني من خلال الاتفاقية بودابست ولكنه لم يعرفه، اكتفى بتعريف الإرهاب بشكل عام سنة 2002 على انه" كل عمل يرتكب بهدف ترويع الأهالي، أو إجبار أو تدمير الهياكل الدستورية أو الاقتصادية أو الاجتماعية لدولة ما أو هيئة دولية ما أو زعزعة استقرارها"، وبعدما قامت دول الأعضاء بتعريفات غير موفقة للإرهاب الالكتروني أتي الاتحاد بهذا التعريف الشامل للإرهاب.[3]

حيث أن فرنسا عرفت الإرهاب الالكتروني على انه" كل هجوم الغرض منه الحصول على معلومات المرتبطة بالغير وإمكانياته واستراتيجياته التي يتخذها لدفاع عن نفسه أو تدمير نظم المعلوماتية أو نشر المعلومات الزائفة من اجل تضليله بتوظيف التكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنت[4]."

كما عرفته إيطاليا انه" كل جماعة إرهابية تستعمل الوسائل التكنولوجيا كالأنترنت من اجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق أو التبادل المهارات والخبرات والأساليب، أو جمع التبرعات من اجل تمويل عماليتهم الإرهابية[5]."

بإضافة إلى أن بعض الدول العربية أيضا حاولت إعطاء تعريف الإرهاب الالكتروني حيث عرفته مصر على انه" الاستخدام الغير القانوني للقوة أو الضعف ضد الأفراد وممتلكات بغية الإرهاب والتهديد لإرغام الحكومة أو السكان المدنيين أو أي فئة أخرى على القبول بهدف سياسي أو اجتماعي أو اقتصادي"

---

[1] عبد الصادق عادل، المرجع السابق، ص106

[2] مجاهد توفيق، عابسة طاهر، **جريمة الإرهاب في ضوء احكام الاتفاقية العربية لمكافحة جرائم التقنية المعلومات لعام 2010**، مجلة العلوم القانونية والسياسية، المجلد09 ، العدد03 ، ديسمبر2018 ، جزائر، ص82

[3] عبد الصادق عادل، مرجع سابق، ص106

[4] شاشوة ياسمينة، **الارهاب الالكتروني بين مخاطره واليات مكافحته**، مذكرة ماستر في الحقوق،، تخصص: قانون جنائي وعلوم جنائية، جامعة آكلي محند أولحاج، البويرة، الجزائر، 2019-2020، ص 14

[5] نفس المرجع

كما عرفته المملكة السعودية على انه" أي فعل يرتكب متضمن استخدام الحاسب الآلي أو شبكة المعلوماتية أو استخدام التقنيات الرقمية المخالفة لأحكام النظام ومن أنواعه السب، التشهير، والابتزاز، والإباحة وكذلك الشائعات وما يتعلق بأمور المالية كاعتداء على البطاقات البنكية بأشكالها واختلاسها[1]."

كما عرفه عادل عبد الصادق بأنه" يعني العدوان أو التخويف أو تهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة من دول أو جماعات أو الأفراد عبر الفضاء الالكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له[2] "

يعرف جينافو فيتش الإرهاب بأنه الأفعال التي من طبيعتها أن تثير قلقا لدى شخص ما من شعور بالتهديد، أو هي الأعمال التي تؤدي إلى التخويف والرعب بأي قدر وبأي وسيلة.[3]

وقد عرف بعض الفقهاء، الإرهاب الالكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان نفسه، بغير حق بشتى أنواعه وصور الإفساد في الأرض.[4]

وهناك من عرفه انه" هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا توجه من اجل الانتقام والابتزاز أو الإجبار أو التأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبتالي لكي يلقب الشخص ما بأنه إرهابي على الانترنت وليس مخترقا فقط فلا بد من أن تؤدي الهجمات التي يشنها إلي عنف ضد الأشخاص أو على الأقل تحدث أذى كافيا من اجل نشر الخوف والرعب[5] .

ولقد عرفه الفقه انه "خرق للقانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إثارة اضطراب خطير في نظام العام عن طريق شبكة المعلومات العلمية الانترنت ".[6]

ومن خلال ما تم عرضه نلاحظ أن كل المجتمع الدولي اقر واعترف بهذا التهديد الجديد، الذي يعتبر حديث العهد ولكنه سريع الانتشار والالتهاب بتسارع تقدم التكنولوجيا المعلومات والاتصالات الرقمية والانترنت، فلإرهاب الالكتروني حظي باهتمام كبير على مستوى المجتمع الدولي بآسره ولكن هناك من لم

---

[1] نجاري بن حاج علي فايزة، المرجع السابق، ص29 – 28

[2] عبد الصادق عادل، **الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة**، ط1 ، مركز الاهرام للدراسات السياسية والاستراتيجية2009 ، ص109

[3] سامي علي حامد عياد، **استخدام تكنولوجيا المعلومات في مكافحة الإرهاب**، دار الفكر الجامعي، مصر، 2008، ص 28

[4] ناظم نواف إبراهيم، **ظاهرة العنف السياسي في العراق المعاصر بعد الاحتلال الأمريكي**، أطروحة دكتوراه، معهد البحوث والدراسات العربية، القاهرة، مصر، 2009، ص 11

[5] الفيل علي عدنان، **الاجرام الالكتروني**، ط1 ، مكتبة زين الحقوقية والأدبية، لبنان،2011 ، ص60

[6] طارق جواد اسراء، الجابري كاظم، **جريمة الإرهاب الالكتروني**، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق،2012 ، ص23 .

يتطرق إلى تعريفه واكتفى بتحديد السلوكيات الإجرامية المرتكبة بتقنيات الحديثة وهذا ينطبق على الاتفاقيات والتشريعات الدولية ،ونلاحظ أن المشرع الجزائري هو الأخر اكتفي بتصدي لظاهرة الإرهاب باستخدام تكنولوجيات الإعلام والاتصال اثر تعديل قانون العقوبات بالقانون 16-02 وإضافة مادتين 87 مكرر 11 و 87مكرر 12 لمواجهة الإرهاب الالكتروني ولم يقدم تعريف لهذه الظاهرة[1]

ورغم كل التعريفات الواردة بحق الإرهاب الالكتروني إلا أنها تبقى غامضة وغير كاملة ولم يتم تناولها بشكل عملي جدي، وسنأخذ بالتعريف الأقرب لصواب وهو تعريف المجمع الفقه الإسلامي" العدوان أو تخويف أو تهديد ماديا ومعنويا باستخدام الوسائل الالكترونية الصادر من الدول أو جماعات أو أفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الفساد في الأرض[2]."

أما الاتفاقية الأولى لمكافحة الإجرام عبر الإنترنت في بودابست عام 2001 فقد عرفت الإرهاب الإلكتروني بأنه: " هجمات غير مشروعة أو تهديد بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجد من أجل الانتقام أو الابتزاز أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. [3]

وفي الأخير نستنتج أن الإرهاب الالكتروني هو كل فعل من أفعال العنف أو التهديد أي كانت بواعثه وأغراضه يقع تنديدا لمشروع إجرامي أو جماعي باستخدام وسائل الكترونية[4]

تعتمد التنظيمات والجماعات الإرهابية إلى إتباع عدة وسائل في سبيل تحقيق أهدافها ومآربها الإرهابية نستعرض أبرزها في الأتي :[5]

أ- **خدمة البريد الالكتروني:** يعد البريد الالكتروني خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات وتعد هذه الخدمة من أعظم الوسائل المستخدمة في الإرهاب الالكتروني من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، كما يقوم الإرهابيون باستغلال البريد الالكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الالكترونية، ومما يقوم به الإرهابيون أيضا اختراق البريد الالكتروني للآخرين وهتك أسرارهم

---

[1] غلاف كريمة، جرلال زوهرة، **جريمة الإرهاب الالكتروني**، مذكرة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، بجاية، 2018-2019، ص15

[2] امير فرج يوسف، **الجرائم الدولية للأنترنت**، ط1 ، المركز القومي للإصدارات القانونية، مصر،2011 ، ص139

[3] الساحي علام، فوزية حاج شريف، **واقع الإرهاب الإلكتروني اليات مكافحته**، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد . الأول، ص162- 163.

[4] عبد الصادق عادل، **الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة**، المرجع السابق، ص 109

[5] سليماني مباركة، **الإرهاب الالكتروني وطرق مكافحته**، مجلة الحقوق والعلوم السياسية العدد 08 ج 01 / جوان 2017، ص 346

والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

ب- اختراق وتخريب المواقع: هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع، ومن المعلوم أن لدى المؤسسات من الإمكانيات والقدرات ما ليس لدى الأفراد، وتتم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الانترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الالكترونية، ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي.[1]

ج- انشاء مواقع الانترنت: إن من أخطر وسائل الإرهاب الالكتروني إنشاء مواقع افتراضية تمثل التنظيمات الإرهابية وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة من منظمات أو جهات دولية أخرى، فالإرهاب الالكتروني يعتمد على استخدام الإمكانات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآمنين، وإلحاق الضرر بهم أو تهديدهم بما يضرهم.

د- التهديد والترويع الإلكتروني: تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي ولإبراز قوة التنظيم الإرهابي من ناحية أخرى، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد، وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية، ولقد تعددت الأساليب الإرهابية في التهديد فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية ونحو ذلك.[2]

هـ- التجسس الالكتروني: يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الإلكتروني بالطريقة العصرية المتمثلة في استخدام

---

[1] الزنط سعد عطوة، **الإرهاب الالكتروني واعادة صياغة استراتيجيات الأمن القومي، ورقة مقدمة إلى مؤتمر الجرائم المستحدثة :كيفية اثباتها ومواجهتها**"، المركز القومي للبحوث الاجتماعية والجنائية ،مصر، (15-16) ديسمبر 2010 ص 03 وما يليها

[2] سليماني مباركة، مرجع سابق، ص 347-348

الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية، وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي، وتجدر الإشارة إلى أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن[1]

ومن اهم الامثلة على توظيف التنظيمات الإرهابية لشبكات التواصل الاجتماعي نجد التنظيمان الإرهابيان القاعدة وداعش، حيث سخرت التنظيمات الإرهابية الشبكة الرقمية والفضائيات لأغراضها الدعائية، منذ شرع تنظيم القاعدة الإرهابي قبل نحو عقد من الزمن في بث بياناته عبر الانترنت وبعض القنوات التلفزيونية العربية والعالمية، حتى برز في السنوات الخمس الأخيرة نشاط "رقمي" فعال للجماعات المتطرفة لتسويق بياناتها وصور فعالياتها عبر مواقع التواصل الاجتماعي لاسيما "فيسبوك" و"تويتر"، في سعيها لتعزيز إستراتيجية "بروباغندا" لا يهدف إلى نشر ثقافتها المتطرفة و"التكفيرية" فحسب، بل إلى شن حرب نفسية للتأثير في الخصوم، والسعي إلى استقطاب الشباب للتطوع في صفوفها والقتال في البلدان التي تحارب فيها مثل افغانستان والعراق وسوريا واليمن ودول أخري، وفيما يتعلق بتنظيم القاعدة الإرهابي مثلا فهناك مواقع الكترونية تقوم بنشر أفكاره نذكر منها [2] موقع نداء الذي يعد الموقع الرسمي لتنظيم القاعدة الإرهابي أسس بعد أحداث 11 سبتمبر ومنه تصدر البيانات الإعلامية للقاعدة .

وكذا موقع ذروة الإسلام وهي صحيفة الكترونية دورية للقسم الإعلامي للقاعدة .

وتم انشاء موقع صوت الجهاد وهي مجلة الكترونية نصف شهرية يصدرها تنظيم القاعدة الإرهابي في جزيرة العرب، بالإضافة إلى موقع البتار هي مجلة عسكرية الكترونية متخصصة تصدر عن التنظيم الإرهابي وتختص بالمعلومات الميدانية والعسكرية والقتالية .[3]

أما تنظيم داعش الإرهابي فقد وظف الإعلام المرئي والمسموع لخدمه أهدافه الترويجية فعمل على إنشاء أذرع إعلامية له منها: ستديو "أجناد" حيث يتم فيه تسجيل الأناشيد الدينية والجهادية، المصاحبة لمقاطع الفيديو المصورة لعمليات التنظيم الإرهابي، وقناة "الفرقان" وتم تأسيسها بدعم من تنظيم القاعدة الإرهابي، وقناة "الاعتصام" التي تختص ببث المعارك في سوريا والعراق من خلال عدد من المراسلين، وقناة "الحياة" المتخصصة في إجراء الحوارات التليفزيونية مع قيادات التنظيم الإرهابي،

---

[1] سليماني مباركة، مرجع سابق، ص 348

[2] عبد الباهي الناهي أحمد، عبد الستار رشيد صدام، **السياسة الاعلامية لتنظيم داعش: الأهداف وسبل المعالجة**، المجلة السياسية والدولية، العراق: الجامعة المستنصرية، العدد30،2016، ص 27

[3] سليماني مباركة، مرجع سابق، ص 348

بالإضافة إلى قنوات موجهة للولايات المتحدة الأمريكية، حيث نجح التنظيم الإرهابي في السيطرة على بعض القنوات الفضائية في العراق وسوريا، إلى جانب إذاعة "البيان" التي يتم بثها في الموصل والأنبار في العراق والرقة في سوريا وعلى شبكة الانترنت.[1]

كما يسيطر تنظيم داعش الإرهابي كذلك على عدد كبير من المواقع والمنتديات الالكترونية التي تحتوي على مكتبة هائلة وواسعة تختص بالأيديولوجيا والخطاب وآليات التمويل والتجنيد والتدريب والتخفي والتكتيكات القتالية وصنع المتفجرات، وكل ما يلزم الجهاديين في عمليات المواجهة في إطار حرب العصابات وسياسات الاستشراف، ومن أهم الإصدارات التي كان لها وقع كبير على "موقع يوتيوب" إصدار "كسر الحدود" بتاريخ 29 جوان 2014، وخطبة البغدادي في الموصل بتاريخ 5 جويلية 2014، هذا ويعتبر فيلم "لهيب النار " من أضخم الإصدارات والأكثر دقة ورعبا ويتضمن تغطية لمعارك عديدة لتنظيم الدولة الإرهابي ورسالة موجهة لدول التحالف المشاركة في الحملة على التنظيم الإرهابي، وقد أصدره الجناح الإعلامي التابع للتنظيم الإرهابي الخاص باللغة الانجليزية "مركز الحياة " بتاريخ 17 سبتمبر 2014[2]

ثانيا: التمييز بين الإرهاب الإلكتروني وغيره من المفاهيم

نجد ان الارهاب الالكتروني بتداخل مع بعض المصطلحات التي تتداخل معه في المفهوم وهو ما سوف نوضحه من خلال العناصر الموالية :

1. التمييز بين الإرهاب الإلكتروني والمقاومة الإلكترونية

الإرهاب الإلكتروني هو من بين تجليات الحرب الإلكترونية وصورة من صورها، فهو ينطلق من الأسس والتصورات الإيديولوجية التي تتبناها الجماعة وتؤمن بها، وهدفه واضح ومحدد ويتمثل في تجسيد التصورات الإيديولوجية للجماعة الإرهابية وإدراجها في صيغتها المادية[3]، بينها المقاومة الإلكترونية هي تسخير القضاء الإلكتروني للقيام بالاحتجاج على أوضاع سائدة أو لدفع الظلم والاستبداد، وهي تقوم على أسس مشروعة معترف بها في القوانين والأعراف الدولية كالدفاع الشرعي والحق في تقرير المصير، فالفرق بين الإرهاب والمقاومة يتكشف بوضوح من خلال القصد الذي تسعى إلى تحقيقه، فالمقاومة تهدف إلى إزاحة اعتداء صدر عن محتل أو عن سلطة مستبدة، وغالبا ما يكون في إطار داخلي ولا يكتسب

---

[1] مكرم رانيا، "**الاعلام الجهادي : كيف وظفت التنظيمات الجهادية وسائل الاعلام ؟** "، المركز العربي للبحوث والدراسات 26أفريل 2016 تم الاطلاع عليه بتاريخ 2025/03/16 عبر الموقع الالكتروني:
http://www.acrseg.org/40137

[2] سليماني مباركة، مرجع سابق، ص 349-350،

[3] طارق إسراء، جواد كاظم الجابري، **الإرهاب الإلكتروني (دارسة مقارنة**، مذكرة الماجستير في القانون العام، كلية الحقوق جامعة النهروان، جمهورية العراق، 2012، ص37-38

صفة العالمية، بينما الإرهاب ذو طابع دولي ومقاصدها مستوحاة من إيديولوجيات متطرفة وهجماتها ليست ذات أهداف نهائية بل هي وسيلة للتأثير السياسي وقلب موازين القوى.[1]

تنبثق ضرورة التمييز بين الإرهاب الإلكتروني والمقاومة الإلكتروني من نفس الضرورة القائمة بين الإرهاب والمقاومة في إطار الفكر التقليدي، ويمكن حصر هذه الأهمية في ثلاث نقاط أساسية؛ تتجلى أولهما في رصد الأحكام القانونية التي تتناول موضوع المقاومة كآلية يتم اللجوء إليها في تقرير المصير ومكافحة الاستعمار بكل مشتملاته، أما ثانيها فتتجلى في الإقرار بهذا الحق وجعله كآلية في بناء صلات وثيقة بين مختلف الشعوب قائمة على اعتبارات حقوق الإنسان ومقتضيات العدالة الدولية وحفظ السيادة والوحدة الوطنية في الدولة، أما ثالثهما فتتمحور على فكرة وضع إرهاب الدولة موضعا يمكن من خلاله أن يدان على الصعيد العالمي[2]

2. التمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية

الفرق بين الإرهاب الإلكتروني والجريمة الإلكترونية يتجلى في الغاية التي تحرك كل منها، فالإرهاب الإلكتروني له أهداف سياسية يسعى إلى تحقيقها باللجوء إلى الساحة الإلكترونية، بينما الجريمة الإلكترونية لا ترتقي إلى هذا المستوى في قصدها الإجرامي، فمفهوم الإرهاب الإلكتروني وإن كان يتضمن جرائم إلكترونية كالتجسس والاختراق والقرصنة والتشهير والتحريض عبر المواقع الإلكترونية وانتحال الشخصية وانتهاك الخصوصية وتهديد التجارة الإلكترونية والتعدي على التعاملات المالية والمصرفية ولكن هذا التضمن مقتصر، فقط على التوظيف ولا يتعداه إلى الغاية [3]، فكلا الأعمال الإرهابية الإلكترونية هي من ضمن الجرائم الإلكترونية ولكن العكس غير صحيح[4]

3. التمييز بين الإرهاب الإلكتروني وحرب المعلومات

تعرف حرب المعلومات على أنها : نشاط اتصالي مخطط له لا يحمل عنفا، يوجه نحو العدو، ويوجه من السلطات نحو شعبها ويوجه نحو الشعوب الصديقة ، فحرب المعلومات من خلال هذا التعرف تتميز بأنها حرب لينة أو ناعمة، إذا يتم توظيف العنف كآلية أو وسيلة فيها، فضلا على أنها لا تستهدف فقط الأعداء ولا توظفها فقط الأنظمة الاستبدادية، بل تستهدف حتى الجهات الصديقة.

و ثمة علاقة وطيدة بين الإرهاب الإلكتروني وحرب المعلومات، ولا يمكن التمييز بينها إلا وفق الغاية والهدف، فالإرهاب الإلكتروني يحوم حول مفهوم حرب المعلومات إذ أنه في حربه الإلكترونية يستعين بها

---

[1] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، غمط جديد وتحديات مختلفة)**، مرجع سابق، ص 145.

[2] ناصر الهاشمي، **الإرهاب: (الجذور، المظاهر، وسبل المكافحة)**، ط01، دار الحامد للنشر والتوزيع، الأردن، 2016، ص 163.

[3] عبد الصادق عادل المرجع نفسه، ص 131.

[4] نجاري فايزة بن حاج علي، **دراسة لظاهرة الإرهاب الالكتروني**، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، 2022، ص 626.

لتحقيق أهدافه، والحرب المعلوماتية قد تتحول إلى إرهابي إلكتروني تأخذ تكييفها القانوني وهذا إما لكونها أداة تستعملها وتوظفها الجماعات الإرهابية، وإما لكون وسائلها وأهدافها هي نفس تلك الأهداف والوسائل التي تتبناها الجماعات المتطرفة[1]

المطلب الثاني: خصائص واسباب الارهاب الالكتروني

تعتبر جريمة الإرهاب الإلكتروني من أحدث التهديدات الأمنية التي تهدد المجتمع الدولي، فطبيعتها الفريدة من نوعها تضفي عليها نوعا من التميز والتعقيد (الفرع الاول)، كما أن الطفرة الإلكترونية الكبير في العصر الحديث والاعتماد المتزايد عليها في إنشاء وإدارة البني التحتية الحرجة قد منح للهجمات الإرهابية أهدافا استراتيجية مهمة وآليات إبداعية متجددة، الأمر الذي عزز التوجه إليها كبديل عن الإرهاب التقليدي لما بينهما من فوارق تكتيكية جمة (الفرع الثاني)، فأصبحت البيئة المعلوماتية والبني المرتبطة بها تواجه أصنافا مميزة من التهديدات غير المتوقعة ذات الأثر التدميري الكبير (الفرع الثالث).

الفرع الاول: الخصائص المتعلقة بطبيعة الجريمة

تنقسم الخصائص المميزة للجريمة الارهابية الالكترونية بحسب طبيعة الجريمة إلى :

أولا: جريمة الإرهاب الإلكتروني جريمة خفية

يعتبر الخفاء من أهم السمات البارزة التي تميز الإرهاب الإلكتروني عن الإرهاب التقليدي، ففي الحين الذين يمكن الكشف فيه عن جرائم الإرهاب التقليدي، وتحديد الجهات المتورطة فيه وبيان أهدافها منه، فإن الإرهاب الإلكتروني يفتقر إلى الآليات التي ترفع بها اللبس طبيعة الجريمة، فالهجمات الإلكترونية ذات الأثر التخريبي يمكن أن يتورط فيه أشخاص لا علاقة لهم بالأهداف والغايات الإرهابية، وعلى رأسهم نجد الباحثون عن الشهرة الذين تستهويهم عمليات الاختراق والقرصنة، وبعض الدول ذات الاتجاه القومي التي تنفذ هجمات إلكترونية بأساليب وآليات متعددة في إطار صراعها من أجندة أخرى، هذا، كما يمكن أن تكون تلك الهجمات داخلة ضمن أساليب المقاومة الإلكترونية المشروعة وشكلا من أشكال الاحتجاج[2]، ويمكن حصر محاور الخفاء الذي تتميز به جريمة الإرهاب الإلكتروني في العناصر التالية:[3]

1. خفاء هوية الجناة:

إن التعرف على الجناة بذواتهم يعتبر ذو أهمية كبيرة وأبعاد عميقة تنصب كلها في تحقيق مقتضيات العدالة الجنائية، فالتعرف على الجناة بالوسائل القانونية المشروعة يعتبر إجراء أوليا وعنصرا

---

[1] عبد الصادق عادل المرجع السابق، ص ص: 137-138

[2] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق، ص 122.

