الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of higher education and scientific research
جامعة محمد البشير الإبراهيمي – برج بوعريريج
University Of Mohamed Al-Bashir Al-Ibrahimi - BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق
تخصص قانون إعلام آلي وأنترنت

الموسومة بـ:

جريمة الإرهاب الإلكتروني

إعداد الطالبتين:
- شرين بولعراس.
- منى بلعيد.

إشراف الأستاذ:
-عبد الجليل بن محفوظ درارجة

لجنـــة المناقشـــة

خضري محمد	أستاذ محاضر أ		**رئيسا**
عبد الجليل بن محفوظ درارجة	أستاذ محاضر أ		**مشرفا ومقررا**
خنتاش عبد الحق	أستاذ محاضر أ		**ممتحنا**

السنة الجامعية 2025/2024

* ملحق بالقرار رقم ....1082.. المؤرخ في ..... 2020 ماي 27

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله.

السيد(ة): بولعراس فتيحة الصفة: طالب. ~~أستاذ. باحث~~

العامل(ة) لبطاقة التعريف الوطنية رقم 118355347 والصادرة بتاريخ 2020.08.27

المسجل(ة) بكلية / معهد الحقوق قسم قانون خاص

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: جريمة الارهاب الالكتروني

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2025/06/24....

توقيع المعني (ة)

شروط تأجيل التصديق

السيد: ...

بطاقة التعريف الوطنية رقم: ...

مسلم بتاريخ: ...

العناصر التي: ...

24 جوان 2025

الرئيس المجلس الشعبي البلدي و بتفويض منه

ضابط الحالة المدنية

حروز زهير

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 2023 ماي 27

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): ملعيد منى الصفة: طالب، أستاذ، باحث