[3] نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، اطروحة دكتوراه في العلوم، تخصص : قانون، جامعة مومود معمري، تيزي وزو، الجزائر، 2023، ص 129

جوهرا لتحقيق العدالة، وضمان حق العقاب الذي ينزله المجتمع بهم عبر ممثلهم أمام القضاء، ومن غير ذلك فإن العدالة تكون عاجزة ومعطلة، والجناة أحرارا طلقاء.

ويعتبر المسئولون في الأعمال الإرهابية من بين أكثر الجناة فرارا من العدالة، وهذا لصعوبة وتعقيد عملية التعرف عليهم، فرغم أن هناك الكثير من الأعمال الإرهابية التي تعلن جهات معينة مسؤوليتها عن تنفيذها إلا أن هذا لا يشكل آلية للتعرف عليهم بذواتهم مما يبقي العدالة معلقة، وحق الأفراد في التعويض عن الخسائر والضحايا وتطييب الخاطر ضائعا، ويضيع أيضا معه حق المجتمع في العقاب الممنوح للسلطة بموجب العقد الاجتماعي، وإذا كان التعرف على هوية الجناة في الأعمال الإرهابية التقليدية أمرا يتسم بكل هذه الصعوبة والبطء والتعقيد فإن الجناة في الأعمال الإرهابية الإلكترونية يعتبر أكثر تعقيدا، نظر لكون المجهولية السمة البارزة في ملايين المتعاملين والمستخدمين للشبكات الإلكترونية، فالفضاء الإلكتروني يوفر بما له من خصائص متعددة نوعا من الحماية للإرهابيين، وذلك من خلال إخفاء هويتهم الحقيقية، فالدخول إلى الفضاء الإلكتروني لا يتطلب بروتكولات معقدة، أو استظهار لبطاقات الهوية، وفتح الحسابات في المواقع والخدمات التي يوفرها هذا الفضاء لا تعتمد إلا على البيانات والمعلومات التي يقدمها فاتح الحساب، ونادرا ما يتطلب الأمر مسح لبطاقات إثبات الهوية، فضلا عن وجود آليات تقنية وبرمجية تمكن الإرهابيين أيضا من إخفاء مواقعهم الجغرافية حال دخولهم إلى ساحات الفضاء الإلكتروني.[1]

2. خفاء الكشف والاستدلال

إن انعدام الدليل المادي الضروري لاكتشاف وإقامة الدليل على جريمة الإرهاب الإلكتروني، يعتبر من بين أهم مظاهر خفاء هذه الجريمة وتسترها، فعدم وجود دليل مادي ملموس يعتبر عائقا في تطبيق منهجية التحقيق التقليدية التي تعتمد أساسا على معطيات مادية بحتة، مما يجعل مسألة إقامة الدليل على مرتكبيها مسألة غاية في الصعوبة، ونظرا لكونها جريمة مرتبطة بآليات تقنية حساسة، فإن الدليل فيها غالبا ما يتعرض للتلاعب، سواء بمحوه أو بتزييفه، كما أن غياب الكشف المبكر عنها يعرضها للتلف والضياع، ضم إلى ذلك أن معظم الأعمال الإرهابية الإلكترونية لا يتم التبليغ عنها خشية التورط بها ومما يزيد الأمر تعقيدا كون الدليل الرقمي في الإثبات الجنائي غير متفق على حجيته نظرا لاختلاف الإثبات الجنائي في الأنظمة المقارنة.[2]

ومع ذلك تبقي هذه الخاصة نسبية نوعا ما، إذ أنه من الممكن جدا الوصول إلى اكتشاف هذه الجريمة والتوصل إلى جناتها، ومن ذلك التوصل إلى الهاكر الإسرائيلي الذي انتهك معلومات حساسية في أجهزة الحاسب التابعة للولايات المتحدة الأمريكية وإسرائيل، وهذا ما حققته أيضا السلطات الألمانية حين

---

[1] نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، مرجع سابق، ص 130

[2] الحوامدة لورنس سعيد، **جريمة الإرهاب الإلكتروني في التَّشريعات الجنائيَّة دراسةٌ تحليليَّة مُقارنةٌ**، مجلة كلية الشريعة والقانون بتفهنا، كلية الحقوق، جامعة طيبة، المملكة العربية السعودية، المجلد 24، العدد 01، 2022، ص ص429

ضبط مرتكب جرم إلكتروني بالتعاون مع السلطات السويسرية، كما تتسم صعوبة الاستدلال عليها بالنسبية أيضا، وذلك أن هناك بعض الأنظمة كثيرا ما تترك آثارا للجريمة فضلا عن وجود تقنيات وبرامج يمكن بواسطتها استرجاع الأدلة الجنائية من الفضاء الإلكتروني.

ثانيا: جريمة الإرهاب الإلكتروني جريمة عابرة للحدود:

لقد أتاحت عالمية الشبكة الإلكترونية لأن تكتسب جرائم الإرهاب الإلكتروني الطابع العالمي، إذ تم تكييفها قانونيا بالجرائم العابرة للحدود، كونها تتخطى الحدود السيادية للدولة كما أنها تتجاوز نطاق الجغرافي الإقليمي، إذ يمكن أن تحدث في أي مكان في العالم وخلال أي زمان دون أي يكون هناك أي تقارب بين الفعل الإجرامي وبين النتيجة التي تتمخض عنه، ورغم أن الإرهاب التقليدي مصنف من بين الجرائم المنظمة العابرة للحدود إلا أن الطبيعة التقنية لإرهاب الإلكتروني تحدث بينما فرقا.[1]

ثالثا: جريمة الإرهاب الإلكتروني جريمة ناعمة:

تعتبر جريمة الإرهاب التقليدي من الجرائم الصلبة التي تتطلب بذل الكثير من الجهد الجسدي من اجل تنفيذها، جهد يبدأ بالتخطيط لها واقتناء المعدات لأجلها، وقد يصل إلى حد التضحية بالنفس لإنجاحها كما هو الحال في الهجمات الانتحارية، أما الإرهاب الإلكتروني فلا يحتاج منفذه إلا إلى معدات آلية بسيطة، ودراية مستفيضة بتقنيات المعلومات وعلم البرمجيات ليحدث بعد ذلك أثار تدميرية هائلة.[2]

وهنا أيضا تبرز خصوصية الجناة في الأعمال الإرهابية الإلكترونية، فهم جناة متخصصون وعلى درجة عالية من الاحتراف تملكنهم من تجوز كل العقبات الأمنية الإلكترونية.[3]

رابعا: جريمة الإرهاب الإلكتروني ذات هدف سياسي

إن تعريف الإرهاب بما فيه الإرهاب الإلكتروني يقوم على عنصر الهدف، فالهدف الذي اتفق عليه جانب كبير من الفقه والقانون هو الهدف السياسي، وهذا ما تمت الإشارة إليه في ما تقدم من كلامنا، يعتبر الهدف السياسي الذي يقف وراء تنفيذ هجمات الإرهاب الإلكتروني، الحد الفاصل بين الإرهاب الإلكتروني وبين إساءة استخدام الكمبيوتر، فالهدف من وراء الهجمات الإلكترونية يحدث فارقا كبيرا في التكييف القانوني لطبيعة الجرم المرتكب[4]

وهذه الخاصية إنما هي خاصية عامة لكل أشكال الإرهاب، وتحمل في كنهها معنى الابتزاز، ومفادها في الغالب القيام بتوجيه الهجمات الإرهابية إلى الجهات التي ليس من صلاحياتها إصدار القرارات التي يردها المهاجمون، ولكن إلى الجهات التي تدخل ضمن نطاق بيئتها، من حمل الجهات التي

---

[1] نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، مرجع سابق، ص 131.

[2] المرجع نفسه.

[3] المرجع نفسه، ص 132.

[4] عبد الصادق عادل، **الإرهاب الإلكتروني : (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق، ص ص123-124.

تمتلك صلاحية إصدار القرار على الرضوخ والانصياع، فالإرهابيون كثيرا ما يوجهون هجمات ضد المستشفيات، أو ضد الشركات، رغم أنها مؤسسات ليس لها أن تصدر قرارا سياسيا، إلا أن استهدافها يشكل ورقة ضغط على الجهات الفعلية للانصياع لرغبات الإرهابيين.

الفرع الثاني: الخصائص المتعلقة بطبيعة الهجمات.

تنقسم الخصائص المميزة للجريمة الارهابية الالكترونية بحسب طبيعة الهجمات إلى :

اولا: المراوغة والمناورة التكتيكية

يعتمد الإرهابيون التقليديون على منهجية محددة في قيامهم بالأعمال التخريبية، فهم يعتمدون بصفة أساسية على أسلوب المراوغة والتدليس وحرب العصابات، حتى أن الانتحاريين منهم يراوغون حتى عن الموت، فلا حتى أسلوب الردع ينفع في حماية الأمن القومي منهم [1]

وهذا الأسلوب في النشاط الإرهابي تمت محاكاته بدقة على الساحة الإلكترونية، فأصبحت هجماتهم فيها كر وفر، والغالب فيها لمن استبق وفر قبل أن يدركه الآخر، وينتج عن هذه الضربات سعي كل طرف في تقوية ترسانته الإلكترونية، وتجديد طرق الحماية والأمان.[2]

ثانيا: سرعة التنفيذ.

إن ما يميز هجمات الإرهاب الإلكتروني عن الإرهاب التقليدي هي السرعة في تنفيذها، وتضيق التباعد الزمني بين الهجمات الكبرى من جهة، وبين التخطيط والتنفيذ من جهة أخرى، وهذا غير متاح للإرهابيين التقليدين، فهجماتهم متباعدة، والفارق الزمن في كل مرحلة من مراحلها يعد كبيرا نظرا للطبيعة المادية التي تتسم بها، وارتباطها بمجال أو فضاء فزيائي. [3]

ثالثا: هجمات الإرهاب الإلكتروني آلية حرب

بقطع النظر عن الخلاف السائد بين الفقهاء والأجهزة التشريعية الدولية عن مسمى " إرهاب الدولة " إلا أن آثاره ظاهرة من خلال الممارسات التي تنتهجها بعض الدول ضد مواطنيها أو ضد دولة أخرى، إذا تقوم بعض الدول باللجوء إلى التقنية الإلكترونية من أجل ممارسة الرعب والعدوان ضد مواطنيها عن طريق القيام بهجمات إلكترونية تهدف إلى غلق الصفحات أو المدونات المعارضة لها، أو هتك خصوصياتهم الإلكترونية، للكشف عن هويتهم من أجل القيام باعتقالهم أو إخفائهم قسريا، كما تقوم أيضا بتسديد ضربات إلكترونية إلى مرافق ومؤسسات دولة معادية لها .[4]

---

[1] نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، مرجع سابق، ص 132

[2] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق ص 124

[3] نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، مرجع سابق، ص 133

[4] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق، ص ص120-121

الفرع الثالث: الخصائص المتعلقة بتقييم طبيعة التهديد

تنقسم الخصائص المميزة للجريمة الارهابية الالكترونية بحسب طبيعة التهديد إلى :

اولا: تقيم القدرات الإرهابية:

يختلف تقييم قدرات المهاجمين الإلكترونيين وفق لأهدافهم السياسية، فالإرهاب الذين تمارسه الدول التي تتمتع بالتقنيات العالية والقدرات الفنية المذهلة غير ذاك الذي تمارسه الجماعات الإرهابية، أو ذاك الذي تمارسه الذئاب المنفردة، إذ أنها لا تملك نفس تلك القدرات التي تملها الدول ولا المعرفة الفنية اللازمة لتسديد الهجمات على صعيد واسع، كما أنها غير متاحة لجمع التنظيمات الإرهابية.[1]

لكن الأمر قد لا يدول طويلا، فقد بدأ التنظيمات الإرهابية مؤخرا في توظيف الفضاء الإلكتروني كمعسكر بديل للتدريب من خلال إصدار عددا من الأدلة التطبيقية عبر ما الوسائط المتاحة على الويب كما تنشر العديد من المقاطع الصوتية والبصرية وما إلى ذلك، وتقدم نماذج عملية وتطبيقية لطرق الانخراط في هذه التنظيمات، وأساليب صنع المتفجرات أو الأسلحة النارية الأخرى، فالفضاء الإلكتروني عموما أصبح يشكل معسكر تدريب افتراضي بالفعل .[2]

ورغم أن هذه المسألة خلافية بين الباحثين، وأن هناك جانب كبير منهم يرفض هذا الطرح، إلا أنه قد طرح فيه جانب من الصواب، فتنظيم القاعدة مثلا قد أصدر موسوعة كاملة – حصلنا على نسخة منها – في تكوين فني تقني لكوادر الاختراق الإرهابي مع منحهم مواقعا لها ثغرات للتدريب عليها.

ثانيا: تقيم آثار التهديد

إن أهداف الأعمال الإرهابية في الإرهاب التقليدي تكون محددة سلفا ونتائجها معروفة مسبقة، وهي نتائج وآثار يصعب تداركها أما هجمات الإرهاب الإلكتروني فهي هجمات ضد أهداف مجهولة وآثارها غير معروفة، إذ يمكن تداركها بالسرعة الهجمات نفسها[3]

---

[1] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق، ص ص 121–122

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة بغيناء استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، حزيران 2013، ص 08.

[3] عبد الصادق عادل، **الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة)**، المرجع السابق، ص122

المبحث الثاني: اركان جريمة الارهاب الالكتروني

إن تحقق الجريمة على الواقع الميداني لا يقوم إلا بتحقيق كافة الأركان الخاصة بها، وهذه الأركان هي التي تحدد نطاق الجريمة وترسم لها كيانها التي تفصلها عن غيرها من الجرائم، والتي تنطوي على الركن الشرعي الذي يقتضي التجريم القانوني للفعل الإجرامي ثم تأكيد إتيان هذه الأفعال المادية وبشكل مطابق للنص القانوني المجرم لها وهو ما يصطلح عليه بالركن المادي للجريمة وارتباط كل ذلك بإرادة مرتكب الفعل فقصده التام إلى إتيان هذه الأفعال على أنها فعل إجرامي أو جريمة معاقب عليها وهو ما تحقق معه الركن المعنوي أو القصد الجنائي .

والجريمة الإرهاب الإلكتروني كغيرها من الجرائم الأخرى لها ثلاثة أركان تقوم عليها الركن الشرعي[1]، المادي، المعنوي، فالأول يتمثل في النص القانوني الذي يجرم هذه الظاهرة، ونجد المشرع الجزائري جرم بعض الأفعال إذا ارتكبت لغرض إرهابي في نص المادة 87 مكرر 11 والمادة 87 مكرر 12 ق ع وأعطى لها وصف إرهاب إلكتروني في حالة ما ارتكبن باستخدام تكنولوجيات الإعلام والاتصال هذا بالنسبة للركن الشرعي أما الركن المادي (مطلب الأول) والركن المعنوي (مطلب الثاني) سنتطرق اليها كما يلي :

[1] عمد المشرع الجزائري على تحديد الركن الشرعي الظاهرة الإرهاب والمتمثلة في النصوص القانونية التي تجرم كافة السلوكيات لهذه الظاهرة سواء في قانون العقوبات عامة وفي قوانين خاصة ونص على ظاهرة الإرهاب في ق ع في المواد 87 مكرر إلى 87 مكرر 10 ولم يقف على تجريم الإرهاب التقليدي بل تدارك الثغر القانونية في سنة 2016 المسايرة التطورات الحاصلة في ارتكاب الجرائم باستعمال التكنولوجيا الحديثة من انترنت ونظام المعلوماتية وما يسمى بتجريم الإرهاب الإلكتروني في قانون رقم 16-02 و**القانون 24-06** الذي يتمم الأمر رقم 66_156 المتضمن قانون العقوبات بموجب المادة 87 مكرر 11 و87 مكرر 12 في القسم الرابع مكرر من الفصل الأول في الكتاب الثالث تحت عنوان الجرائم الموصوفة بالأفعال الإرهابية والتخريبية، كما عمدت على تجفيف منابع تمويل الإرهابيين من خلال القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما . المعدل والمتمم بالقانون رقم 15-04
ولم يكتفي بهذا القدر يل استحدث بموجب قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكرس من خلاله تدابير وقائية لمنع وقوع الجريمة واليات خاصة لمكافحة ومتابعة هذه الظاهرة بالإضافة إلى الإجراءات العامة الواردة في ق إ ج المستخدمة في كشف الجريمة وجمع أدلتها . كما نجد القانون رقم القانون 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 مؤرخة في 16 غشت 2009، تعديل قانون العقوبات المواد المتعلقة أساسا بالمساس بأنظمة المعالجة الالية للمعطيات في المواد 394 مكرر إلى مكرر 7 نلاحظ أنه المشرع الجزائري لم ينص صراحة في هذه المواد على جريمة الإرهاب الإلكتروني ولكن يفهم ضمنيا بأنه اعتبرها جريمة

المطلب الأول: الركن المادي لجريمة الإرهاب الإلكتروني

يعتبر الركن المادي جسم الجريمة حسب مبدأ "لا" جريمة دون الركن المادي"، وهو ذلك الفعل المحظور الذي يخرج إلى العالم الخارجي ويشكل اعتداء على الحق الذي يحميه القانون ويهدد النظام والأمن العام ويتكون الركن المادي من ثلاثة عناصر أساسية مترابطة فيما بينها ولابد من اجتماعها التي تتمثل في السلوك الإجرامي من المجرم، والنتيجة الإجرامية المتحققة في العالم الخارجي وفي الاخير العلاقة السببية بين المجرم والنتيجة[1] .

الفرع الأول : السلوك الإجرامي

هو ذلك النشاط المادي الصادر من الجاني بصفة اختيارية ويحدث أثر في العالم الخارجي ويعاقب عليه القانون وهو نوعان : إما سلبي أو سلوك إيجابي، فالأول يتحقق في حالة الامتناع عن فعل أو قول يأمر عليه القانون، أما الثاني هو القيام بفعل يجرمه القانون ويؤدي إلى إحداث نتيجة في الجرائم ذات النتيجة وكذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية ولا يعتد القانون بالوسيلة المستعملة سواء كانت مادية أو معنوية في ارتكاب السلوك الإجرامي .[2]

و بما أن المشرع الجزائري جرم فعل الإرهاب الإلكتروني في نص المادتين 87 مكرر 11 و87 مكرر 12 ومن هاتين المادتين يمكن استخلاص السلوكيات الإجرامية المكونة للركن المادي لهذه الجريمة.

أولا : السلوك الوارد الإجرامي الوارد في نص المادة 87 مكرر 11 ق ع ج

نقتصر في هطا العنصر ذكر السلوكات الإجرامية المنصوص عليها في المادة 87 مكرر 11 ق ع ج [3] والتي نجد المشرع الجزائري جرم جملة من الأفعال وتتمثل في :

1. فعل السفر باستخدام تكنولوجيا الاعلام والاتصال : جرمت الفقرة الأولى من نص المادة 87 مكرر 11 ق ع ج فعل سفر الجزائريين أو الأجانب المقيمين بالجزائر بصفة شرعية أو غير شرعية لارتكاب

---

[1] خلفي عبد الرحمان، **محاضرات في القانون الجنائي العام،** دار الهدى، عين مليلة الجزائر، 2012، ص ص 101 102

[2] رحماني منصور، **الوجيز في قانون الجنائي العام،** دار العلوم لنشر والتوزيع، عنابة، 2006، ص ص 98 –99

[3] تنص المادة 87 مكرر 11 من الامر رقم 66/156 " ..... كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أغير شرعية يسافر أو يحاول السفر من دولة لأخرى بغرض ارتكاب أفعال إرهابية أو تدريها أو الإعداد لها أو المشاركة فيها او التدريب على ارتكابها او لتلقي تدريب عليها .

ويعاقب بنفس العقوبة كل من : يوفر أو جمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب المذكورة في الفقرة الأولى من هذه المادة .

–قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر.

–يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في المادة

أفعال إرهابية أو تدريبها او الاعداد لها، ويقصد بفعل السفر مفارقة الاقامة، أي انتقال الشخص من مكان لآخر بهدف العمل أو السياحة او التجارة أو الزيارة أو الدراسة أو العبادة أو بهدف سياسي، سواء كانت لفترة قصيرة أو طويلة او إلى مكان بعيد أو قريب، ومن صياغة المادة لارتكاب افعال إرهابية " نجد أنها تجرم فعل السفر إذا كان الهدف منه القيام بعمليات إرهابية أو التدريب عليها او الإعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها[1].

ونجد المشرع الجزائري اشترط في الفقرة الأخيرة من نص المادة استخدام تكنولوجيا الإعلام والاتصال في ارتكاب هذا الفعل حتى يتغير شكل الجريمة من الإرهاب التقليدي إلى جريمة الإرهاب الإلكتروني محل الدراسة، ونحن برأينا نرى ان المشرع لم يوفق في تجريم الارهاب الالكتروني بمجرد تغيير وسيلة ارتكاب الفعل، حيث نجد فعل السفر يصعب حدوثه باستعمال التكنولوجيا الإعلام والاتصال إذا كان مقصوده بالمعنى الراجح لتعريف السفر الذي يتم بتنقل الجسد من بقعة جغرافية إلى أخرى، أي الخروج من بلد إلى آخر، إلا إذا كان قصده السفر عبر الشبكة العالمية العنكبوتية باستعمال البيئة الافتراضية التي تتيح فرصة تبادل الأفكار بين عدة أشخاص حول العالم أو تنفيذ مخططاتهم الإجرامية عبر مواقع الاتصال دون الخروج من بنيان البلدة التي يسكنها[2]

2 . فعل التمويل باستخدام تكنولوجيا الاعلام والاتصال : كم جرم المشرع فعل التمويل ويظهر من خلال مصطلح :"يوفر أو يجمع عمدا أموالا " و"قام عمدا بتمويل " [3]وقد عرف المشرع الجزائري فعل التمويل بموجب قانون 15-06 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما في نص المادة 3 منه : "كل فعل يقوم به كل شخص بأية وسيلة كانت مباشرة أو غير مباشرة وبشكل غير مشروع وبإرادة الفاعل من خلال تقديم أو جمع أموال بنية استخدامها كليا أو جزئيا من أجل ارتكاب الجرائم الموصوفة بأفعال إرهابية أو تخريبية [4]

ونجد المشرع الجزائري اشترط استخدام تكنولوجيا الإعلام والاتصال للحصول على التمويل عن طريق انشاء حسابات ومواقع إلكترونية خاصة بالتنظيمات الإرهابية والتي تتخذها كأداة لتوفير وجمع الأموال بصورة مباشرة عن طريق اختراق الحسابات البنكية أو تهديد الأشخاص عبر البريد الإلكتروني واجبارهم على تحويل مبالغ إلى حساباتهم الخاصة أو بصورة غير مباشرة كالادعاء بوجود نشاطات خيرية أو اجتماعية أو ثقافية أو عن طريق أنشطة غير مشروعة كجريمة تبييض الأموال أو الاتجار بالمخدرات

---

[1] انظر المادة 87 مكرر 11 المرجع نفسه.

[2] غلاف كريمة، جرلال زوهرة، مردع سابق، ص 36

[3] الفقرة الثانية من نص المادة 87 مكرر 11 السالفة الذكر

[4] المنصوص والمعاقب عليها بالمواد 87 مكرر إلى 87 مكرر 10 من قانون العقوبات. المادة 3 من القانون رقم15- 06 المؤرخ في 15 فبراير 2015 يعدل ويتمم القانون رقم 05/01 المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما المعدل والمتمم .

والأسلحة وتزوير العملة أو اختطاف الرهائن وطلب فدية منهم أو السرقة واستغلالها لتمويل سفر اشخاص إلى دول اخرى بغرض ارتكاب اعمال ارهابية.

ولقد حدد المشرع الجزائري طبيعة الأموال التي يتم استخدامها كليا أو جزئيا لغرض إرهابي في نص المادة 4 من القانون 15-06 السالف الذكر : أي نوع من الأموال المادية أو غير المادية لاسيما المنقولة أو غير المنقولة التي يحصل عليها بأية وسيلة كانت . والوثائق أو الصكوك القانونية أيا كان شكلها، بما في ذلك الشكل الإلكتروني أو الرقمي والتي تدل على ملكية تلك الأموال أو مصلحة فيها بما في ذلك الإئتمانات المصرفية وشبكات السفر والشبكات المصرفية والحوالات والأسهم والأوراق المالية والسندات والكمبيالات وخطابات الاعتماد".[1]

وقد جاء في هذه المادة أنه لا تتخذ إجراءات المتابعة من أجل تمويل الإرهاب إلا إذا كانت الافعال الأصلية المرتكبة في الخارج تكتسي طابعا إجراميا في قانون البلد الذي ارتكبت فيه وفي القانون الجزائري[2]

كما نجد المشرع أعطى تعريفا واسعا لأموال، سواء كانت أموال مادية أو معنوية او كانت منقول أو عقار أو شيكات أو وثائق أو أي شيء يحمل طابع مالي كما جرم فعل التمويل أيضا في نص المادة 87 مكرر الفقرة الأخيرة ق ع ج "تمويل إرهابي أو منظمة إرهابية.[3]

ثانيا : فعل التجنيد الوارد في نص المادة 87 مكرر 12 ق ع ج"[4]

نجد المشرع الجزائري نص صراحة في هذه المادة على فعل التجنيد من خلال مصطلح "لتجنيد الاشخاص "، ويقصد به استقطاب أعضاء جدد بغرض إدخالها في التنظيمات والجماعات الإرهابية لضمان بقاءها واستمراريتها فقد أصبح الإعلام الإلكتروني المنبر المفضل للتنظيمات الإرهابية الصيد أعضاء جدد وخاصة مع استخدام الفضاء السيبراني الذي يجعل التفاعل عابر للحدود الجغرافية، مما يسهل نقل المعلومات بين الأشخاص حول العالم[5]، ومنه تسهيل عملية التجنيد وجذب أكبر عدد ممكن من الاشخاص، ويعتبر فئة الشباب والمراهقين أكثر استهدافا في هذه العملية باعتبارهم الأكثر تواجدا في

---

[1] المادة 4 المرجع نفسه من القانون رقم15-06

[2] بلواضح الطيب قسمة محمد، **مكافحة جريمة تمويل الارهاب على المستويين الدولي والوطني**، مجلة الدراسات والبحوث القانونية، المجلد 02، العدد 05، 2017، ص 62

[3] المادة 87 مكرر من الامر رقم 66/156

[4] وتنص المادة 87 مكرر 12 ق ع ج على :" ... كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام خذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة

[5] اماني مهدى، **توظيف التنظيمات الارهابية لشبكات التواصل الاجتماعي في استقطاب الشباب استراتجيات واليات المواجهة**، مقال منشور 12مارس 2018 تم الاطلاع عليه يوم 29.04.2025 على الساعة 19:09 متاح على الرابط: https://democraticac.de/?p=52894

منصات التواصل الاجتماعي، كما أدركت التنظيمات الإرهابية أهمية هذه المواقع واعتبرتها الأداة العلمية والتكنولوجيا المهمة لنشر أفكارها وتنفيذ مشروعها الإيديولوجي، سواء بصورة مباشرة عن طريق التهديد او الترهيب، أو استعمال القوة وإجبار مستخدمي الانترنت للانضمام إليها، أو بصورة غير مباشرة بأسلوب الترغيب والإغراء واستمالة المشاعر عن طريق التلاعب بالعواطف واستخدام عبارات حماسية براقة عبر غرف الحوارات والدردشة[1] .

و نلاحظ في نص المادة 87 مكرر 12 ق ع ج سالفة الذكر أن المشرع الجزائري بين الجهات التي تجند لصالحها وهي : إما إرهابي أو جمعية إرهابية أو تنظيم إرهابي أو جماعة إرهابية أو منظمة إرهابية[2]. ونحن برأينا نجد المشرع لم يوفق في إعطاء المصطلحات لهذه الجهات، حيث اعتبر مصطلح التنظيم مختلف عن المنظمة والجماعة عن الجمعية من خلال استعماله حرف " أو " وهو حرف يفيد الإبهام أو الشك أو التخيير، ومن خلال استعمال مصطلح إرهابي الذي يختلف عن هذه المصطلحات وبالعودة إلى قاموس المعاني نجد مرادف كلمة جمعية اتحاد تنظيم جماعة رابطة منظمة، هيئة وهذا ما يؤكد أن هذه المصطلحات تفيد نفس المضمون.[3]

ثالثا : الشرط الخاص المشترك في الركن المادي لجريمة الإرهاب الإلكتروني

لقد اشترط المشرع الجزائري من خلال نص المادتين 87 مكرر 11 و87 مكرر 12 أنه في حالة ما إذا تم ارتكاب هذه السلوكيات الإجرامية باستعمال وسيلة المتمثلة في تكنولوجيا الإعلام والاتصال نكون أمام جريمة الإرهاب الإلكتروني وإذا تم ارتكابها دون هذه الوسيلة نكون أمام جريمة إرهاب تقليدية، فهذه الوسيلة تعتبر العنصر المشترك بين المادتين السالفتين الذكر .

الفرع الثاني : النتيجة الجرمية في جريمة الإرهاب الإلكتروني

النتيجة الجرمية هي العنصر الثاني من عناصر الركن المادي إلى جانب عنصر السلوك الإجرامي ويقصد بها الأثر الطبيعي المترتب على السلوك الإجرامي، والذي يحدث تغييرا في العالم الخارجي سواء كان ماديا أو معنويا وليس لكل جريمة نتيجة فهناك جرائم يقوم ركنها المادي على السلوك المجرد بغض النظر عن النتيجة وعليه تنقسم الجرائم إلى جرائم مادية وإلى جرائم شكلية[4].

الجرائم المادية أو ما يسمى بالجرائم ذات النتيجة أو جرائم الضرر : وهي الجرائم التي تحدث بطبيعتها نتيجة مادية محسوسة وضارة ناشئة عن الفعل الذي ارتكبه الجاني، أما الجرائم الشكلية أو ما يسمى

---

[1] غلاف كريمة، جرلال زوهرة، مردع سابق، ص 41

[2] بن سالم ايمان، **جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري**، ط01، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2028، ص 53

[3] غلاف كريمة، جرلال زوهرة، مردع سابق، ص 42

[4] منصوري رحماني، مرجع سابق، ص 102 .

بالجرائم غير ذات النتيجة أو جرائم الخطر فهي من الجرائم التي لا تحدث بطبيعتها أية نتيجة مادية، فالضرر فيها محتملا بمجرد التهديد بالعدوان الذي ينال من المصلحة محل الحماية الجنائية[1] .

وباعتبار أن جريمة الإرهاب الإلكتروني تأخذ حكم الجريمة المعلوماتية فهي بذلك تعد من الجرائم الشكلية التي يفترض فيها الضرر مستقبلا المتمثل في نتيجتها الجرمية فبمجرد استخدام تكنولوجيا الاعلام والاتصال للقيام بالسلوكيات الواردة في نص المادتين 87 مكرر 11 و87 مكرر 12 من ق ع ج من فعل السفر أو تمويل أو تجنيد لأغراض إرهابية تقوم الجريمة حتى وإن لم تتحقق هذه الأفعال كونها جريمة خطر وليست ضرر وذلك بالنظر إلى الوسيلة المعتمدة عليها في تنفيذ هذه السلوكيات الإجرامية

الفرع الثالث : العلاقة السببية في جريمة الإرهاب الإلكتروني

تعرف العلاقة السببية بأنها الرابطة التي تصل بين العنصرين السابقين، أي توافر السببية بين السلوك والنتيجة، فإذا انقطعت العلاقة السببية انتفت المسئولية الجنائية باعتبارها أحد عناصر الركن المادي، وتقتصر على فئة واحدة من الجرائم وهي الجرائم ذات النتيجة أو الجرائم المادية، بينما تستثنى الجرائم الشكلية من هذه العلاقة، كون لا يدخل في ركنها المادي ضرورة توافر نتيجة إجرامية معينة وعدم وجود نتيجة للفعل بطبيعته لا يترك محلا للبحث عن العلاقة السببية[2] وبما أن جريمة الإرهاب الإلكتروني من الجرائم الشكلية فإنه لا يثور في شأنها العلاقة السببية، حيث لم يستلزم المشرع في نموذجها الإجرامي تحقيق النتيجة الجرمية لقيام ركنها المادي، فبمجرد استخدام البيئة الافتراضية وإنشاء مواقع حسابية واستخدام البريد الإلكتروني لتسهيل عملية السفر أو تمويل منظمتها إرهابية أو لاستقطاب واستدراج أشخاص إلى جماعتها من أجل ارتكاب أعمال إرهابية فهي تشكل جريمة تامة حتى وإن لم تتحقق النتيجة ي عدم وصول المجرم الإرهابي إلى تحقيق السلوكيات الواردة في نص المادتين 87 مكرر 11 و87 مكرر 12 ق ع ج سالفتين الذكر.

كما تستثنى جريمة الإرهاب الإلكتروني من موضوعين رئيسيين إلى جانب العلاقة السببية وهما الشروع والخطأ غير العمدي (وهو ما سنتناوله في الركن المعنوي).

عدم تصور الشروع في جريمة الإرهاب الإلكتروني

نص المشرع الجزائري على الشروع تحت مصطلح المحاولة وعرفه في نص المادة 30 من ق ع ج: "كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها[3]، حتى وإن لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها " ومن هذا التعريف فالشروع

[1] خلفي عبد الرحمان، مرجع سابق، ص 105.

[2] خلفي عبد الرحمان، **القانون الجنائي العام (دراسة مقارنة)**، دار بلقيس للنشر دار البيضاء، الجزائر، 2017، ص 203

[3] المادة 30 من الامر رقم 66/156

حسب المشرع الجزائري يأخذ ركنين وهي البدء في التنفيذ وانعدام العدول الإرادي[1] حيث يمكن للجاني أن يبدأ في تنفيذ السلوك الإجرامي ولا يكتمل أو يكتمل السلوك الإجرامي ولا تقع النتيجة بسبب عامل خارج عن إرادته ويطلق على الصورة الأولى اسم الجريمة الموقوفة وعلى الصورة الثانية الجريمة الخائبة.[2]

ويتصور الشروع في كل الجنايات وبعض الجنح المنصوص عليه قانونا وفي الجرائم ذات نتيجة ،أما الجرائم الشكلية لا يمكن أن تكون موقوفة أو خائبة لأن الجرائم الشكلية تتحقق بمجرد البدء بتنفيذها ولا يشترط حصول النتيجة فيها .

المطلب الثاني: الركن المعنوي لجريمة الإرهاب الإلكتروني

لا تكفي وحدها الواقعة المادية سواء حققت النتيجة أولم تتحقق لقيام الجريمة، بل لابد من وجود باعث نفسي يحمل الشخص للقيام بالسلوكيات الإجرامية والمعبر عنه بالركن المعنوي لأنه به تتحدد وتكتمل المسؤولية الجنائية للجاني للقاعدة القائلة : "لا جريمة بدون الركن المعنوي ".

والعناصر النفسية الماديات الجريمة تأخذ صورتين إما اتجاه الجاني إلى اتخاذ حركات إرادية غير مشروعة مع رغبته في تحقيق النتيجة وهو ما يعني بالقصد الجنائي أو صورة العمد، أما الصورة الثانية تتمثل في اتجاه ارادته في اتيان الفعل دون الرغبة في تحقيق النتيجة وهي صورة الخطأ غير العمدي وجريمة الإرهاب الإلكتروني من الجرائم التي لا يتصور فيها الخطأ فهي تعد من الجرائم العمدية، ونجد المشرع الجزائري أورد في المادة 87 مكرر 11 ق ع ج عبارة تفيد القصد العمدي لهذه الجريمة من خلال "يوفر أو يجمع عمدا "، "قام عمدا"[3] " ما يؤكد عدم تصور الخطأ في الجريمة الارهابية الالكترونية[4] .

عدم تصور الخطأ غير العمدي في جريمة الإرهاب الإلكتروني، لم يعرف المشرع الجزائري ما هو الخطأ غير العمدي، وإنما عرفه القضاء بتعاريف مختلفة ومن بين تلك التعاريف، الخطأ هو كل فعل أوترك ارادي ترتب عليه نتائج لم يردها الفاعل مباشرة أو بطريقة غير مباشرة [5]، ولكنه كان بوسعه اتخاذ واجبات الحيطة والحذر لمنع النتيجة الضارة التي كان بوسعه توقعها وتجنبها[6]، ومن هذا التعريف نستنتج أن المهم من الخطأ هو النتيجة التي تتحقق بسب اهمال الجاني وعدم اتخاذ الاحتياطات الازمة التي يدعوا إليها الحذر، ولا يعتد بالفعل الذي يحدثه الجاني، وهذا ما يكون عدم تصور الخطأ في جريمة الإرهاب الإلكتروني التي لا يشترط تحقق النتيجة فيها .

---

[1] كركوم لمين الطيب رزيق، **الشروع في الجريمة**، مذكرة للنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية ،ك ج ع من جامعة عبد الرحمان ميرة بجاية 2014/2015، ص 11

[2] خلفي عبد الرحمان، القانون الجنائي العام (دراسة مقارنة)، مرجع سابق، ص 213

[3] المادة 87 مكرر 11 من الامر رقم 66/156

[4] غلاف كريمة، جرلال زوهرة، مردع سابق، ص47

[5] منصوري رحماني، مرجع سابق، ص 125

[6] انقوش سعاد، اشعلال صورية، **الركن المعنوي في الجريمة**، مذكرة ماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية .ك ح ع من جامعة عبد الرحمان ميرة بجاية 2016/2017، ص 22 .

وبالتالي فإن الركن المعنوي لهذه الجريمة يقوم بقصد عام وقصد خاص والذي سوف نتطرق إليه فيما يلي :

الفرع الاول : القصد الجنائي العام

يعبر القصد الجنائي عن تلك الارادة الخبيثة للجاني في مخالفة المسار القانوني على النحو الصحيح الذي رسمه المشرع، فقد عرفه الفقه على أنه : " العلم بعناصر الجريمة وارادة ارتكابها[1] ومن هنا يتضح لنا أنه للقصد الجنائي العام عنصرين جوهريان يتمثلان في العلم والإرادة بحيث لا بد من توافرهما لاكتمال الركن المعنوي للجريمة فالأول يعرف على انه :" حالة ذهنية أو قدر من الوعي يسبق تحقق الإرادة ويعمل على إدراك الأمور على نحو صحيح مطابق للواقع[2]، وهي الحالة التي يكون فيها الجاني على دراية تامة بمكونات الجريمة وأن السلوك الذي أتى به مجرما فإذا انتفى العلم انعدم القصد الجنائي لديه .

وأما العنصر الثاني عرفه الفقه على أنه عبارة عن قوة نفسية أو نشاط نفسي يوجه كل أعضاء الجسم أو بعضها نحو تحقيق غرض غير مشروع[3]، وعليه تعبر الإرادة عن بلورة الحالة النفسية للجاني في توجيه أعضاءه لإتيان سلوك مجرم قانونا عن علم وادراك وبالتالي فإنه لكي يتوافر القصد الجنائي العام لدى المجرم لا بد من اقتران العلم بالإرادة معا، ويشمل القصد الجنائي العام في جريمة الإرهاب الإلكتروني في علم الجاني بارتكابه سلوك مجرم قانونا المتمثل في فعل السفر والتمويل والتجنيد وعلمه بالوسيلة المستعملة في ارتكاب هذه الأفعال وهي تكنولوجيا الإعلام والاتصال، مع اتجاه إرادته إلى استخدام هذه الوسيلة في تنفيذ هذه الأفعال لأغراض إرهابية.[4]

الفرع الثاني: القصد الجنائي الخاص

هو الغاية أو المصلحة التي تدفع الجاني إلى ارتكاب الجريمة، وهذا القصد يتطلبه القانون في بعض الجرائم إلى جانب القصد العام[5] ويتحقق في هذه الجريمة في اتجاه نية الإرهابي إلى القيام بفعل السفر أو التمويل أو التجنيد باستخدام تكنولوجيا الإعلام والاتصال بغرض ارتكاب أفعال إرهابية .[6]

وعليه فالقصد الخاص في هذه الجريمة هو الغاية أو الغرض الذي يرمى إليه الجاني من ارتكاب السلوكيات السالفة الذكر باستخدام وسيلة مستحدثة لارتكاب أفعال إرهابية، ونجد المشرع الجزائري نص

---

[1] خلفي عبد الرحمان، **محاضرات في القانون الجنائي العام**، مرجع سابق، ص151

[2] المرجع نفسه، ص 152

[3] المرجع نفسه، ص 154

[4] غلاف كريمة، جرلال زوهرة، مردع سابق، ص 48

[5] خلفي عبد الرحمان، **القانون الجنائي العام (دراسة مقارنة)**، مرجع سابق، ص 214

[6] غلاف كريمة، جرلال زوهرة، مردع سابق، ص 48

على الأفعال التي تعد إرهاب في نص المادة 87 مكرر ق ع ج والتي تستهدف أمن الدولة واستقرارها وتتمثل في:

- ✓ بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المساس بممتلكاتهم
- ✓ عرقلة حركة المرور وحرية التنقل في الطرق والتجمهر او الاعتصام في الساحات العمومية
- ✓ الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور .
- ✓ الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني .
- ✓ الاعتداء على المحيط وادخال مادة أو تسربها في الجو أو باطن الأرض أو إلقاءها عليها أو في المياه بما فيه المياه الإقليمية من نشأتها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.
- ✓ عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.
- ✓ عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين
- ✓ والتنظيمات .
- ✓ تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل .
- ✓ إتلاف منشئات الملاحة الجوية أو البحرية أو البرية .
- ✓ تخريب أو إتلاف وسائل الاتصال .
- ✓ احتجاز الرهائن .
- ✓ الاعتداء باستعمال المتفجرات أو المواد البيولوجية أو الكيماوية أو النووي أو المشعة.
- ✓ تمويل إرهابي أو منظمة إرهابية ""[1]

[1] المادة 87 مكرر من الامر رقم 66/156

الفصل الثاني :

سبل وآليات مكافحة

الجريمة الارهابية

الالكتَرونيةً

يعتبر الإرهاب الإلكتروني آخر ما توصل إليه العقل الإجرامي، فبتنامي الثورة التكنولوجية والمعلوماتية تنامت العقول الإجرامية الإرهابية، وبالتوافر السهل لشبكة الإنترنت وملحقاتها المادية أصبح العالم دولا وأفرادا يتعرض اليوم لهجمات إرهابية عبر الفضاء الرقمى، وتختلف حدة هذه الهجمات حسب نوعها وهدفها وغايتها، ، المصالح الأساسية للدول وأمنها أو سيادتها القومية، وقد تستهدف سلامة المواطنين وطمأنينتهم، فالإرهاب الإلكتروني هو أحد الجوانب الأكثر سلبية في استغلال التطور الحاصل في تقنية المعلومات، ونظرا خطورة جريمة الإرهاب الإلكتروني، والتي تتعدد ضحاياها بين الأفراد والدول والكيانات الأخرى، ولما تثيره هذه الجريمة من مخاوف وقلق لدى المجتمع الدولي والمحلي بسبب تهديدها وتطورها المستمرين، وغايتنا من هذه الفصل إبراز مختلف الجهود الدولية والاقليمية وكذا الوطنية لمكافحة الإرهاب الإلكتروني، وعليه سوف نخصص المبحث الاول إلى الجهود الدولية لمكافحة الارهاب الالكتروني، وفي المبحث الثاني نستعرض الجهود الوطنية لمكافحة الارهاب الالكتروني.

المبحث الاول: الجهود الدولية لمكافحة الارهاب الالكتروني

الجهود الدولية لمكافحة الإرهاب الإلكتروني تشمل مجموعة واسعة من المبادرات والاتفاقيات الدولية، بهدف تعزيز الأمن السيبراني ومواجهة التهديدات التي يشكل الإرهاب الإلكتروني .تتضمن هذه الجهود تطوير استراتيجيات عالمية، بناء قدرات الدول الأعضاء، وتنسيق الجهود بين الدول والمنظمات الدولية.

المطلب الاول: مكافحة الارهاب الالكتروني على المستوى العالمي.

تعّد مكافحة الإرهاب الإلكتروني من أهم التحديات التي تواجه المجتمع الدولي في الوقت الحالي، إذ يتم استعمال التكنولوجيا والإنترنت لتنظيم وتنفيذ الأعمال الإرهابية؛ وتشمل هذه التهديدات الإلكترونية الهجمات على البنية التحتية للإنترنت والتجسس الإلكتروني والاحتيال الإلكتروني واختراق الأنظمة الإلكترونية والاعتداء على بيانات المستخدمين، وغيرها من الأنشطة الإلكترونية الخبيثة، وبالتالي فإن تحليل التهديدات الإلكترونية وتعزيز القدرات الدفاعية ضد هذه التهديدات يعّدان من أهم الأولويات للحفاظ على الأمن والاستقرار العام .[1]، وعليه نتطرق من خلال هذا المطلب إلى المعاهدات والاتفاقيات الدولية في الفرع الاول، ثم جهود المنظمات الدولية في الفرع الثاني.

الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية

سنتطرق في هذا الفرع لمكافحة الإرهاب الإلكتروني في كل اتفاقية إساءة استعمال تكنولوجيا المعلومات، واتفاقية بودابست.

أولا: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات

أصدرت الاتفاقية العالمية لمكافحة إساءة استعمال تكنولوجيا المعلومات رقم (55/63) في 12 أبريل 2000 من قبل الجمعية العامة لمنظمة الأمم المتحدة وهذا نتيجة لتزايد الجرائم المرتكبة عبر الانترنت، وقد كان هدف هذه الجمعية الدعوة إلى الانضمام إلى جميع الاتفاقيات ذات الصلة بغية تكثيف الجهود لمحاربة الجريمة العابرة للحدود الوطنية ومنها الإرهاب الإلكتروني، والعزم على أن تكفل إتاحة منافع التكنولوجيا الجديدة وخاصة تكنولوجيا المعلومات والاتصالات للجميع بما يتفق مع التوصيات الواردة في الإعلان الوزاري الصادر من الدورة الموضوعية للمجلس الاقتصادي والاجتماعي للأمم المتحدة لعام 2000. [2]

---

[1] دريعي عبد السادة سحر، **مكافحة الإرهاب الالكتروني :تحليل التهديدات وتعزيز القدرات الدفاعية**، مجلة قضايا سياسية، العدد74، 2023، ص 269

[2] قاسمي رحمة، بوخروبة كريمة، **الارهاب الالكتروني(التحديات والمواجهات)**، مذكرة ماستر في الحقوق، تخصص: قانون اعلام الي، جامعة محمد البشري الابراهيمكي، برج بوعريريج، الجزائر، 2021-2022، ص 36

كما تشير أيضا على أن قرار الجمعية العامة رقم (45/121 المؤرخ في 14 ديسمبر (1990) أيد توصيات مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، والذي دعا الدول أن تكثف جهودها لمكافحة إساءة استعمال الحواسيب بفعالية أكبر.[1]

نصت المادة 1 من اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 55/63 لسنة 2000 في الفقرات (أحد) على ما يلي:

أ- ينبغي للدول أن تكفل عدم توفير قوانينها وممارستها فيها ملاذ أمن للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية "

ب- ينبغي أن تنسق جميع الدول المعنية للتعاون في مجال إنفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[2]

ج- ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية ".

د- ينبغي تدريب العاملين في مجال نفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[3]

تشير الجمعية العامة في ديباجة اتفاقية الأمم المتحدة لمكافحة الجريمة العابرة للحدود إلى أهمية مواصلة العمل بشأن صياغة بروتوكول خاص بمكافحة صنع الأسلحة النارية والاتجار بها بصورة غير مشروعة، وهو ما انتهى إليه الحال بوضع الأحكام النهائية للبروتوكول المذكور في 31 ماي عام 2001، ويعتبر هذا البرتوكول عنصرا أساسيا في مجال مكافحة الجريمة العابرة للحدود وفي مجال مكافحة الإرهاب، فقد أكد قرار مجلس الأمن رقم 1373 على العلاقة الموجودة بين الجريمة العابرة للحدود والإرهاب، إذ يعتبر الإتجار غير المشروع بالأسلحة أحد دعائم الإرهاب [4]

فقد أشار البروتوكول في ديباجته إلى أهمية منع ومكافحة واستئصال هذا النشاط، نظرا لما له من آثار سلبية على أمن الدول [5]

أما عن أهم الأحكام الواردة في هذا البرتوكول، فتبين المادة 4 منه على ما يلي:

---

[1] عمر عباس، العبيدي خضير، **الإرهاب الإلكتروني في نطاق القانون الدولي**، رسالة ماجستير، كلية الحقوق، جامعة تكريت العراق 2019، ص47-48

[2] شاشوة ياسمينة، ، مرجع سابق، ص 74.

[3] نفس المرجع، ص 74.

[4] تراقي أمال، **الجريمة المنظمة والجهود المبذولة لمكافحتها**، مذكرة لنيل درجة الماجستير في القانون، كلية الحقوق، جامعة بجاية، 2012، ص 47

[5] أشار البرتوكول في ديباجته إلى أن الدول الأطراف تضع في اعتبارها " مبدأ المساواة في الحقوق ومبدأ تقرير المصير الشعوب".

" الغرض من هذا البرتوكول هو ترويج وتيسير وتعزيز التعاون بين الدول الأطراف، بغية منع ومكافحة واستئصال صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة، والإتجار بها بصورة غير مشروعة وقد أكد عليه أيضا في المادة 04فقرة 01 منه على[1]:.

"لا ينطبق هذا البروتوكول على الصفقات من دولة إلى أخرى أو عمليات النقل بين الدول في الحالات التي يكون من شأن تطبيق البروتوكول فيها أن يمس بحق دولة طرف في اتخاذ إجراءات حرصا على مصلحة الأمن الوطني بما يتفق على ميثاق الأمم المتحدة .[2]

ولتحقيق هذا الغرض يشترط البروتوكول وسم الأسلحة النارية بهدف تحديد هوية كل سلاح ناري واقتناء أثره، وانشاء أنظمة فعالة لإصدار رخص للتصدير والاستيراد وكذا اتخاذ تدابير بشأن العبور الدولي فيما يخص نقل الأسلحة النارية وأجزائها ومكوناتها والذخيرة .[3]

أما في مجال التعاون بين الدول الأطراف، فقد حددت المادة 13 منهجية التعاون على مستويات متعددة مثل المستوى الثنائي، الإقليمي والدولي، مع ضرورة تحديد كل دولة لنقطة اتصال واحدة على المستوى الوطني تعمل كحلقة وصل مع الدول الأطراف بشان المسائل المتعلقة بالبروتوكول.[4]

وتلتزم الدول الأطراف بوضع ما يلزم من تدابير وفق نظمها القانونية الداخلية لمنع وقوع هذه الأسلحة في أيدي أشخاص غير مأذون لهم، وذلك بضبط تلك الأسلحة وتدميرها، مع العلم أنه يجب مراعاة ما ورد في المواد 14.13.12 من اتفاقية باليرمو التي تطبق على ضبط في العائدات الإجرامية المصادرة والناتجة عن نشاطات الجريمة ومصادرة والتصرف المنظمة..[5]

ثانيا: اتفاقية بودابست

تعرف اتفاقية بودابست بالاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية، وقد وضعت هذه الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية،

---

[1] المادة 02، من بروتوكول مكافحة صنع الأسلحة النارية وأحزانها ومكوناتها والذخيرة والإتجار بها بصورة غير مشروعة، المرجع السابق

[2] المادة 04 فقرة 01، من بروتوكول مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والإتجار بها بصورة غير مشروعة، المرجع السابق

[3] النظر المادتين 08 و10، من المرجع نفسه.

[4] أنظر المادتين 13 و18، من المرجع نفسه

[5] ورد استثناء في هذا البروتوكول بشأن تعديل تدابير التصرف في العائدات الإجرامية والممتلكات المصادرة الواردة في المادة 14 من اتفاقية باليرمو وذلك في المادة 02فقرة 06 التي تنص على تدمير الأسلحة مالم يكن قد صدر إن رسمى بالتصرف فيها بطريقة أخرى شريطة أن تكون الأسلحة النارية قد وسمت بعلامات

وعرضت للتوقيع في بودابست في 23/11/2001 ودخلت حيز التنفيذ في ،2004، وهذه الاتفاقية متاحة أمام أية دولة من دول العالم للانضمام إليها.[1]

أبرمت معاهدة بودابست لمكافحة الجرائم المعلوماتية سنة 2001، تعتبر أول معاهدة دولية تهدف إلى تنسيق التعاون الدولي من اجل محاربة الجرائم المعلوماتية لما وصلت إليه هذه الأخيرة من مخاطر تهدد أمن الأشخاص وممتلكاتهم على الصعيد الوطني والدولي ،وتم التوقيع عليها من طرف المسؤولين الأوروبيين ومن طرف أمريكا واليابان وكندا وجنوب إفريقيا، عقدت هذه الاتفاقية بعد نتائج العديد من الدراسات التي توصلت إلى أن التعاون الدولي هو الوسيلة الوحيدة القادرة على ردع الجرائم المعلوماتية التي تعبر الحدود الدولي ومن اجل ضمان تطبيق القوانين وتامين احترام حقوق الإنسان مثل الحقوق الملكية الفكرية وتتلخص الجوانب وأهداف هذه المعاهدة في:

– العمل على توحيد التدابير التشريعية بين الدول للوقاية من الجرائم المعلوماتية وتفعيل الجانب الموضوعي والإجرائي للحد منها.

– تحقيق التوازن بين حقوق الأساسية الراسخة في العلاقات الدولية، تحديد الطرق الواجب إتباعها في التحقيق في الجرائم المعلوماتية التي تعهدت الدول بالتعاون من اجل مكافحتها.

– تنسيق بين الجهود وتوحيدها من أجل نتائج فعالة في الحد منها.

كما تناولت هذه الاتفاقية العديد من الجرائم المعلوماتية التي تشهد انتشارا عالميا مثل: الإرهاب الالكتروني وعمليات تزوير بطاقات الائتمان، دعارة الأطفال، المساعدة المتبادلة في إجراء اعتراض المراسلات تفعيل نظام سريع وفعال للتعاون الدولي. [2]

تكونت هذه الاتفاقية من 48 مادة وأكدت الاتفاقية على الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة المعلوماتية واعتبرت مرجعا لا يستهان به في ميدان محاربة الإجرام السيبيري سواء بالنسبة لبعض الاتفاقيات اللاحقة ذات الصلة أو بالنسبة للتشريعات الداخلية لبعض الدول لقد ركزت اتفاقية بودابست على ثلاثة عناصر أساسية:

العنصر الأول: يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية.

العنصر الثاني: يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الالكترونية.

العنصر الثالث: أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم، والانطلاق مما أنجز من جهود دولية وإقليمية في هذا المجال، وكان ذلك في مواد الاتفاقية الموزعة على أربعة فصول:

الفصل الأول: تضمنت تعريفا للمصطلحات الأساسية[1]

---

[1] عوينات بن عمر نجيب، **الإرهاب الإلكتروني: المفهوم والجهود الدولية والإقليمية لمكافحته**، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 02، العدد 02، جوان 2017، ص 18

[2] ناني لحسن، **التحقيق في الجرائم المتعلقة بتكنولوجيا المعلومات**، دار النشر الجامعي الجديد، الجزائر،2018 ، ص 43

الفصل الثاني: وجاء تحت عنوان الخطوات الواجب اتخاذها على الصعيد الوطني، وهو مؤلف من ثلاثة أقسام: الأول: يضم المواد من 2 إلى 13 التي تعالج النصوص الموضوعية لجرائم الحاسوب والثاني: يضم المواد من 14 إلى21 وتتعلق بالقواعد الإجرائية والثالث: يضم المادة 22 ويتعلق بالاختصاص.

الفصل الثالث: وجاءت تحت عنوان التعاون الدولي[2]

الفصل الرابع: ويتضمن الأحكام الختامية من المادة 36 حتى 148، كما حددت اتفاقية بودابست الجرائم المعلوماتية وصنفتها في خمسة عناوين في القسم الأول من الاتفاقية هي كالتالي :

العنوان الأول: ويضم جوهر جرائم الحاسب أو الجرائم المعلوماتية وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات والنظم.

العنوان الثاني: ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي: التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.

العنوان الثالث: ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى وهي التي تخص الإنتاج والنشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، في المادة التاسعة من الاتفاقية.

العنوان الرابع: ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة 10من الاتفاقية.

العنوان الخامس: وهو يشتمل على أحكام إضافية بخصوص المشروع والاشتراك طبقا للمعايير الدولية الحديثة بالنسبة المسؤولية الأشخاص وأيضا الجزاءات والتدابير المعنوية[3].

وفي إطار التعاون نصت الاتفاقية على أن " تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم، " كما أنه يمكن لأي طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريع مثل الفاكس او البريد الإلكتروني على ان تستوفي تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك.[4]

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الدولية إن المنظمات الدولية

إن المنظمات الدولية في سعي دائم للحفاظ على السلم والأمن الدوليين وخاصة بعد انتشار الجرائم المعلوماتية مما سهل انتشارها خاصة بعد ظهور الارهاب الالكتروني سارعت من اجل التدخل بهدف الوقاية منها ومكافحتها وهو ما سوف نستعرضه من خلال هدا الفرع لبعض المنظمات الدولية التي اهتمت بمكافحة الارهاب الالكتروني.

---

[1] المادة 1 من معاهدة بودابست2001

[2] وهو من المادة 23 حتى 35.

[3] طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة مكملة لنيل شهادة الماجستير في العلوم القانونية، قسم الحقوق، جامعة الجزائر1، 2013، ص65.

[4] عوينات بن عمر نجيب، المرجع السابق، ص18.

أولا: جهود منظمة الأمم المتحدة ومجموعة الدول الثمانية

في سعي دائم للحفاظ على الأمن الدولي وذلك بعد الانتشار الرهيب للجرائم خاصة بعد اقترانها بالشبكة المعلوماتية، مما سهل وسرع انتشارها فكان لابد من التدخل السريع من أجل الحد منها خاصة بعد ظهور الإرهاب الإلكتروني الذي سارعت كل من منظمة الأمم المتحدة ومجموعة الدول الثمانية بوضع مجموعة من القرارات والقوانين من أجل مكافحته.

1.منظمة الأمم المتحدة

أصدرت الأمم المتحدة مجموعة من القوانين عبر جمعيتها العامة التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداما غير سلمي، ففي 22 نوفمبر 2002 اتخذت قرار بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس السنة اتخذت قرار إرساء ثقافة عالمية لأمن الفضاء الإلكتروني واعتبر من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الإرهاب الإلكتروني. [1]

وقد أكدت تقارير وقرارات صادرة عن الأمم المتحدة مؤخراً تأكيدا خاصا على أهمية مكافحة استخدام الانترنت في أغراض إرهابية باعتبارها جزءًا رئيسيا من أي إستراتيجية شاملة لمكافحة الإرهاب، ففي تقرير الأمين العام المقدم للجمعية العامة عن عام 2006 والذي حمل عنوان "الإتحاد" في مواجهة الإرهاب توصيات الإستراتيجية عالمية لمكافحة الإرهاب" أفاد الأمين العام صراحة بأن القدرة على إيجاد الأموال ونقلها، وعلى حيازة الأسلحة وتجنيد الكوادر وتدريبها على الاتصال خاصة باستخدام الانترنت هي كلها عناصر أساسية بالنسبة للإرهابيين، واستطرد الأمين العام مؤكدًا على أن الانترنت قد باتت أداة تتسارع وتيرة توسع الإرهابيين في استخدامها في تجنيد الأفراد ونشر المعلومات والدعاية، الأمر الذي لابد من مواجهته بعمل منسق بين الدول الأعضاء مع احترام حقوق الإنسان والتقيد بالالتزامات الأخرى التي يفرضها القانون الدولي[2].

هذا وقد نبه مجلس الأمن في القرار ذي العدد (1963) لعام 2010) إلى ازدياد استخدام الإرهابيين التكنولوجيا الجديدة للمعلومات والاتصالات وخاصة الإنترنت لأغراض التجنيد عبر الإنترنت وكذلك التحريض على دعم الأعمال الإرهابية بوصفها أنماط مستحدثة الاستخدامات الإرهابيين للإنترنت لمعطيات الشبكة الدولية للمعلومات، وكان القرار ذي العدد (2255 في شباط عام (2015) أكثر شمولا لطرق استخدام الإرهابيين للإنترنت في أنشطتهم الإرهابية، إذ تضمن الإعراب عن قلقه من تزايد لجوء

[1] بوحادة سارة، **أثر الإرهاب الإلكترونى على أمن واستقرار الدول**، المدرسة الوطنية للعلوم السياسية، الجزائر، 2016، ص 13

[2] دريعي عبد السادة سحر، مرجع سابق، ص 41

الإرهابيين إلى استعمال تكنولوجيا المعلومات ولاسيما شبكة الإنترنت من أجل تسيير الأعمال الإرهابية والتحريض الإرهاب أو تجنيد مرتكبيها أو تمويلها".[1]

وفي مؤتمر منظمة الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية عام (2010)، عقد هذا المؤتمر في سلفادور البرازيل من 1912 نسيان عام 2010) تحت عنوان إستراتيجيات شاملة في تحديات عالمية والذي نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، وتضمن جدول الأعمال ثمانية بنود وكان من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة هذه الجريمة .[2]

2. مجموعة الدول الثمانية

عملت مجموعة الدول الثمانية على مكافحة الإرهاب الإلكتروني من خلال الإعلانات والمؤتمرات والملتقيات والاجتماعات حيث سعت إلى تعزيز الحرية والديمقراطية وحقوق الإنسان والتعاون الدولي في القضايا المتعلقة بالانترنت حيث أنشأت الفريق الفرعي للجرائم الإرهابية الإلكترونية التقنية في قمة مجموعة (G-8) في (2004/10/11) حيث تم اعتماد وزراء العدل والداخلية التابعين لبلدان المجموعة في اجتماعاتهم المختلفة آلية لمكافحة العديد من جرائم الإنترنت.

وتستند إلى المبادئ التالية:[3]

– التنسيق بين جميع الدول المعنية بملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بصرف النظر عن مكان حدوث الضرر

عدم إتاحة ملذات آمنة للمعتدين على تكنولوجيا المعلومات تدريب الموظفين المكلفين بتنفيذ القوانين، إضافة لتجهيزيهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالمية[4].

كما ناقشت مجوعة الدول الثماني في (موسكو روسيا) سنة 2006 الجريمة الإرهابية الإلكترونية وقضايا الفضاء الإلكتروني وأصدرت بيان موسكو الذي تم التأكد فيه على منع الأعمال الإجرامية المحتملة واتخاذ التدابير الضرورية، وكذلك اجتمع وزراء العدل والداخلية لدول (G-8) في 23-25 ماي عام 2007 في (ميونيخ ألمانيا) واتفق الأعضاء على العمل من خلال الأطر القانونية لتجريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية.[5]

وفي عام 2011 في فرنسا أصدرت أيضا الدول الثمانية الجزء الثاني من الإعلان في قضايا الإنترنت في البنود 4) إلى (22) حيث أكدت فيه أن شبكة الإنترنت أصبحت ضرورية في كافة أنحاء العالم، حيث

---

[1] الشمري نايف أحمد ضاحي، العبيدي عمر عباس خضير، **جرائم الأمن السيبراني واليات مكافحتها في إطار القانون الدولي**، المؤتمر الدولي الخامس للقضايا القانونية، 2021، ص 406

[2] الشمري نايف أحمد ضاحي، العبيدي عمر عباس خضير، مردع سابقص 406.

[3] شاشوة ياسمينة، المرجع السابق، ص 82.

[4] المرجع نفسه.

[5] المرجع نفسه.

تلعب دورا في نمو المجتمعات واقتصاديات الدول وتعزيز الحرية والديمقراطية وحقوق الإنسان حيث دعى الإعلان إلى تعزيز التعاون داخل جميع المحافل الدولية التي تتناول حركة الانترنت. [1]

ثانيا: جهود المنظمات العالمية المتخصصة

وهما المنظمة العالمية للملكية الفكرية ومنظمة التعاون الاقتصادي

1. المنظمة العالمية للملكية الفكرية

تم التوقيع على الاتفاقية المنشئة لها في ستوكهولم 1967، وأصبحت تابعة لأمم اعتبارا من عام 1974، تشجع هذه المنظمة على توقيع معاهدات دولية جديدة والتنسيق بين التشريعات القومية وتقديم المساعدات القانونية للدول النامية بهدف حماية الملكية الفكرية وتنميتها، ومع تزايد حاجة المنظمة على غرار باقي المنظمات لحماية البرامج شكلت مجموعة عمل تضم عددا من الخبراء بهدف حماية برامج الحواسيب من التهديد أو الهجوم الإلكتروني حيث أفضى ذلك بعد سلسلة من الاجتماعات إلى انتهاج أغلب الدول والميل إلى برامج الحاسوب لقوانين حماية حق المؤلف .[2]

2. منظمة التعاون الاقتصادي والتنمية.

تسعى منظمة التعاون الاقتصادي والتنمية بأول مبادرة دولية لها أن تتعامل مع المشكلات المتمثلة بالاعتداء على الأموال المعلوماتية والمتكونة من مجموعة الأدوات المكونة للحاسوب والبرامج والبيانات والتي يترتب عليه مشكلات قانونية. [3]

إن الهدف من هذه المنظمة من هذه المنظمة تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية يظهر اهتمام هذه المنظمة بالجرائم الإرهابية الإلكترونية الدولية من خلال وضعها لعديد من الأدلة التي تبناها مجلس المنظمة مع توصية الأعضاء بالالتزام بها في سبيل مكافحة الإرهاب الإلكتروني، كما عملت أيضا على إرسال استبيان إلى الدول الأعضاء فيها لتحديد مفهوم جرائم الحاسوب وتعريفها مع تبيين أفعال جرائم الإرهاب الإلكتروني وتكييف نصوص الاتفاقيات الدولية لمكافحة هذه الأنشطة المستحدثة، وقامت هذه المنظمة في عام 1983 بعقد اجتماع في باريس للبحث في جرائم الإرهاب الإلكتروني [4]

3. دور الانتربول في مكافحة الجريمة الارهابية الالكترونية المنظمة

تسهل منظمة الشرطة الجنائية الدولية أعمال إنفاذ القانون عالميا, وتدعم وتساعد جميع المنظمات والهيئات التي تتمثل مهمتها في منع أو مكافحة الجريمة بكل أنماطها المعروفة, كما يهدف الإنتربول

---

[1] المرجع نفسه، ص 83.

[2] علي بوعمرة، **جريمة الارهاب الالكتروني**، مذكرة ماستر في الحقوق، تخصص : قانون جنائي وعلوم جنائية، جامعة العربي تبسي، تبسة، الجزائري، 2020-2021ص 40.

[3] يونس عرب، **جرائم الكومبيوتر والإنترنت**، ط 1 اتحاد المصارف العربية، بيروت، 2002، ص322

[4] المرجع نفسه، ص 322.

الدولي لتحقيق التنمية الاقتصادية والاجتماعية وفقا لروح الإعلان العالمي لحقوق الإنسان من جانب أمني فقط دون أي تدخل في الأنشطة ذات الطابع السياسي أو العسكري أو الديني[1]

منظمة دولية حكومية لها كيان دائم وتتمتع بالشخصية القانونية الدولية [2]كما تعد اكبر منظمة دولية انشات في عام 1923 مكونة من قوات الشرطة لـ 194 دولة ومقرها الرئيسي في مدينة ليون بفرنسا تلعب المنظمة الدولية للشرطة الجنائية الانتربول عددا من الادوار الهامة في مختلف جوانب الجنائية للتحقيقات المتعلقة بملفات الاشخاص المفقودين والاتجار بالبشر وتهريب المخدرات والممنوعات وغيرها من الجرائم ذات الصلة التي تمتد عبر الحدود الدولية وقد انشئت في عام 1923 حيث تسهل المنظمة تعاون الشرطة عبر الحدود وتدعم وتساند جميع المنظمات والسلطات والمصالح التي تتمثل مهمتها في منع الجريمة الدولية ومكافحتها[3]

تهدف هذه المنظمة إلى رفع مستوى التعاون بين أجهزة تنفيذ القوانين في الدول المختلفة في مختلف المجالات من تبادل المعلومات والتحري والمتابعة القانونية، وتوحيد الإرادة السياسية للدول بشأن التصدي لهذه الجريمة، وتشجيعها على تطوير التشريعات بما يكفل مكافحة الجريمة المنظمة بصورة فعالة.[4]

وقد حددت المادة الثانية من القانون الأساسي للمنظمة أهدافها على النحو التالي:

1- تأكيد وتطوير المساعدة المتبادلة وعلى أوسع نطاق بين سلطات الشرطة الجنائية في إطار القوانين المعمول بها في مختلف الدول وعلى ضوء الإعلان العالمي لحقوق الإنسان.

2- إنشاء وتطوير كافة النظم الفعالة للوقاية من الجرائم والعقاب عليها، وقد حظرت المادة الثالثة من الميثاق المذكور التدخل في الشؤون ذات الطابع السياسي أو العسكري أو الديني أو العرقي أو ممارسة أي نشاط من هذا القبيل.

وينتج عن ثبوت صفة العضوية في منظمة الإنتربول، إلزام الدول الأعضاء بالالتزامات الواردة في دستور المنظمة المتمثلة في الآتي:

أ- احترام سيادة الدول الأعضاء في المنظمة، وذلك بالقيام بتعاون شرطي في حدود ما يسمح به قانون الدول الأعضاء في منظمة الإنتربول (المادة الثانية من دستور المنظمة).

---

[1] عمروش الحسين، **آليات مكافحة جريمة الفساد في نطاق منظمة الشرطة الجنائية الدولية**، الملتقى الوطني حول مكافحة الفساد وتبيض الأموال، يومي 10-11 مارس 2009، ص 01

[2] فنور حاسين، **المنظمة الدولية للشرطة الجنائية والجريمة لمنظمة**، رسالة ماجستير، كلية الحقوق، جامعة الجزائر ،السنة الجامعية2013-2014، ص 35

[3] نفس المرجع، ص 35

[4] يوبي سعاد، **الإنتربول كآلية دولية شرطية لمكافحة جريمة الفساد**، المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار، الجزائر المجلد03 ، العدد01، جوان2019، ص 114

ب- أن يكون التعاون في نطاق منظمة الإنتربول لا علاقة له بأي نشاط ذو طابع سياسي أو عسكري أو ديني (المادة الثالثة من دستور الإنتربول، وإنما هو تعاون يستهدف مكافحة جرائم القانون العام مثل القتل والسرقة وتزييف العملة، والاتجار في المخدرات أو في الرقيق.

ج- تلتزم الدول أعضاء الإنتربول بالتعاون مع بعضها في مكافحة الجريمة دون أن تقف الحواجز الجغرافية أو العضوية عائقا في سبيل تحقيق هذا التعاون.

د- تلتزم الدول الأعضاء بأن تتعاون من خلال المكاتب المركزية الوطنية للشرطة الجنائية الدولية الموجودة في إقليم كل منها كافة الأجهزة الموجودة في الدول والمتعلقة بمكافحة الجريمة.

هـ- ج- تلتزم الدول الأعضاء بأن تنشئ في إقليم كل منها مكتب مركزي وطني للشرطة الجنائية الدولية بناء على نص المادة (32) من دستور المنظمة .

و- تلتزم كافة الدول الأعضاء في المنظمة بالإسهام في النفقات المالية للمنظمة طبقا للمادة 38 الفقرة ألف من دستور المنظمة.[1]

ز- تلتزم الدول الأعضاء في المنظمة بتنفيذ القرارات الصادرة عن المنظمة بناء على نص المادة التاسعة من دستور المنظمة.

ح- تلتزم الدول الأعضاء في المنظمة بتنفيذ القرارات الصادرة عن المنظمة بناء على نص المادة التاسعة من دستور المنظمة..[2]

إن المهمة الرئيسية للمنظمة الدولية للشرطة الجنائية الانتربول هي تأمين التعاون المستمر بين الدول وتحديدا بين أجهزتها الأمنية في مجال مكافحة الجريمة، وخاصة في ظل تصاعد معدل الجريمة المنظمة بوتيرة لم يسبق لها مثيل لكونها أصبحت لا تقتصر على الجرائم التقليدية بل توسعت لتشمل الجرائم الحديثة التي تأثرت بالتطور التكنولوجي لمختلف مجالات الحياة في جميع الدول. ولقد نصت المادة الثانية من القانون الأساسي للمنظمة على أنها تعمل على تأمين وتنمية التعاضد على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار الأنظمة القائمة في مختلف الدول والبيان العالمي الحقوق الإنسان، كما تهدف المنظمة إلى إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفاعلة في الوقاية من جرائم القانون العام، وقد أوضحت المادة الثالثة من القانون الأساسي أنها تحظر على المنظمة أي نشاط يتعلق بالقضايا ذات الطابع السياسي أو العسكري أو الديني أو العنصري[3].

وتماشيا مع تطورات صور الإجرام المنظم العابر للحدود الوطنية أنشأت المنظمة الدولية للشرطة الجنائية (الأنتربول) فرعا للجريمة المنظمة ألحق بالسكرتارية العامة لإجراء كافة الدراسات

---

[1] يوبي سعاد، المرجع السابق، ص 114

[2] نفس المرجع، ص 115

[3] غربي أسامة، **المنظمة الدولية للشرطة الجنائية الانتربول، ودورها في مكافحة الجريمة المنظمة،** مجلة دراسات وأبحاث، المجلد 03- العدد الثالث، 2018، ص 157

المتصلة بهذا النوع من الإجرام كما نظمت قاعدة معلومات للمنظمات الإجرامية تشمل جميع الأشخاص المتورطين في الأعمال غير المشروعة[1]. وفي عام 1993 أنشأت الأنتربول **وحدة تحليل للمعلومات الجنائية** ملحقة بالسكرتارية العامة تهدف إلى وضع طريقة شاملة لتحليل الجريمة وظيفيا ومهنيا باستخدام أساليب معينة لمساعدة الدول الأعضاء[2].

ولقد لعبت **المنظمة الدولية للشرطة الجنائية** دورا هاما في تحديد معايير مفهوم الجريمة المنظمة من خلال عقدها المؤتمر الخامس للتصدي للجريمة المنظمة عبر الوطنية في ليون بفرنسا سنة 1996 حيث حددته السكرتارية العامة للمنظمة بالعناصر اللازمة لتعريف الجريمة المنظمة والمتمثلة في

- إتحاد يضم أكثر من شخصين، التخصص في نشاط محدد(نوعي).
- الاستمرارية لفترة طويلة أو غير محددة المدة، قوام المنظمة الطاعة والانضباط.
- ارتكاب الجرائم الخطيرة لا تتوان عن استخدام العنف ووسائل إرهابية أخرى.
- اتخاذ هيكلية وبنيان اقتصاد السوق، التفنن في عملية غسيل الأموال[3]:

كما تعمل منظمة الشرطة الجنائية على تنظيم المؤتمرات لدراسة ظاهرة الجريمة المنظمة، وتوثيق التعاون فيما بين الدول[4].

و يمارس المكتب التابع لمنظمة الشرطة الدولية عمليات الملاحقة إذا ما توصل إلى علمه البحث عن أحد الأشخاص بناء على نشرة دولة أو إرسالية من قبل مكتب الأنتربول، يتضمن وصفا دقيقا للواقعة وبيانات الشخص محل البحث فيقوم هذا الأخير بالتأكد من وجود الشخص المطلوب على إقليم الدولة، ويصدر أمرا بضبطه واحتجازه بمعرفة الانتربول، ويقوم بإعداد مذكرة وافية بالواقعة ويتم حجز المعني لحين ترحيله إذا وافقت الدولة على تسليمه.

ومن أهم عمليات التسليم التي تمت بفضل منظمة الشرطة الدولية قيام أمانة المنظمة بإبلاغ استونيا أنها تلقت من الولايات المتحدة عن عامي 2009 و2010 ثلاثة طلبات تسليم لثلاثة مجرمين متهمين بالانتماء لمنظمات إجرامية، كانوا قد ارتكبوا جرائم احتيال في مصر باستخدام الحاسوب، واستخدمت في تقديم تلك الطلبات اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية

---

1 محمد مسفر عبد الخالق الشمراني، **الجريمة المنظمة وسياسة المكافحة في التشريع الإسلامي والقانون الجنائي الإسلامي والأنظمة الجنائية المعاصرة لجريمة تهريب المخدرات،** (بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية)، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2001،ص 198.

2 تبادل المعلومات والخبرات في المجالات الأمنية والقضائية، ورقة عمل مقدمة من قبل الوفد اللبناني إلى الاجتماع الأول لرؤساء النيابات العامة (الإدعاء العام) في الدول العربية،عمان 7-2007/08/10،ص 8.

[3] فنور حاسين، **المنظمة الدولية للشرطة الجنائية والجريمة المنظمة،** مذكرة للحصول على شهادة الماجستير في القانون الدولي والعلاقات الدولية، كلية الحقوق بن عكنون، جامعة الجزائر 2012-2013،ص 60.

[4] نهايلي رابح، قيرة سعاد، **دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)** مجلة البحوث القانونية والاقتصادية، المجلد 04-العدد 02- 2021، ص 133

كأساس قانوني، ومعاهدة تسليم المجرمين لعام2006 المبرمة بين حكومة استونيا وحكومة الولايات المتحدة، واتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، وسلمت إستونيا المجرمين الثلاثة إلى الولايات المتحدة ولا تزال قضاياهم قيد النظر.[1].

كما أولت المنظمة اهتماما خاصا بمكافحة الجريمة المنظمة من خلال العديد من القرارات الهامة التي تم اتخاذها على مستوى الجمعية العامة للانتربول، ومن أهم هذه القرارات القرار رقم 17/ AGN/57/RES الذي تم اتخاذه خلال دورة الجمعية العامة 57 المنعقدة في بانغوك عام 1988 بعنوان الجريمة المنظمة، والقرار AGN/ 62/RES/8 الذي تم تبنيه في دورة الجمعية 62 المنعقدة في أوربا عام 1993 تحت عنوان التعاون الدولي والحرب ضد الجريمة المنظمة. كما أعلنت الجمعية العامة للانتربول في جلستها السابعة والستين في القاهرة عام 1998 بأن محاربة الجريمة المنظمة يمثل إحدى أولويات الشرطة الدولية في قيامها بالدور الهام المتمثل بتنسيق تعاون الشرطة الدولية ضد الجريمة المنظمة[2].

وقد أشار المؤتمر الدولي لقانون العقوبات المنعقد في بودبست عام 1999 إلى التطور الملحوظ في مجال التعاون الشرطي لمكافحة الجريمة من خلال استخدام وسائل وقنوات جديدة للاتصال بين العديد من الدول، والتعاون مع الأجهزة الشرطية الإقليمية مثل "الإيربول" في أوروبا، واستخدام الوسائل التكنولوجية الحديثة كنظام المراقبة عبر الحدود بواسطة الأقمار الصناعية[3].

تعتمد المنظمة الدولية للشرطة الجنائية لتحقيق أهدافها دوليا على مجموعة من الوسائل نجيز أهمها على النحو الأتي:

1- **منظومة اتصالات الأنتربول العالمية:**مع الضعف المتزايد لمعنى الحدود الوطنية بالنسبة للمجرمين تزايدت أهمية الاتصالات الشرطية الفعالة عبر الحدود أكثر من أي وقت مضى، وتتمثل إحدى مهام الأنتربول الأساسية في تمكين أجهزة الشرطة في العالم من تبادل المعلومات بشكل مأمون وفعال. وقد طور الأنتربول منظومة الاتصالات الشرطية العالمية "24/7 " لوصل أجهزة إنفاذ القانون في البلدان الأعضاء، الأمر الذي يتيح للمستخدمين المرخص لهم تبادل البيانات الشرطية الهامة فيما بينهم والوصول إلى قواعد بيانات المنظمة وخدماتها على مدار الساعة [4].

ولتعميم نظم الاتصالات العالمية تم إبرام اتفاق بين الأنتربول والمحكمة الجنائية الدولية في سنة 2005، منح بموجبه للمحكمة الجنائية الدولية حق الوصول إلى منظومة الأنتربول العالمية للاتصالات الشرطية، وذلك فيما يتعلق بتبادل المعلومات الشرطية وإجراء التحليلات الجنائية، والبحث عن المجرمين

[1] بوعكاز أسماء،مباركي دليلة، المرجع السابق، ص 128

[2] غربي أسامة، المرجع السابق، 158

[3] نهايلي رابح، المرجع السابق، ص 133

[4] غربي أسامة، المرجع السابق، ص 158

الفارين وإصدار وتعميم نشرات الأنتربول، وأصدر الأنتربول أول نشرة حمراء ضد 5 أشخاص مطالبين أمام المحكمة الجنائية الدولية، لارتكابهم جرائم حرب وضد الإنسانية في شمال أوغندا ومن بينهم رئيس المجموعة الجنرال JOSEPH KONY الذي وجهت إليه 21 جريمة ضد الإنسانية،و 21جريمة حرب في جوان 2016. "[1]

2- **الاتصالات اللاسلكية:** وهي تشكل أداة جوهرية بحيث تعد الاتصالات الدولية السريعة والمضمونة شرط لا غنا عنه للتعاون، لذلك فإن الدول الأعضاء في المنظمة ترتبط فيما بينها وبين الأمانة العامة بشبكة اتصالات لاسلكية كهربائية متنقلة، وهي شبكة الاتصالات اللاسلكية للشرطة، بحيث ترتبط جغرافيا بمحطات إقليمية وتتصل من خلالها بالمحطة المركزية القومية الواقعة في فرنسا تعمل على توجيه رسائل بين المكاتب المركزية القومية أو مع الأمانة العامة في أقصى سرعة ممكنة وتساعد على النقل السريع للصور والبصمات الخاصة بالأصابع عن طريق نظام التصوير اللاسلكي ،ومن خلاله يمكن الكشف السريع مابين الدول على المسالك التي تعتمد عليها عصابات الجريمة المنظمة العابرة للحدود الوطنية

3- **النشرات الدولية** : هي العروة الوثيقة بين منظمة الشرطة الجنائية وبين الدول الأعضاء والكيانات الدولية لتحقيق متطلبات التعاون الجنائي على المستوى الدولي، ولضمان مكافحة الجريمة وضبط المطلوبين في أي مكان من العالم ومحاكمتهم عما اقترفوه، وأهم هذه النشرات[2]:

أ- **النشرة الدولية الحمراء:** تعد أقوى النشرات الدولية الصادرة من قبل الأمانة العامة للمنظمة، بناء على طلب من أحد المكاتب المركزية الوطنية لأي من الدول الأعضاء

- النشرة الزرقاء : جمع معلومات إضافية عن هوية شخص أو نشاطاته غير المشروعة في سياق قضية جنائية .

- النشرة الخضراء: للتزويد بالتحذيرات بشأن أشخاص ارتكبوا جرائم جنائية ويرجح ارتكابهم جرائم مماثلة في بلدان أخرى.

- النشرة الصفراء : للمساعدة على تحديد مكان أشخاص مفقودين لاسيما القاصرين أو على تبيين هوية أشخاص عاجزين عن التعريف بأنفسهم .

- النشرة السوداء : للحصول على معلومات عن جثث مجهولة الهوية .

- النشرة البرتقالية : لتحذير الشرطة والهيئات العامة والمنظمات الدولية من مواد خطرة أو أحداث أو أعمال إجرامية يمكن أن تمثل خطرا على الجمهور.[3].

---

[1] يوعكاز أسماء، مباركي دليلة، المرجع السابق، ص 125

[2] نفس الرجع،، ص124

[3] غربي أسامة، المرجع السابق، ص 160

المطلب الثاني: مكافحة الإرهاب الالكتروني على الصعيد الاقليمي

نستعرض من خلال هذا المطلب إلى الجهود الاقليمية في مكافحة الجريمة الالكترونية المنظمة حيث نتطرق من خلال الفرع الأول إلى مكافحة الإرهاب الالكتروني على المستوى الاوروبي، ثم جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني في الفرع الثاني

الفرع الاول: مكافحة الإرهاب الالكتروني على المستوى الاوروبي

اعتمدت الدول الاوروبية اتفاقية سنة 2001 تهدف إلى تقديم المساعدة للبلدان من أجل مكافحة جرائم الانترنت من قبل المجلس الأوروبي، وتم التصديق عليها من قبل دول الأطراف المعنية سنة 2010، وتتجلى أهدافها في مجال التصدي للجرائم المعلوماتية فيما يلي:

سن قوانين ضرورية للتعامل مع مختلف أنواع جرائم التقنية العالمية مع إعطاء الحكومات حق المراقبة وتقديم المساعدة اللازمة بين الدول الأطراف في جمع الأدلة وفرض القانون، إستوجاب إصدار قوانين جديدة في كافة دول العالم تجرم الجرائم الالكترونية او تحديث قوانين تقليدية بهد تحقيق التناسق الكافي بينها. [1]

اعتمدت الدول الأعضاء هذه الاستراتيجية بتاريخ 08 سبتمبر 2006 ، والتي أتت على شكل قرار أو خطة عمل من شأنها تحسين التعاون الدولي في مجال مكافحة الإرهاب الإلكتروني، حيث جاء في المادة الثانية من الفقرة الثانية من نص البيان " :الاستفادة من الإطار الذي تتيحه المنظمات الدولية والإقليمية ودون الإقليمية المعنية لتبادل أفضل الممارسات في مجال بناء القدرة على مكافحة الإرهاب، وتيسير إسهامها في الجهود التي يبذلها المجتمع الدولي في هذا المجال[2] "

تتناول اتفاقية برن، التي اعتمدت بتاريخ09 سبتمبر 1886حماية المصنفات وحقوق مؤلفيها . وتتيح الاتفاقية للمبدعين، مثل المؤلفين والموسيقيين والشعراء والرسامين وما إلى ذلك، سبل التحكم في طريقة استخدام مصنفاتهم ومن يستخدمها وبأية شروط .وتستند الاتفاقية إلى ثلاثة مبادئ أساسية وتشمل مجموعة من الأحكام المتعلقة بالحد الأدنى للحماية الواجب منحها وبعض الأحكام الخاصة التي وضعت لمصلحة البلدان النامية التي ترغب في استخدامها[3].

في عام 2002 اعتمد مجلس الإتحاد الأوروبي القرار الإطاري (JHA/2002/475) الصادر في 13 حزيران / يونيه 2002 بشأن مكافحة الإرهاب والذي يوحد تعريف الجرائم الإرهابية في جميع دول الأعضاء في الاتحاد الأوروبي عبر طرح تعريف محدد ومشترك لمفهوم "الإرهاب" ويُؤسس قواعد للولاية

---

[1] جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات**، الطبعة الأولى، دار البداية، ليبيا، 2010، ص 229-228 .

[2] هلالي عبد إلاه احمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية**، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007، ص 05

[3] جغدم محمد الأمين، **جرائم الارهاب الالكتروني والجرائم المنظمة**، مجلة القانون الدولي والتنمية، المجلد06، العدد01، 2018ص 238

القضائية لضمان إمكانية ملاحقة الجرائم الإرهابية قضائيا بفاعلية، ويُبين تدابير محددة فيما يخص ضحايا الجرائم الإرهابية، وفي إطار التصدي لخطر الإرهاب المتزايد بما يشمل استخدام تكنولوجيا جديدة مثل الانترنت، عدل القرار الإطار (JHA/2002/475) في عام 2008 ليتضمن على وجه التحديد أحكاما بشأن التحريض العلني على ارتكاب جرائم إرهابية والتجنيد والتدريب بغرض الإرهاب، وفي ذلك القرار أتى مجلس الاتحاد الأوروبي أيضا على ذكر قرار مجلس الأمن رقم 1624 (2005) الذي دعا فيه المجلس الدول أن تحظر بنص القانون التحريض على ارتكاب عمل إرهابي أو أعمال إرهابية وأن تمنع ذلك التصرف.[1]

ويوفر القرار الإطاري (JHA/2008/919) سند للملاحقة القضائية بشأن نشر الدعاية الإرهابية والدراية الفنية اللازمة لصنع القنابل عبر الانترنت، إذ كان هذا النشر متعمدا ومستوفيا لشروط الجرائم المذكورة، وتستند تعديلات القرار الإطاري (JHA/2002/475) فيما يتعلق بالتحريض العلني والتجنيد والتدريب إلى أحكام مشابهة في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، وقد استحدث القرار الإطاري (JHA/2008/919) جرائم جديدة فيما يتعلق بالسلوكيات التي قد تؤدي إلى أعمال إرهابية بغض النظر عن الوسائل أو الأدوات التكنولوجية التي ترتكب هذه الجرائم عبرها، وكما هو الحال في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، تشمل أحكام القرار الإطاري (JHA/2008/919) الأنشطة التي تمارس عن طريق الانترنت وإن كانت غير مخصصة لها.[2]

الفرع الثاني: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني

تصدت جامعة الدول العربية كمنظمة إقليمية عربية للأنشطة غير المشروعة المرتكبة بواسطة تقنية المعلومات وأن ميثاقها لا ينص صراحة على مكافحة الإرهاب وما يرتبط به من تفرعات، ولكن المادة (2) منه أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها، وهذا ما تنطوي عليه وسائل الإرهاب الإلكتروني من تجاوزات وإخلال السلطة وسيادة الدول عبر التعرض لنظم المعلومات بالمؤسسات السيادي، فضلا عن إمكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدول العربية المستهدفة الأمر الذي يستدعي الدول العربية لمواجهة مثل هذه الأنشطة الإرهابية في الفضاء الإلكتروني، وهو اتجاه أكدته المادة (3) من الميثاق حينما حولت مجلس الجامعة بتقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن والسلم، ويمكن اعتبار الاعتداء على نظم المعلومات التي تعتمده المؤسسات الرسمية للدول العربية ومحاولة تدميرها أو الإضرار بها وإشاعة الرعب والتحريض ضد النظام القائم التي تتم عبر آليات الإرهاب الإلكتروني من صور العنوان وفقا لقواعد القانون الدولي وميثاق منظمة الأمم المتحدة.[3]

---

[1] سحر عبد السادة دريعي، مرجع سابق، ص 38

[2] نفس المرجع.

[3] شاشوة ياسمينة، المرجع السابق، ص 100.

تمكنت الدول العربية من تعزيز جهود التعاون (الأمني، والقضائي، والتقني) بينها في مجال مكافحة الإرهاب الإلكتروني من خلال التوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرَّرة في القاهرة بتاريخ 21 ديسمبر عام 2010، والتي تضم العديد من الجرائم الإلكترونية[1] مثل: سرقة بطاقات الائتمان، وجرائم الإنترنت والإرهاب الإلكتروني، وتصنيع الفيروسات أو نشرها، والقرصنة واختراق الأنظمة، والوصول والاختراق غير المشروع ... وغيرها، وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في محاربة الجرائم الإلكترونية، وتؤكد على أهمية تنفيذ قوانين حقوق الملكية، وتطبيق العقوبات على منتهكي شروط ولوائح الاتفاقية.

كما أقرت دول مجلس التعاون لدول الخليج العربي مرسوم رقم 27 لسنة 2008 بشأن اتفاقية لمكافحة الإرهاب بكافة صوره وأشكاله بما فيها الإرهاب السيبراني في إطار المسؤولية الجماعية في المحافظة على الأمن والاستقرار، بناءً على مبدأ الأمن الجماعي، واعتبار أمن واستقرار دول المجلس كلًا لا يتجزأ، ورغبة من دول المجلس في وقاية مجتمعاتها وشعوبها ومكتسباتها التاريخية ومنجزاتها الحضارية ومصالحها من خطر الإرهاب.

أما على صعيد المؤتمرات الإقليمية، فنذكر على سبيل المثال: المؤتمر الإقليمي للأمن السيبراني، والذي قامت مصر بالإشراف عليه في مدينة "شرم الشيخ" المصرية في أكتوبر 2016، وهدف المؤتمر إلى تعزيز التعاون الدولي؛ لمكافحة الإرهاب الإلكتروني وجرائم الفضاء السيبراني وتبادل الخبرات حول العالم[2]

وقد ناقشت دول الخليج في فاعليات مؤتمر "مواجهة التطرف الفكري"، والذي انعقد في دولة الكويت في شهر يناير 2017، مقترح إنشاء جيش خليجي إلكتروني لمواجهة الإرهاب عبر الإنترنت، على أن يتكون هذا الجيش المقترح من خبراء تقنيين واجتماعيين وشرعيين لتحليل المعلومات التي تم جمعها، خاصة وأن المنطقة الخليجية تحظى بالكفاءات والخبرات النادرة في هذا المجال، والتي أثبتت قدرتها وكفاءتها

وأيضًا منتدى "فرست الإقليمي" للمنطقة العربية والإفريقية، والذي استضافته مصر بمدينة شرم الشيخ في الفترة من 2–3 نوفمبر 2016، وتم من خلاله التأكيد على أهمية تبادل الخبرات والتعاون بين الدول والمنظمات الدولية والإقليمية. وكان من النجاحات المترتبة على هذا المؤتمر، عمل منصة تواصل مع المنظمات الأمنية العالمية الكبيرة كالاتحاد الدولي للاتصالات، وفريق الاستجابة لطوارئ الحاسب الآلي التابع لمنظمة التعاون الإسلامي

---

[1] شرف الدين وردة، **مكافحة جريمة تهريب المهاجرين في قانون العقوبات الجزائري** ،.مجلة الاجتهاد القضائي، العدد (10)، 2018، ص 93.

[2] فرج يوسف أمير، "**جريمة مكافحة الإرهاب الإلكتروني "الإرهاب الرقمي" في دول الخليج العربي في ظل اتفاقية دول مجلس التعاون لمكافحة الإرهاب**"، القاهرة: دار الكتب والدراسات العربية، الطبعة الأولى، 2016، ص 95

تم الاتفاق على إنشاء المنظمة العربية لمكافحة الجرائم المعلوماتية والإنترنت وهي منظمة عربية غير حكومية علمية ومهنية، ولها اهتمامات معينة ذات طابع قانوني واقتصادي، تعنى بتنظيم مختلف الأطر القانونية والإجرائية والمؤسسية لمكافحة الجرائم التي تتم عبر الإنترنت وكافة جرائم المعلومات، وتهدف هذه المنظمة إلى مكافحة الجرائم الإلكترونية بجميع أشكالها (الأجهزة والبرامج والشبكات والمعلومات والبيانات والأموال ووسائل الاتصال والجرائم ضد السمعة والجرائم ضد الشخصية) وأيضا تهتم بمكافحة الجرائم ضد الإنسانية وجميع أشكال الجرائم ضد الأمن القومي، وتسعى على العموم لمكافحة جميع الجرائم التي يكون أداة لارتكابها الحاسب أو الإنترنت أو يكونا أحد أهدافها [1]

[1] فيصل بدري، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، رسالة دكتوراه جامعة الجزائر 01- بن يوسف بن خدة- 2017/2018، ص91

المبحث الثاني: الجهود الوطنية لمكافحة الارهاب الالكتروني

في القانون الجزائري، يتم مكافحة الإرهاب الإلكتروني من خلال مزيج من التشريعات والقوانين التي تهدف إلى حماية الفضاء الإلكتروني ومنع استخدام الإنترنت لارتكاب أعمال إرهابية. تشمل هذه التشريعات قوانين متعلقة بالجرائم الإلكترونية، وقوانين مكافحة الإرهاب، بالإضافة إلى القوانين المتعلقة بحماية الأمن الوطني بالضافة إلى هيئات متخصصة، وهو ما سوف نتطرق اليه في المطلب الاول، كما تم استحداث اليات الجرائية للكشف عن هذه الجرائم وهو موضوع المطلب الثاني.

المطلب الاول: الاليات القانونية والمؤسساتية لمكافحة الارهاب الالكتروني

إن الجزائر شأنها شأن الدول الأخرى بعد معاناتها الطويلة من الإرهاب أصبحت ذات خبرة في التعامل معه، لذلك فإنه بعد بروز الإرهاب الإلكتروني سارعت مباشرة إلى من نصوص قانونية لمكافحته والتخلص منه، لذا خصصنا هذا المطلب لدراسة هذه الجريمة داخل الوطن وقد تطرقنا إلى ما يلي:

حيث صرح القائد العام للدرك الوطني الجزائري السابق في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول الأمن السيبراني"، حيث قال أن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر من خلال تنامي مظاهر الترويج لكل أشكال العنف ولإرهاب والتطرف باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الإلكترونية لذلك دعا إلى إطلاق خلايا أمنية متخصصة من أجل حماية المواطن الجزائري وخاصة عنصر الشباب.[1]

أما التنظيم الإرهابي "داعش" فله أزيد من 50 ألف موقع إلكتروني، 90 ألف باللغة العربية على موقع التواصل الاجتماعي "فيسبوك" و40 ألف بلغات أخرى، ورغم الخطورة الكبيرة التي يخلفها هذا التنظيم عبر مواقعه إلا أن تأثيره على المجتمع الجزائري كان قليلا، فقد كشف السيد محمد عيسى وزير الشؤون الدينية والأوقاف السابق أن التجنيد الإلكتروني لداعش في الجزائر عن طريق شبكة الانترنت ومواقع التواصل الاجتماعي لم يتجاوز 100 شاب جزائري [2]

إن هاته الحصيلة رقم ضئيل إذا ما قورن بعدد المجندين من دول عربية أخرى، وهذا يعود لنتائج العشرية السوداء التي عاشاها الجزائريون نهاية القرن الماضي. [3]

---

[1] بن مرزوق عنترة، الكر محمد، **البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب**، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان 2018، ص 37.

[2] المرجع نفسه.

[3] المرجع نفسه.

الفرع الثاني : إجراءات الوقاية لمكافحة الإرهاب الإلكتروني

سنتطرق من خلالها إلى عنصرين مهمين آلا وهما:

أولا: إنشاء مراكز التوجيه العسكري

إن الأزمات التي مرت بها الكينونة الجزائرية في القرن الماضي قد أظهرت بشكل جلي التحديات الأمنية الخطيرة التي مر بها العالم النظام الأمني الجزائري على غرار بقية الأنظمة لدول العالم الثالث خلال فترة التحول من الحرب الباردة إلى ما بعد هذه الحرب، وذلك من حيث بنائها وطرق التقرب منها والتحدي الوحيد الذي يواجهه النظام الأمني الجزائري على غرار النظام العالمي هو التهديدات التي يثيرها الإرهاب الحديث. [1]

وعلى هذا الأساس يأتي مركز التوجيه العسكري في عمليات مكافحة الإرهاب، وهي مقاربة إجرائية للحصول على نتائج إستراتيجية أو أثر عملياتي على التنظيمات الإرهابية المنتشرة إلكترونيا وحدوديا على وجه التحديد وذالك من خلال تطبيق تعاون مضاعف ومتعدد الجوانب على أوسع مدى للقدرات العسكرية والغير عسكرية، وهذه المقاربة تعتبر مقاربة تكيفية تتخذ شكلا متداخلا لتمتد وتشمل الأبعاد الميدانية والعملياتية والاستراتيجية لأي اشتباك.[2]

إن هذا الأساس المتين لهذه العمليات يتضمن خلق بعض الأحداث وحسن الاستفادة منها، وبالرجوع إلى الهدف الأساسي لمركز التوجيه العسكري الجزائري في مكافحة الإرهاب هو على المستوى الإستراتيجي أو السياسي فإن هذا يؤدي إلى مفهوم عمق الاستراتيجية وبأن الحرب نفسها هي ببساطة امتداد للسياسة بوسائل أخرى وهذا يتطلب الحاجة إلى توجيه سياسي حول إطار إستراتيجي، بحيث يجري التخطيط للعمليات المجدية في مركز التوجيه العسكري الجزائري في عمليات مكافحة الإرهاب والتي يمكن تعريفها بالتطبيق المتماسك والمترابط لكافة الموارد القومية وعلى مختلف الأصعدة الوطنية توجهها الأهداف الإستراتيجية، والجدوى من هذا المفهوم هو إعطاء القادة ذوي الفكر الواسع القدرة على تحديد هدف التنظيمات الإرهابية بطريقة تسهل تحقيق الهدف كاملا للإستراتيجية الحاذقة وهو استلام الجماعات الإرهابية دون قتال"، ما يعرف بالشلل الإستراتيجي للخصوم. [3]

وبالنظر إلى تزايد حجم التهديدات الإرهابية الخطيرة على الجزائر، تم في نهاية 2014 استحداث لجنة أمنية مشتركة متخصصة في مجال مكافحة الإرهاب من طرفي وزارتي الداخلية والدفاع، بالإضافة إلى تعقب المنتديات الجهادية في مسعى جديد يأتي في ظل تنامي المخاطر الأمنية، وعلى خلفية تزايد نشاط شبكات التجنيد التي تم تفكيكها من طرف وحدات الدرك الوطني ومصالح الأمن والجيش في العديد

---

[1] بلهول نسيم، **مفهوم المذهب العسكري الجزائري لثنائية بيئة الضبط العملياتي والدين في مكافحة الإرهاب**، مجلة العلوم القانونية والسياسية، جامعة ديالي العراق، العدد الأول 2015، ص 16.

[2] المرجع نفسه.

[3] المرجع نفسه، ص 17.

من ولايات الجمهورية، وبعدما كشفت أيضا الكثير من التحريات الأمنية الدقيقة عن وجود صفحات بمواقع التواصل الاجتماعي تروج للأفكار الجهادية المتطرفة، وتعمل أيضا في الجهة المقابلة على استقطاب مقاتلين مفترضين عبر الانترنت في سبيل الالتحاق بصفوف الجماعات الإرهابية في كل من العراق وسوريا وليبيا .[1]

ثانيا: إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

لقد عرفت الجزائر أزيد من 100 جريمة إلكترونية سنة 2014 وتضاعف هذا العدد خلال السداسي الأول لسنة 2015، حيث سجلت المصالح الأمنية أزيد من 200 جريمة إلكترونية متنوعة، وفي هذا الإطار عملت الدولة الجزائرية على تأسيس الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها في 9 أكتوبر 2015، بعدما وقع رئيس الجمهورية على مرسوم رئاسي يقضي بإنشاء هذه الجديدة والتي تعد بمثابة سلطة إدارية مستقلة لدى وزير العدل، كما تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسئولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقاء .[2]

كما تضم الهيئة قضاة وضباطا تابعين لمصالح الاستعلامات العسكرية والدرك والأمن الوطنيين، وأعوانا من الشرطة القضائية وفقا لأحكام قانون الإجراءات الجزائية، وتكلف هذه الآلية الجديدة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الحديثة، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام.[3]

وهنا على سبيل المثال كمحاربة كل المضامين الإرهابية المتطرفة التي تدعو إلى الغلو الديني أو تسعى إلى تجنيد الشباب الجزائري في صفوفها، كما تعمل هذه الهيئة على جمع المعلومات والتزويد بها من خلال الخبرات القضائية وضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي واستثناء هيئات وطنية أخرى.[4]

---

[1] بلهول نسيم، المرجع السابق، ص 17

[2] علي بوعمرة، المرجع السابق، ص 55.

[3] المرجع السابق، ص56.

[4] المرجع نفسه.

الفرع الثاني: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني والنتائج المحققة في هذا الإطار

قد خصصنا هذا الفرع للكشف عن النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني، والنتائج المتوصل لها.

أولا: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني

تندرج مكافحة الإرهاب الإلكتروني في الجزائر ضمن مكافحة الجريمة السيرانية بكافة أشكالها، مع أنه يوجد غموض وعدم دقة في النصوص القانونية الوطنية في تعريف هذا النمط من الجرائم المستحدثة، لقد تنبه المشرع الجزائري إلى ضرورة جعل المنظومة القانونية مواكبة للتطور الحاصل في تكنولوجيا المعلومات والاتصال في هذا الصدد، صدر القانون رقم 04-15 [1]المتعلق بالمعالجة الآلية للمعطيات (نوفمبر 2004)، ثم القانون رقم09-04[2] لسنة 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها . [3]

ومن التدابير المتخذة من قبل الحكومة الجزائرية ما يتعلق بالوقاية الإلكترونية التي تشمل كما حددها القانون 09_04 الوقاية من جرائم الإرهاب والماس بأمن الدولة، الوقاية من التعدي على أنظمة معلومات يكون هدفه المساس بالدفاع الوطني، ما تقتضيه التحريات والتحقيقات القضائية والمساعدات القضائية الدولية، كما نص القانون على قواعد تفتيش منظومات المعلومات وحجز المعطيات في إطار التحريات[4].

كما نص قانون العقوبات على عقوبات بالسجن والغرامة المالية، تختلف باختلاف الجريمة المرتكبة، مثال ذلك المادة 394 مكرر، مع مضاعفة العقوبة بالنسبة للجرائم التي تمس أمن الدولة والدفاع الوطني بنص المادة 394 مكرر 3 . [5]

واهتمت وزارة الدفاع الوطني بحفظ الأمن السيبراني، عبر وضع سياسات وبرامج واستحداث آليات لمكافحة الجريمة السيبرانية وحماية البيئة التحتية للمعلومات، تعبئة عدد من الأجهزة المتخصصة لحماية أمن الفضاء السيبراني والوقاية من الجريمة مثل: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا

---

[1] القانون رقم 04-15 المؤرخ في 10 نوفمبر2004 ، المتضمن قانون العقوبات المعدل والمتمم71 ، ج.ر، العدد 71 ص 11 و12

2 القانون 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق5 غشت سنة2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد47 ، الصادر بتاريخ25 شعبان عام 1430 هـ، الموافق 16 غشت سنة2004

[3] جعيجع عبد القادر، تيغزة زهرة، **تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة**، مجلة دفاتر السياسة والقانون، المجلد 13 العدد الأول، الجزائر، 2021، ص552

[4] المرجع نفسه.

[5] المرجع نفسه.

الإعلام والاتصال، هيئات ذات اختصاص إقليمي تعني بالجرائم الإلكترونية الواقعة خارج الحدود الوطنية والتي تمس الأمن الوطني، المعهد الوطني للأدلة الجنائية، وعلم الإجرام، المديرية العامة للأمن الوطني.[1]

وقد صدر القانون رقم 20_05 أفريل 2020[2]المتعلق بالوقاية من التميز ومكافحتهما، ليشكل تكملة لجملة القوانين والنصوص المتعلقة بمكافحة الإجرام ولإجرام الإلكتروني، ويهدف إلى أخلقة الحياة العامة مع توصية بإنشاء مرصد وطني للوقاية من التمييز وخطاب الكراهية، ينص القانون على تدابير وعقوبات متنوعة تمس كذلك من يستخدم تكنولوجيا الإعلام والاتصال وهنا إشارة إلى شبكات التواصل الاجتماعي) بغرض الدعاية والكراهية ونشر العنف، مع التنديد في جريمة استخدام هذه التكنولوجيا لنشر العنف في المجتمع.[3]

وكتقييم لبعض الجهود الدولية في مجال مكافحة الإرهاب الإلكتروني يمكن القول إن استمرار التطور التكنولوجي والاستخدام المتزايد لشبكة الانترنت من بين أهم التحديات التي تقف في وجه سياسات واستراتيجيات الدول، إلى جانب عدم وجود تعريف جامع للإرهاب الإلكتروني، والثغرات القانونية بالنسبة لهذا النوع من الجرائم، مثل غياب العنصر المادي أحيانا وصعوبة كشف الجريمة في حينها، يضاف إلى ذلك غياب سياسة تشريعية موحدة في مجال الإرهاب الإلكتروني كما هو الحال لدى الدول العربية[4].

ثانيا: النتائج المحققة في إطار مكافحة الإرهاب الإلكتروني في الجزائر

تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني، وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة ،إلكترونية، منها 30 بالمائة على مواقع التواصل الاجتماعي. [5]

هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016، وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بتهديدات إرهابية بإسم تنظيم داعش الإرهابي، لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء.[6]

---

[1] جعيجع عبد القادر، تيغزة زهرة، مرجع سابق، ص552.

[2] القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق ل 28 أبريل سنة 2020 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، الجريدة الرسمية، العدد25 ، الصادرة بتاريخ 6 رمضان 1441 هـ الموافق ل 29 أبريل سنة 2020م.

[3] عبد القادر جعيجع وزهرة تيغزة المرجع السابق، ص552-553

[4] المرجع نفسه، ص553.

[5] بن صويلح أمال، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام**، الملتقى الدولي حول الاجرام السيبرياني، المفاهيم والتحديات خطو هامة نحو مكافحة الارهاب الالكتروني في الجزائر، جامعة قالمة، يومي 11-12 افريل، 2017، ص 9.

[6] المرجع نفسه.

هذا وقد استطاع الجيش الإلكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا، كما تمكن من فك شفرات الرسائل المتبادلة، وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة، وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب اتصالات محلية ودولية[1]

المطلب الثاني: الاليات الاجرائية لمكافحة الارهاب الالكتروني

إن إجراءات البحث والتحري من الإجراءات الأولية الأساسية التي يشرع بها ضباط الشرطة القضائية، بحيث أن القانون جعلهم يتميزون بكل الحقوق والواجبات اللازمة خلال أداء مهمتهم ألا وهي كشف وقائع الجريمة والتحقيق مع المجرمين المتورطين، يكون ذلك مباشرة بعد وقوع الجريمة وتتوقف إجراءاتها بعد إحالة ملف القضية إلى قاضي التحقيق ومثول المتهم أمام القاضي الجزائي الاقتصادي والمالي، ويمكن إجمال هذه الإجراءات من حيث الاجراءات التقليدية (الفرع الاول) ثم الاجراءات المستحدثة (الفرع الثاني) على النحو التالي:

الفرع الأول :أساليب التحري التقليدية

تنص الفقرة الثالثة من المادة 12 من ق. إ. ج ويناط بالشرطة القضائية مهمة البحث والتحري على الجرائم المقررة في ق.ع. وجمع الأدلة عنها والبحث عن مرتكبها مادام لم يبدأ فيها التحقيق"[2]، ولقد نص المشرع الجزائري على توسيع الاختصاص المحلي للشرطة القضائية في الجرائم محل اختصاص الأقطاب الجزائية المتخصصة، وهذا ما نصت عليه المادة 16/7 من ق. إ. ج، ومنه نوضح عمل الشرطة القضائية كالتالي:

أولا: تفتيش المساكن.

إن المتتبع لأحكام قانون الإجراءات الجزائية يجده يخلو من ن ص صريح يضبط تفتيش المساكن بمناسبة جرائم معينة، إلا أن تفتيش المساكن إجراء يتخذ بمناسبة الجرائم الجسيمة الجنايات والجنح، ولا يحق تفتيش المساكن بحثا عن أدلة تخص مخالفة، لأنها من البساطة التي لا يجوز معها إهدار حرمة السكن.[3]

وقد حدد المشرع الآحكام الخاصة بتفتيش المسكن بموجب المادة44 و45 و 47من قانون الإجراءات الجزائية، وفق ضوابط معينة، الإذن والميقات وحضور صاحب المنزل، غير أنه عندما يتعلق الآم ر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الما س ة بأنظمة المعالجة

---

[1] بن صويلح أمال، مرجع سابق، ص 9.

[2] خلقي عبد الرحمان، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، ط. 4 دار بلقيس للنشر، الجزائر، 2019، ص 68.

[3] بارش سليمان، **شرح قانون الإجراءات الجزائية الجزائري**، دار الشباب بائنة الجزائر، طبعة 1986، ص 187.

الالية للمعطيات وجرائم تبييض الآموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف؛ فإنه يجوز إجراء التفتيش والمعاينة والحجز في المحل السكني في ال ساعة من ساعات النهار أو الليل، وذلك بنا ء على إذن مسبق من وكيل الجمهورية المختص، والذي قد يكون بمناسبة الجريمة الاقتصادية والمالية وكي ل الجمهورية لدى القطب الجزائي الاقتصادي والمالي، وتحت إمرته ضباط الشرطة القضائية، وفق ما نصت عليه المادة 211 مكرر 15 من الآمر 04-20 ، والتي تنص على أنه في حالة التخلي، تطبق أحكام قانون الإجراءات الجزائية المتعلقة بتحريك الدعوى العمومية وممارستها والتحقيق القضائي والمحاكمة.

ولقاضي التحقيق، عندما يتعلق بالجريمة الاقتصادية والمالية والجرائم المذكورة في المادة 47 من قانون الإجراءات الجزائية، أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني، أو يأمر ضباط الشرطة القضائية المختصة للقيام بذلك.

كما يمكن اتخاذ التدابير الآخرى المنصوص عليها في التشريع المعمول به، وأن يأمر بأية تدابير تحفظية، إما تلقائيا أو بناء على تسخير من النيابة العامة، أو بناء على طل ب من ضباط الشرطة القضائية، على أن لا تمس هذه الآحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية، وهذا بحسب ما نصت عليه الفقرة الآخيرة من المادة 47 من نفس القانون، وهو ما ينسجم مع ما جاء به الآمر رقم20-04 المعدل والمتمم لقانون الإجراءات الجزائية[1] .

وهي الإجراءات التي من شأنها أن تمنح صلاحيات واسعة سواء للضبطية القضائية أو وكيل الجمهورية أو قاض ي التحقيق، من أجل القضاء على هذه الجرائم وسرعة تنفيذ الإجراءات، حتى لا تترك فرصة للجناة بالإفلات من العقاب أو طمس الآدلة.

إن الملاحظ لهذه الإجراءات التي تحكم تفتيش المساكن خاصة منها الاستثنائية الخروج على الميقات القانوني، يجد أن المشرع لم يلحق أهم الجرائم الاقتصادية والمالية كجرائم الفساد والتهريب لتشملها هذه التدابير الاستثنائية، مما يوحي أن عملية التفتيش هنا تخضع للإجراءات العامة كبقية الجرائم العادية، وعليه، ان الآجدر بالمشرع أن ي درجها ضمن الجرائم المحددة في المادة 47 من قانون الإجراءات الجزائية، ما دام أن المشرع نص على توسيع الاختصاص بمناسبة متابعة هذه الجرائم إلى كامل الإقليم الوطني، حسب ما جاء في الآمر 20-04 خاصة المادة 211 مكرر 02 منه.

ثانيا: التوقيف للنظر.

إن التوقيف للنظر وكذا الآمر بالقبض الذي تقوم به الجهات القضائية منتجان لآثارهما إلى غاية صدور أمر مخالف من قاض ي التحقيق بالقطب الجزائي الاقتصادي والمالي، الذي يصبح الضامن

[1] المادة 211 مكرر 1 والمادة 211 مكرر ،2 والمادة 211 مكرر .4 والمادة 211 مكرر 14 من الأمر 20-04 المعدل والمتمم لقانون الإجراءات.

لشرعية الإجراءات، وهذا ما يؤكد صلاحيات القطب الجزائي في اتخاذ أو الإبقاء على هذه الآوامر بحسب ما نصت عليه المادة 211 مكرر13 و 211مكرر 14 من الآمر رقم20-04 ، والذي يمارس إجراءات التوقيف للنظر وفق الآحكام الخاصة في قانون الإجراءات الجزائية.

يعتبر التوقيف للنظر من الإجراءات السالبة للحرية، باعتباره إجراء يؤمر به لوضع المشتبه به في أماكن خاصة بذلك لمدة زمنية محددة، لأسباب يقتضيها البحث والتحري من طرف ضباط الشرطة القضائية .[1]

وقد حدد القانون مدة التوقيف للنظر بمدة لا تتجاوز 48 ساعة، غير أن الآشخاص الذين لا توجد ضدهم دلائل تجعل ارتكابهم أو محاولة ارتكابهم للجريمة مرجحا لا يجوز توقيفهم سوى المدة اللازمة لأخذ أقوالهم.

وبالرجوع إلى قانون الإجراءات الجزائية، نجد أن المشرع قد نص على إمكانية تمديد آجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات مرة واحدة، كما يمكن التمديد مرتين في جرائم الاعتداء على أمن الدولة، وثلاث مرات في جرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الآموال والجرائم المتعلقة بالتشريع الخاص بالصرف.

أما في الجرائم الموصوفة بأفعال إرهابية أو تخريبية فيكون التمديد خمس مرات، حسب ما نصت عليه المادة 51 من الآمر رقم 15-02 والملاحظ أن المشرع لم يدرج أهم الجرائم الاقتصادية والمالية وهي جرائم الفساد والتهريب ض من حالات التمديد الخاصة والتي تضمنتها المادة 51 ضمن الجرائم السالفة الذكر.

ولكن بالرجوع إلى نص المادة 51 مكرر 01 من الآمر السابق التي تحدثت على مختلف حقوق الموقوف للنظر، نجد أن المشرع أدرج جرائم الفساد ضمن الجرائم السالفة الذكر، وبالتالي مكن مرتكب هذه الجرائم والموقوف من أن يتلقى زيارة محاميه بعد انقضاء نصف المدة القصوى المنصوص عليها في المادة 51 من قانون الإجراءات الجزائية .وتتم الزيارة في غرفة خاصة توفر الآمن وتضمن سرية المحادثة وعلى مرأى من ضباط الشرطة القضائية، وحيث لا تتجاوز مدة الزيارة ثلاثين(30) دقيقة.

غير أن المشرع تناول مسألة تمديد التوقيف للنظر بالنسبة لجرائم الفساد في الفصل الثاني من قانون الإجراءات الجزائية تحت عنوان :في التحقيق الابتدائي، بحيث نصت المادة 65 من الآمر رقم 15-02 المؤرخ في 23 يوليو 2015[2] السالف الذكر، على أنه إذا دعت مقتضيات التحقيق الابتدائي

---

[1] أوهايبية عبد الله، **ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي**، دار هومة، الطبعة الأولى، بدون تاريخ، ص 164

[2] الأمر 15-02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، الصادرة في 23 جويلية 2015

ضابط الشرطة القضائية إلى أن يوقف للنظر شخصا توجد ضده دلائل تحمل على الاشتباه في ارتكابه جناية أو جنحة يقرر لها القانون عقوبة سالبة للحرية مدة تزيد عن 48 ساعة، فإنه يتعين عليه أن ي قدم ذلك الشخص قبل انقضاء هذا الآجل إلى وكيل الجمهورية، وبعد أن يقوم وكيل الجمهورية باستجواب الشخص المقدم إليه، يجوز بإذن كتابي أن يمدد حجزه إلى مدة لا تتجاوز 48 ساعة أخرى بعد فحص ملف التحقيق.

وهنا نلاحظ أن هذا الإجراء يتخذ لمجرد الاشتباه في الشخص، مما يدل على حجم خطورة الجريمة والشخص المشتبه به.

وفيما يتعلق بتمديد المدة الأصلية للتوقيف للنظر في الجرائم الاقتصادية والمالية، فيتم ذلك بإذن كتابي من وكيل الجمهورية المختص، وتكون مدة التمديد ثلاث مرات، شأنها شأن جرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص بالصرف.

كما يجوز بصفة استثنائية من ح إذن التمديد بقرار مسبب دون تقديم الشخص إلى النيابة، مع الآخذ بعين الاعتبار الالتزام بما جاء في المواد 51 و51 مكرر و51 مكرر 01 و52 من قانون الإجراءات الجزائية.

الفرع الثاني: الاساليب المستحدثة

بصدور قانون رقم 06-22 : (115) المؤرخ في 20 ديسمبر 2006 المعدل ق. إ..ج فإن المشرع الجزائري أضاف أساليب جديدة خاصة للتحري وتتمثل في المراقبة واعتراض المراسلات والاصوات والتقاط الصور والتسرب. أما قانون الفساد فقد ذكرها بصيغة أخرى وهي التسليم المراقب، الترصد الإلكتروني والاختراق وهذا ما هو منصوص في نص المادة 56 من قانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته[1]

أولا: اعتراض المراسلات:

يعتبر الحق في سرية المراسلات جوهر الحق في الخصوصية، وذلك لأن الرسائل أيا كان نوعها، لا يجوز لغير مصدرها ومن توجه إليه الاطلاع عليها، ويقصد بحق المرسلات عدم جواز الكشف عن محتوياتها، لما يتضمنه ذلك الكشف من اعتداء على حق الخصوصية [2]، كما أن الحق في الصور ة يعتبر انعكاس الشخصية الإنسان، لذلك ي عد جسم الإنسان أكثر عناصر الشخصية استحقاقا لأقصى درجات الحماية القانونية ضد العدسات الملتصقة بآلات التصوير الفوتوغرافي والسينماتوغرافي والنشر.[3]

---

[1] خلفي عبد الرحمان، مرجع سابق، ص 97.

[2] عبد الزعبي علي أحمد، **حق الخصوصية في القانون الجنائي** "**دراسة مقارنة**"، المؤسسة الحديثة للكتاب، طرابلس-لبنان، 2006، ص 180

[3] عبد الزعبي علي أحمد، المرجع السابق، ص 180

ورغم الحماية التي وفرها القانون لكل من المرسلات وتسجيل الآصوات والتقاط الصور [1]، فإن هذه الحقوق تعتبر الآكثر تعرضا للاعتداء، نظرا للتطور الهائل للوسائل التقنية المتعلقة بالتصنت والتسجيل، وبالتالي التعدي على الحياة الخاصة وسرية المكالمات.[2]

ورغم ذلك، فإنه إذا اقتضت ضرورات التحري في الجريمة المتلبس بها وفي بعض الجرائم المتعلقة بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الما س ة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الآموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، وهي مجمل الجرائم التي تمثل الجريمة الاقتصادية والمالية، سمح المشرع للضبطية القضائية باعتراض المراسلات والتقاط الصور وتسجيل الكلام المتفوه به سواء في أماكن عامة أو خاصة، حتى داخل المنزل وبدون علم الآشخاص الذين يملكون الحق على المسكن ودون رضاهم.[3]

غير أن تنظيم المشرع لهذه الإجراءات جعله يحيطها بمجموعة من الضمانات، نظرا للخطورة التي تكتسيها ومسا س ها بحرمة الحياة الخاصة واقتصار تنفيذها على بعض الجرائم فقط، ومنها الجرائم المتعلقة أساسا بالجريمة الاقتصادية والمالية وكذا الجرائم المرتبطة بها، ومجمل هذه الضمانات تتمثل في:

أ. الحصول على إذن مكتوب من طرف وكيل الجمهورية إذا دعت الضرورة لاتخاذ هذه الإجراءات، يتضمن هذا الإذن معلومات تتعلق بالإجراء المراد اتخاذه، سواء تعلق الآمر باتصال أو التقاط صور وكذا الآماكن المقصودة، سواء سكنية أو غيرها، بالإضافة إلى الجريمة التي دعت لاتخاذ هذا الإجراء.

ب – تكون مدة الإذن محددة بأربعة (04) أشهر قابلة للتجديد، مع التزام ضابط الشرطة القضائية بالحفاظ على السر المهني كما أن لضابط الشرطة القضائية تسخير أي عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو هيئة خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية ..[4]

ت – بعد الانتهاء من العملية، يحرر ضابط الشرطة القضائية المأذون له أو المناب، محضرا عن العملية اعترا ض أو تسجيل المراسلات، وكذا عن وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها، وتنسخ وتترجم المكالمات التي تتم باللغة الآجنبية عند الاقتضاء بمساعدة مترج م ي س خ ر لهذا

---

[1] المادة 46 و47 من القانون رقم 16-01 المؤرخ في 06 مارس 2016 يتضمن التعديل الدستوري الجريدة الرسمية عدد 14. الصادر بتاريخ 07 مارس 2016، تقابلها المواد 47 و48 من دستور الجزائر لسنة 2020 المؤرخ في 30 ديسمبر 2020 بموجب المرسوم الرئاسي رقم 445/20، المؤرخ في 2020/12/30، المتضمن اصدار التعديل الدستوري لسنة 2020، الجريدة الرسمية، (الجزائر)، العدد: 82، صادرة بتاريخ 2020/12/20

[2] أشرف حامد الشافعي، **الحماية الجنائية لحق الخصوصية**، أطروحة دكتوراء غير منشورة كلية الحقوق بجامعة القاهرة، 2012. 2013، ص 61

[3] الشلقاني أحمد شوقي، **مبادئ الإجراءات الجزائية في التشريع الجزائري**، ج02، ديوان المطبوعات الجامعية، الجزائر، الطبعة الرابعة، 2008، ص 157.

[4] وهذا حسب ما نصت عليه المواد 65 مكرر 05 و65 مكرر 07 من قانون 06-22

الغرض، حسب ما نصت عليه المادة 65 مكرر 09 و65 مكرر 10 من القانون06-22، وهذا المحضر يوع في ملف المتهم، غير أن الإشكال الذي ي طرح هو فيما يتعلق بالإذن ومدى وضعه في ملف الإجراءات بصفة عادية، لأن المشرع لم ينص على ذلك، وهذا عكس الإذن المتعلق بعملية التسرب الذي يوضع في الملف بعد الانتهاء مباشرة من عملية التسرب، وربما هدف المشرع من ذلك هو عدم تعريض الإجراء التقني إلى تسريب معلومات تخصه أو تخص من وجه له، وهذا ما يجسد سعي المشرع إلى احترام حق الخصوصية.

ثانيا: التسرب:

تقتضي متابعة الجرائم الاقتصادية والمالية استخدام تقنية مستحدثة تتمثل في التسرب، ويتم بموجب هذه العملية قيام ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، ويتم ذلك بإخفاء الهوية الحقيقية بإيهامهم بأنه فاعل أو شريك[1].

وبالرجوع إلى قانون الإجراءات الجزائية، نجد أن المشرع على غير العادة، قد عرف التسرب كآلية مستحدثة للبحث والتحري في جرائم الفساد اونه نظام جديد، بحيث نصت المادة 65 مكرر 12 من قانون 06-22 [2]بقولها" :يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الآشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف."...

وهذا الإجراء منصوص عليه تحت عنوان" **في التسرب** "بموجب المواد من 65 مكرر 11 إلى 65 مكرر 17 من القانون السابق .بحيث تتيح عملية التسرب لضابط الشرطة أن يستعمل هوية مستعارة، ويرتكب عند الضرورة جريمة، أو فعلا من الآفعال المنصوص عليها في المادة 65 مكرر 14 دون أن تشكل هذه الآفعال تحريضا على ارتكاب الجريمة.

كما يمكن للضابط اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

كما يمكن أن يضع تحت تصرف مرتكبي الجريمة وسائل ذات طابع قانوني أو مالي، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال دون أن يتابع جزائيا من يسخر للقيام بالتسرب، وقد أحاط المشرع الجزائري هذا الإجراء وربط تطبيقه بالشروط التالية:

أ. الحصول على إذن مكتوب ومسبب، يشمل هذا الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، كما تحدد هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد الإذن أيضا المدة المحددة لعملية التسرب، والتي حددها المشرع بأربعة (04) أشهر قابلة للتجديد حسب مقتضيات البحث والتحري التحقيق.

---

[1] خلفي عبد الرحمان، **محاضرات في قانون الإجراءات الجزائية**، دار الهدى عين مليلة – الجزائر، طبعة 2018، ص 75

[2] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية

ب. إذا تم تجاوز المدة المحددة لعملية التسرب أو عدم تمديد هذه المدة، يمكن للعون المتسرب مواصلة، النشاطات [1]الوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك مدة أربعة أشهر.

ت – بعد الانتهاء من عملية التسرب يتم تحرير محضر يتضمن تقريرا عن هذه العملية من طرف ضباط الشرطة القضائية، كما يجوز سماعه كشاهد عن العملية.

ث – إن عملية التسرب، وبالنظر لكونها تحمل في طياتها تحريضا على ارتكاب الجريمة، لفت المشرع إلى تطبيقها في حدود ضيقة وفي جرائم محددة قانونا، ومنها الجرائم الاقتصادية والمالية، وهذا ما يبرر حرص المشرع وسعيه إلى مكافحتها والتصدي لها.

ج. تودع رخصة التسرب في ملف الإجراءات بعد الانتهاء من عملية التسرب ..

خول المشرع لقاض ي التحقيق سلطا ت واسعة لتنفيذ إجراءات اعتراض المراسلات وتسجيل الآصوات والتقاط الصور، رغم أن هذا الإجراء يقوم به ضباط الشرطة القضائية بناء على إذن من وكيل الجمهورية، كما تمت الإشارة إليه سابقا، غير أنه في حالة فتح تحقي ق قضائي في الجرائم المتعلقة بالفساد، فإن هذه العمليات تتم بناء على الإذن القانوني من طرف رجال القضاء وهو ما من شأنه حماية الحياة الخاصة .[2]

وبناء على هذا الإذن الذي خول له أن يسمح بتنفيذ هذه العمليات بالدخول إلى المساكن والمحلات وغيرها حتى دون رضا المشتبه فيه[3]، كما يستنتج من هذه النصوص، أن قاض ي التحقيق لا يباشر هذه الإجراءات بنفسه، بل يقوم بها ضابط الشرطة القضائية، وهذا ما يطرح صعوبة في تطبيق هذه الإجراءات باعتبار ضباط الشرطة القضائية تابعين لوكيل الجمهورية.

ولقيام قاضي التحقيق بهذه الإجراءات تراعى فيها إجراءات أخرى، اونه مرتبط بإجراءات الحبس المؤقت خاصة في حالة التمديد [4]، وكذا الرقابة القضائية وإجراءات تنفيذها.[5]

تتمثل سلطة قاضي التحقيق في تنفيذ عملية التسرب في الإذن الذي يمنحه بعد إخطار وكيل الجمهورية، إذا اقتضت ضرورة البحث والتحري أو التحقيق في أحد الجرائم الاقتصادية والمالية أو الجرائم الآخرى الخاصة المنصوص عليها قانونا.

وتتم عملية التسرب تحت رقابة قاض ي التحقيق على النحو الذي تم دراسته في مهام الضبطية القضائية وسلطاتها في عملية التسرب.[1]

---

[1] المذكورة في المادة 65 مكرر 17 والتي تحيل إلى المادة 65 مكرر 14 من قانون 06-22

[2] بن ذياب عبد المالك، **حق الخصوصية في التشريع العقابي الجزائري**، رسالة ماجستير غير منشورة كلية الحقوق بجامعة الحاج الخضر، باتنة، الجزائر، 2012-2013، ص 155

[3] طبقا لنص المادة 65 مكرر 06 وما بعدها من قانون 06-22

[4] المواد: 123 إلى 125 مكرر من الأمر 15-02 المعدل والمتمم لقانون الإجراءات الجزائية

[5] سلطة قاضي التحقيق في الرقابة القضائية المادة 125 مكرر 1 وما بعدها من نفس الأمر

كما يمكن لقاضي التحقيق الذي رخص بإجراء عملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة[2]، والرخصة الخاصة بعملية التسرب لا تودع في ملف الإجراءات إلا بعد الانتهاء من عملية التسرب، أي أنه لا يمكن الاطلاع عليها قبل ذلك من طرف محامي المتهم، وهذا ما يشكل مساسا بحق الدفاع في الاطلاع على ملف الإجراءات.

غير أن الهدف من ذلك هو محاولة إبقاء عملية التسرب سرية حفاظا على نجاح هذه العملية، خاصة وأن ضابط الشرطة القضائية لا يكشف عن هويته الحقيقية، وأن عملية التسرب محاطة بضمانات، وأن تطبيقها استثناء من القاعدة العامة، ولا يكون إلا في جرائم محددة تتسم بالخطورة الكبرى، وهذه الإجراءات تتم تحت إدارة وإشراف وكيل الجمهورية أو قاضي التحقيق لدى القطب الجزائي الاقتصادي والمالي، في حال ما إذا كانت الجرائم تدخل في نطاق اختصاصهم، فيصبح القطب الجزائي الاقتصادي والمالي هو الضامن لشرعية الإجراءات.

---

[1] طبقا لنص المادة 65 مكرر 11 من قانون 06-22: عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه .

[2] طبقا لنص المادة 65 مكرر 15 من قانون 06-22: يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان .

تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته و يحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر .

يمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية .

و يجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل إنقضاء المدة المحددة .

تودع الرخصة في ملف الإجراءات بعد الإنتهاء من عملية التسرب

الخاتمة

الخاتمة

الخاتمة

مما سبق نستطيع القول أن الإرهاب الإلكتروني هو تلك الأعمال الارهابية التقليدية لكن عبر الأجهزة الإلكترونية الموصولة بشبكة الإنترنت بحيث تنطوي هذه الأعمال على التخويف والتهديد، أو نشر أفكار ومعتقدات متطرفة وعنصرية، أو اختراق النظم وبيانات الشخص بذاته أو شركة أو دولة معينة.

وخلصنا من خلال هذه الدراسة إلى النتائج التالية :

– أصبح الإرهاب الإلكتروني واقعًا ملموسًا يحمل أبعادًا خطيرة يصعب التنبؤ بها، خاصة مع تزايد عدد مستخدمي الإنترنت والنمو السريع لتقنيات الحاسوب، مما يجعل جهود مكافحته أكثر تعقيدًا.

– يُعتبر الإرهاب الإلكتروني من الجرائم المستمرة التي لا تنتهي، حيث يصعب ردع المجرم الإلكتروني ومحاسبته على أفعاله. فعند مواجهة أعماله الإرهابية، يمكنه التخطيط لجرائم جديدة، وحتى إذا تم التعرف عليه والقبض عليه، فإن هناك من يحل محله إذا كان مرتبطًا بجماعة إرهابية.

– لم تكن الجهود المبذولة لمكافحة الإرهاب الإلكتروني متناسبة مع خطورته، حيث لم تكن مساعي منظمة الأمم المتحدة في هذا المجال واضحة أو ثابتة، مما يفسر عدم وجود اتفاقية دولية خاصة لمكافحة الإرهاب الإلكتروني. ورغم أن اتفاقية بودابست لمكافحة جرائم الحاسوب تناولت بعض جوانب مكافحة الأعمال الإرهابية عبر الإنترنت، إلا أن ذلك لا يكفي في ظل التطور المستمر والتهديدات المتزايدة التي يمثلها مرتكبو جرائم الإرهاب الإلكتروني.

– لا يمكن مقارنة الجهود الدولية بجهود الحكومات المختلفة، حيث قامت بعض الدول بوضع قوانين وتشريعات خاصة لمكافحة الإرهاب الإلكتروني. في المقابل، لم تقم دول أخرى، خاصة في العالم الثالث، بتحديث تشريعاتها في هذا المجال، باستثناء بعض الجوانب المتعلقة بهذه الجريمة، مثل اختراق الأنظمة، كما هو الحال مع المشرع الجزائري.

– إن الأعمال العدائية الإلكترونية التي تقوم بها الدول المسيطرة على الساحة الدولية تجاه دول أخرى لا تختلف عن الأنشطة التي تمارسها الجماعات الإرهابية باستخدام التكنولوجيا. وبالتالي، يمكن أن يكون مرتكب الإرهاب الإلكتروني فردًا أو جماعة أو حتى دولة.

– ضعف الجهود الدولية والإقليمية خاصة العربية منها في مكافحة الإرهاب الإلكتروني، لعل ذلك راجع إلى الأزمات المتتالية التي مر ويمر بها الوطن العربي.

نقترح من خلال هذه الدراسة بما يلي :

– من الضروري أن تكون هناك جهود وقائية لمكافحة جريمة الإرهاب الإلكتروني، وذلك من خلال توعية الأفراد والمواطنين عبر تثقيفهم حول هذه الجريمة، خصوصًا في المجتمعات الفقيرة التي تعاني من الجهل والظروف الاجتماعية الصعبة، مما يسهل انضمامهم إلى الجماعات الإرهابية. ينبغي أن تكون هذه التوعية على مستوى وطني ودولي.

الخاتمة

– كما يُعتبر إدراج موضوع مكافحة الإرهاب الإلكتروني في المناهج الدراسية بجميع مراحلها من الوسائل الفعالة في تعزيز التربية الإلكترونية لدى التلاميذ والطلاب. فهذه الفئة من المجتمع هي الأكثر استخدامًا للإنترنت، بما في ذلك مواقع التواصل الاجتماعي، التي تُستخدم من قبل الجماعات الإرهابية للتواصل مع الأفراد والترويج لأفكارها.

– ينبغي تعزيز دور الجمعيات الوطنية والمنظمات الدولية، وخاصة منظمة الأمم المتحدة، في مكافحة الإرهاب الإلكتروني بشكل فعّال.

– بالإضافة إلى الجهود الوقائية لمواجهة الإرهاب الإلكتروني، يتعين على الدول الالتزام بتطوير تشريعات داخلية من خلال سن قوانين حديثة قادرة على التصدي لهذا النوع من الجرائم الخطيرة.

– يجب على الدول أن تتعاون بشكل جماعي لتأسيس إطار تشريعي ومؤسساتي دولي لمكافحة الإرهاب الإلكتروني، وذلك من خلال توقيع اتفاقيات دولية، وإنشاء محكمة دولية متخصصة في جرائم الإنترنت، ووضع استراتيجية دولية شاملة وفعّالة لمواجهة الإرهاب الإلكتروني.

– ينبغي أن يتوسع نطاق التجريم ليشمل ليس فقط الأعمال الإرهابية الإلكترونية، بل أيضًا مجموعة من السلوكيات المادية المرتبطة بالحرب الإلكترونية، مثل اختراق دولة ما لأنظمة جيش دولة أخرى أو إصابة أنظمتها الأمنية المعلوماتية بفيروسات بهدف السيطرة عليها.

– يتعين على حكومات الدول تحديث تشريعاتها وتدريب القضاة في مجال المعلوماتية، حيث يتطلب عصر الرقمنة إنشاء مؤسسات قضائية متخصصة في الفضاء الرقمي، بالاستعانة بخبراء في هذا المجال.

– من الضروري تأمين البيانات والمعلومات الحساسة بشكل مستمر، سواء كانت تتعلق بالأفراد أو الدول أو الشركات.

المصادر

والمراجع

المصادر والمراجع

أولا: المصادر

1.الدستور

- دستور الجزائر لسنة 2020 المؤرخ في 30 ديسمبر 2020 بموجب المرسوم الرئاسي رقم 445/20، المؤرخ في 2020/12/30، المتضمن اصدار التعديل الدستوري لسنة 2020، الجريدة الرسمية، (الجزائر)، العدد: 82، صادرة بتاريخ 2020/12/20

2.القوانين

- القانون 15-02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، الصادرة في 23 جويلية 2015
- القانون 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق5 غشت سنة2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ25 شعبان عام 1430 هـ، الموافق 16 غشت سنة2004
- القانون رقم 04-15 المؤرخ في 10 نوفمبر2004 ، المتضمن قانون العقوبات المعدل والمتمم71 ، ج.ر، العدد 71 ص11 و12
- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية
- القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق ل 28 أبريل سنة 2020 يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، الجريدة الرسمية، العدد25 ، الصادرة بتاريخ 6 رمضان 1441هـ الموافق ل 29 أبريل سنة 2020 م.
- القانون رقم15- 06 المؤرخ في 15 فبراير 2015 يعدل ويتمم القانون رقم 05/01 المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما المعدل والمتمم .

ثانيا: المراجع

1.المعاجم

- أبو الفضل ابن منظور، **لسان العرب**، المجلد الأول، الطبعة الثالث، مادة (رهب)، بيروت، لبنان
- بن أبي بكر الرازي محمد ، **مختار الصحاح**، (مادة رهب)، 1962
- مجمع اللغة العربية، **المعجم الوسيط**، ج01، دار عمران للطباعة والنشر، القاهرة

2.الكتب العامة

- امير فرج يوسف، **الجرائم الدولية للأنترنت**، ط1 ، المركز القومي للإصدارات القانونية، مصر،2011
- أوهايبية عبد الله، **ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي**، دار هومة، الطبعة الأولى، بدون تاريخ
- بارش سليمان، **شرح قانون الإجراءات الجزائية الجزائري**، دار الشباب بائنة الجزائر، طبعة 1986

المصادر والمراجع

- جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات**، الطبعة الأولى، دار البداية، ليبيا، 2010
- خلقي عبد الرحمان، **الإجراءات الجزائية في التشريع الجزائري والمقارن**، ط. 4 دار بلقيس للنشر، الجزائر، 2019
- رحماني منصور، **الوجيز في قانون الجنائي العام**، دار العلوم لنشر والتوزيع، عنابة، 2006
- الشلقاني أحمد شوقي، **مبادئ الإجراءات الجزائية في التشريع الجزائري**، ج02، ديوان المطبوعات الجامعية، الجزائر، الطبعة الرابعة، 2008.
- عبد الزعبي علي أحمد، **حق الخصوصية في القانون الجنائي "دراسة مقارنة"**، المؤسسة الحديثة للكتاب، طرابلس– لبنان، 2006،
- ناصر الهاشمي، **الإرهاب: (الجذور، المظاهر، وسبل المكافحة)**، ط01، دار الحامد للنشر والتوزيع، الأردن، 2016
- المناعسة أسامة احمد، الزعبي جلال محمد، **جرائم التقنية نظم المعلومات الالكترونية، دراسة مقارنة**، ط2 ، دار الثقافة لنشر والتوزيع، عمان، الأردن،2014
- ناظم نواف إبراهيم، **ظاهرة العنف السياسي في العراق المعاصر بعد الاحتلال الأمريكي**، أطروحة دكتوراه، معهد البحوث والدراسات العربية، القاهرة، مصر، 2009
- ناني لحسن، **التحقيق في الجرائم المتعلقة بتكنولوجيا المعلومات**، دار النشر الجامعي الجديد، الجزائر، 2018
- الفيل علي عدنان، **الاجرام الالكتروني**، ط1 ، مكتبة زين الحقوقية والأدبية، لبنان،2011
- هلالي عبد إلاه احمد، **اتفاقية بودابست لمكافحة جرائم المعلوماتية**، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007
- يونس عرب، **جرائم الكومبيوتر والإنترنت**، ط 1 اتحاد المصارف العربية، بيروت، 2002

3.الكتب المتخصصة

- بن سالم ايمان، **جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري**، ط01، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2028
- بوحادة سارة، **أثر الإرهاب الإلكترونى على أمن واستقرار الدول**، المدرسة الوطنية للعلوم السياسية، الجزائر، 2016
- الجهماني ثامر إبراهيم ، **مفهوم الإرهاب في القانون الدولي، دراسة قانونية ناقدة**، ط1 ، دار الكتاب العربي، الجزائر،2002
- سامي علي حامد عياد، **استخدام تكنولوجيا المعلومات في مكافحة الإرهاب**، دار الفكر الجامعي، مصر، 2008.

المصادر والمراجع

- عبد الصادق عادل، **استخدام الإرهاب الالكتروني في الصراع الدولي**، دار الكتاب الحديث، القاهرة، 2015
- عبد الصادق عادل، **الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة**، ط1 ، مركز الاهرام للدراسات السياسية والاستراتيجية2009
- فرج يوسف أمير، "**جريمة مكافحة الإرهاب الإلكتروني "الإرهاب الرقمي" في دول الخليج العربي في ظل اتفاقية دول مجلس التعاون لمكافحة الإرهاب**"، القاهرة: دار الكتب والدراسات العربية، الطبعة الأولى، 2016

4.المحاضرات

- خلفي عبد الرحمان، **القانون الجنائي العام (دراسة مقارنة)**، دار بلقيس للنشر دار البيضاء، الجزائر، 2017
- خلفي عبد الرحمان، **محاضرات في القانون الجنائي العام**، دار الهدى، عين مليلة الجزائر، 2012
- خلفي عبد الرحمان، **محاضرات في قانون الإجراءات الجزائية**، دار الهدى عين مليلة – الجزائر، طبعة 2018

5.المقالات والمدخلات

- أحمد أبو الوفا، **ظاهرة الإرهاب على ضوء أحكام القانون الدولي العام**، مجلة البحوث والدراسات العربية، العدد السابع عشر، 1990
- باخوية دريس، **جرائم الإرهاب في دول المغرب العربي**(تونس، الجزائر، والمغرب أنموذجاً)، مجلة دفاتر السياسة والقانون، المجلد06، العدد 11، 2014
- بلهول نسيم، **مفهوم المذهب العسكري الجزائري لثنائية بيئة الضبط العملياتي والدين في مكافحة الإرهاب**، مجلة العلوم القانونية والسياسية، جامعة ديالي العراق، العدد الأول 2015
- بلواضح الطيب قسمة محمد، **مكافحة جريمة تمويل الارهاب على المستويين الدولي والوطني**، مجلة الدراسات والبحوث القانونية، المجلد 02، العدد 05، 2017
- بن صويلح أمال، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام**، الملتقى الدولي حول الاجرام السيبرياني، المفاهيم والتحديات خطو هامة نحو مكافحة الارهاب الالكتروني في الجزائر، جامعة قالمة، يومي 11-12 افريل، 2017
- بن عمروش فريدة، **الإرهاب الالكتروني :دراسة في إشكالات المفهوم والأبعاد**، المجلة الجزائرية للعلوم الاجتماعية والإنسانية، المجلد08 ، العدد02، 2022
- بن مرزوق عنترة، الكر محمد، **البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب**، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان 2018،

المصادر والمراجع

- جعيجع عبد القادر، تيغزة زهرة، **تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة**، مجلة دفاتر السياسة والقانون، المجلد 13 العدد الأول، الجزائر، 2021
- جغدم محمد الأمين، **جرائم الارهاب الالكتروني والجرائم المنظمة**، مجلة القانون الدولي والتنمية، المجلد06، العدد01، 2018
- الحوامدة لورنس سعيد، **جريمة الإرهاب الإلكتروني في التَّشريعات الجنائيَّة دراسةٌ تحليليَّة مُقارنةٌ**، مجلة كلية الشريعة والقانون بتفهنا، كلية الحقوق، جامعة طيبة، المملكة العربية السعودية، المجلد 24، العدد 01، 2022
- دريعي عبد السادة سحر، **مكافحة الإرهاب الالكتروني :تحليل التهديدات وتعزيز القدرات الدفاعية**، مجلة قضايا سياسية، العدد74، 2023
- الزنط سعد عطوة، **الإرهاب الالكتروني واعادة صياغة استراتيجيات الأمن القومي، ورقة مقدمة إلى مؤتمر الجرائم المستحدثة :كيفية اثباتها ومواجهتها**"، المركز القومي للبحوث الاجتماعية والجنائية ،مصر، (15–16) ديسمبر 2010
- الساحي علام، فوزية حاج شريف، **واقع الإرهاب الإلكتروني اليات مكافحته**، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد . الأول.
- سليماني مباركة، **الإرهاب الالكتروني وطرق مكافحته**، مجلة الحقوق والعلوم السياسية العدد 08 ج 01 / جوان 2017
- شرف الدين وردة، **مكافحة جريمة تهريب المهاجرين في قانون العقوبات الجزائري** ،.مجلة الاجتهاد القضائي، العدد (10)، 2018
- الشمري نايف أحمد ضاحي، العبيدي عمر عباس خضير، **جرائم الأمن السيبراني واليات مكافحتها في إطار القانون الدولي**، المؤتمر الدولي الخامس للقضايا القانونية، 2021
- عبد الباهي الناهي أحمد، عبد الستار رشيد صدام، **السياسة الاعلامية لتنظيم داعش: الأهداف وسبل المعالجة**، المجلة السياسية والدولية، العراق: الجامعة المستنصرية، العدد30، 2016
- عمروش الحسين، **آليات مكافحة جريمة الفساد في نطاق منظمة الشرطة الجنائية الدولية**، الملتقى الوطني حول مكافحة الفساد وتبيض الأموال، يومي 10–11 مارس 2009
- عوينات بن عمر نجيب، **الإرهاب الإلكتروني: المفهوم والجهود الدولية والإقليمية لمكافحته**، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 02، العدد 02، جوان 2017
- غربي أسامة، **المنظمة الدولية للشرطة الجنائية الانتربول، ودورها في مكافحة الجريمة المنظمة**، مجلة دراسات وأبحاث، المجلد 03– العدد الثالث، 2018

المصادر والمراجع

- مجاهد توفيق، عابسة طاهر، **جريمة الإرهاب في ضوء احكام الاتفاقية العربية لمكافحة جرائم التقنية المعلومات لعام2010** ، مجلة العلوم القانونية والسياسية، المجلد09 ، العدد03 ، ديسمبر2018 ، جزائر،
- نجاري فايزة بن حاج علي، **دراسة لظاهرة الإرهاب الالكتروني**، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، 2022
- نهايلي رابح، قيرة سعاد، **دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)** مجلة البحوث القانونية والاقتصادية، المجلد 04-العدد 02-2021
- يوبي سعاد، **الإنتربول كآلية دولية شرطية لمكافحة جريمة الفساد**، المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار، الجزائر المجلد03 ، العدد01، جوان2019

6.الأطروحات

- أشرف حامد الشافعي، **الحماية الجنائية لحق الخصوصية**، أطروحة دكتوراء غير منشورة كلية الحقوق بجامعة القاهرة، 2012. 2013
- عباس شافعة، **الظاهرة الارهابية بين القانون الدولي والمنظور الديني**، اطروحة دكتوراه في علوم القانون، تخصص قانون دولي وعلاقات دولية، جامعة الحاج لخضر، 2010-2011
- فيصل بدري، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، رسالة دكتوراه جامعة الجزائر 01- بن يوسف بن خدة- 2017/2018
- نجاري بن حاج علي فايزة، **مكافحة الارهاب الالكتروني في القانون الدولي**، اطروحة دكتوراه في العلوم، تخصص : قانون، جامعة مومود معمري، تيزي وزو، الجزائر، 2023

7.الرسائل

- بن ذياب عبد المالك، **حق الخصوصية في التشريع العقابي الجزائري**، رسالة ماجستير غير منشورة كلية الحقوق بجامعة الحاج الخضر، باتنة، الجزائر، 2012-2013
- تراقي أمال، **الجريمة المنظمة والجهود المبذولة لمكافحتها**، مذكرة لنيل درجة الماجستير في القانون، كلية الحقوق، جامعة بجاية، 2012
- طارق جواد اسراء، الجابري كاظم، **جريمة الإرهاب الالكتروني**، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق،2012 .
- طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة مكملة لنيل شهادة المـاجستير في العلوم القانونية، قسم الحقوق، جامعة الجزائر1، 2013.
- عمر عباس، العبيدي خضير، **الإرهاب الإلكتروني في نطاق القانون الدولي**، رسالة ماجستير، كلية الحقوق، جامعة تكريت العراق 2019

المصادر والمراجع

- فنور حاسين، **المنظمة الدولية للشرطة الجنائية والجريمة لمنظمة**، رسالة ماجستير، كلية الحقوق، جامعة الجزائر ،السنة الجامعية2013-2014
- محمد مسفر عبد الخالق الشمراني، **الجريمة المنظمة وسياسة المكافحة في التشريع الإسلامي والقانون الجنائي الإسلامي والأنظمة الجنائية المعاصرة لجريمة تهريب المخدرات**، (بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية)، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2001
- نجاري بن حاج علي فايزة، **الاليات القانونية للإرهاب الالكتروني**، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2016

8.المذكرات

- انقوش سعاد، اشعلال صورية، **الركن المعنوي في الجريمة**، مذكرة ماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية .ك ح ع من جامعة عبد الرحمان ميرة بجاية 2016/2017
- شاشوة ياسمينة، **الارهاب الالكتروني بين مخاطره واليات مكافحته**، مذكرة ماستر في الحقوق،، تخصص: قانون جنائي وعلوم جنائية، جامعة آكلي محند أولحاج، البويرة، الجزائر، 2019-2020
- علي بوعمرة، **جريمة الارهاب الالكتروني**، مذكرة ماستر في الحقوق، تخصص : قانون جنائي وعلوم جنائية، جامعة العربي تبسي، تبسة، الجزائري، 2020-2021.
- غلاف كريمة، جرلال زوهرة، **جريمة الإرهاب الالكتروني**، مذكرة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، بجاية، 2018-2019
- قاسمي رحمة، بوخروبة كريمة، **الارهاب الالكتروني(التحديات والمواجهات)**، مذكرة ماستر في الحقوق، تخصص: قانون اعلام الي، جامعة محمد البشري الابراهيمكي، برج بوعريريج، الجزائر، 2021-2022
- كركوم لمين الطيب رزيق، **الشروع في الجريمة**، مذكرة للنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية ،ك ج ع من جامعة عبد الرحمان ميرة بجاية 2014/2015

9.مواقع الانترنت

- http://www.acrseg.org/40137
- https://democraticac.de/?p=52894

الفهرس

الفهرس

مقدمة 1

الفصل الأول: مفهوم الارهاب الالكتروني . . . . . .

المبحث الأول: تعريف وخصائص الإرهاب الالكتروني 6

المطلب الأول: تعريف الإرهاب الإلكتروني 6

الفرع الأول: مدلول الظاهرة الإرهابية. 6

الفرع الثاني: مدلول الإرهاب الالكتروني 9

المطلب الثاني: خصائص واسباب الارهاب الالكتروني 18

الفرع الاول: الخصائص المتعلقة بطبيعة الجريمة 18

الفرع الثاني: الخصائص المتعلقة بطبيعة الهجمات. 21

الفرع الثالث: الخصائص المتعلقة بتقييم طبيعة التهديد 22

المبحث الثاني: اركان جريمة الارهاب الالكتروني 23

المطلب الأول: الركن المادي لجريمة الإرهاب الإلكتروني 24

الفرع الأول : السلوك الإجرامي 24

الفرع الثاني : النتيجة الجرمية في جريمة الإرهاب الإلكتروني 27

الفرع الثالث : العلاقة السببية في جريمة الإرهاب الإلكتروني 28

المطلب الثاني: الركن المعنوي لجريمة الإرهاب الإلكتروني 29

الفرع الاول : القصد الجنائي العام 30

الفرع الثاني: القصد الجنائي الخاص 30

الفصل الثاني: سبل وآليات مكافحة الجريمة الارهابية الالكتَرونية . . . .

المبحث الاول: الجهود الدولية لمكافحة الارهاب الالكتروني..... 34

المطلب الاول: مكافحة الارهاب الالكتروني على المستوى العالمي. 34

الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية 34

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الدولية إن المنظمات الدولية..... 38

3. دور الانتربول في مكافحة الجريمة الارهابية الالكترونية المنظمة 41

المطلب الثاني: مكافحة الإرهاب الالكتروني على الصعيد الاقليمي..... 47

الفرع الاول: مكافحة الإرهاب الالكتروني على المستوى الاوروبي 47

الفرع الثاني: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني 48

الفهرس

المبحث الثاني: الجهود الوطنية لمكافحة الارهاب الالكتروني 51

المطلب الاول: الاليات القانونية والمؤسساتية لمكافحة الارهاب الالكتروني 51

الفرع الثاني : إجراءات الوقاية لمكافحة الإرهاب الإلكتروني 52

الفرع الثاني: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني والنتائج المحققة في هذا الإطار 54

المطلب الثاني: الاليات الاجرائية لمكافحة الارهاب الالكتروني 56

الفرع الأول :أساليب التحري التقليدية 56

الفرع الثاني: الاساليب المستحدثة 59

الخاتمة 65

مخلص الدراسة

الملخص:

تهدف هذه الدراسة إلى تبيان مختلف الجهود لمكافحة الإرهاب الإلكتروني، حيث تتمايز هذه الجهود بين الطابع الدولي والوطني، والتي ومن خلالها كان الاهتمام بمكافحة هذا النوع من الإجرام الخطير والمستحدث على المستويين الدولي والداخلي، ولهذه الدراسة أهمية تتمثل في أن الإرهاب الإلكتروني هو خطر يهدد على حد سواء سلامة الكيان الطبيعي أو الكيان المعنوي، فالمجرم الإرهابي اليوم استفاد بشكل سلبي من تطور تقنية المعلومات والشبكات العنكبوتية التي هي مورد هام وأساسي في ارتكاب الجريمة الإرهابية الرقمية، مما حتم على الدول مجتمعة ومنفردة مكافحة هذا النوع الخطير من الإجرام بمختلف الأساليب والطرائق، وقد خلصنا إلى أن هذه الجهود تلعب دورا هاما في مجابهة الإرهاب الإلكتروني إلا أنه وبالرغم من ذلك لا تزال هذه الظاهرة الإجرامية قائمة وتعاني منها الدول والأفراد على حد سواء، مما يستوجب إيجاد وسائل تكون أكثر وقائية ومجابهة لها .

الكلمات المفتاحية: الإرهاب الإلكتروني ، الحرب الإلكترونية، مكافحة الإرهاب الإلكتروني

Abstract:

This study aims to highlight the various efforts to combat cyberterrorism, which are differentiated between international and national efforts. These efforts have focused attention on combating this dangerous and emerging form of crime at both the international and domestic levels. This study is important because cyberterrorism is a threat that threatens both the safety of natural and legal entities. Today's terrorist criminals have negatively benefited from the development of information technology and the internet, which are an important and essential resource for committing digital terrorist crimes. This has made it imperative for countries, both collectively and individually, to combat this dangerous form of crime using various methods and approaches. We conclude that these efforts play an important role in combating cyberterrorism. However, despite this, this criminal phenomenon persists and continues to plague both countries and individuals. This necessitates the development of more preventative and countermeasures.

Keywords: cyberterrorism, cyberwarfare, combating cyberterrorism.