العامل(ة) لبطاقة التعريف الوطنية رقم 118096156 والصادرة بتاريخ 2020-07-07

المسجل(ة) بكلية / معهد الحقوق قسم قانون خاص

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

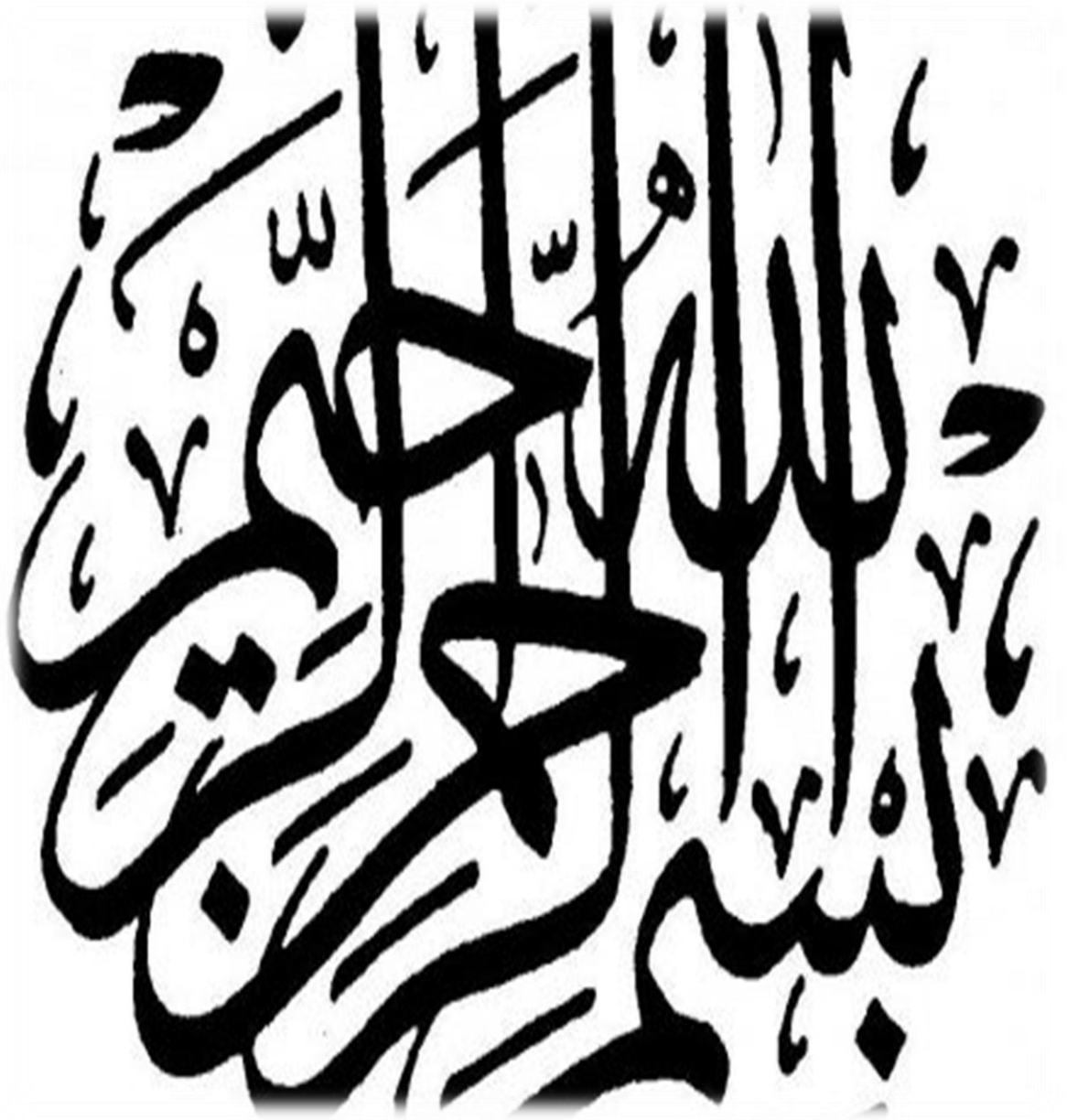
عنوانها: حريمة الإرهاب الالكتروني

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025.06.24

توقيع المعني (ة)

شوهد تأجل التصديق
السيد: ...
ببطاقة التعريف الوطنية رقم: ...
مستخرج بتاريخ: ...
العناصر في: ...
ع/رئيس المجلس الشعبي البلدي و بتفويض منه
ضابط الحالة المدنية
حروز زهير
2025 جوان 24



"..... نَرْفَعُ دَرَجَاتٍ مَنْ نَشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ...."

(سورة يوسف/الآية 76)

شكر وعرفان

.

قال تعالى: "ولئن شكرتم لأزيدنكم" صدق الله العظيم

سورة ابراهيم الاية 7

نحمد الله تعالى حمد الشاكرين الذي وفقنا وسدد خطانا وهيأ لنا الأسباب لنتم هذا العمل في أحسن صورة.

نتقدم بجزيل الشكر والعرفان وعظيم الإمتنان للأستاذ الفاضل عبد الجليل بن محفوظ دوارجة " على مجهوداته المبذولة وتوجيهاته المقدمة لنا، فكان خير معلم ونعم الأستاذ، فله منا جزيل الشكر ووافر التقدير والإحترام وجعله الله ذخر طلبة العلم وجزاه عنا خير جزاء

ونشكر أيضاً كل عمال مكتبة كلية الحقوق والعلوم السياسية الذين قدموا لنا يد العون في توفير المراجع الخاصة ببحثنا هذا.

كما نشكر كل من مد لنا يد العون من قريب أو من بعيد بجامعة محمد البشير الإبراهيمي دون استثناء.

إهداء

" بسم الله خالقي وميسر أموري

و عصمت أمري لك كل الحمد والامتنان "

أهدي هذا النجاح لنفسي أولا ثم الى كل من سعى معي لإتمام هذه المسيرة دمتم لي سندا لا عمرا.

الى من دعمني بلا حدود وأعطاني بلا مقابل، الى من علمني أن الدنيا كفاح وسلاحها العلم والمعرفة، والى من غرس في روحي مكارم الاخلاق داعمي الأول في مسيرتي وقوتي من بعد الله "

والدي الغالي بلعيد حمد "

الى من جعل الله جنة تحت أقدامها الى من كان دعائها سر نجاحي وحنانها بلسم جراحي، قدوتي ومعلمتي الأولى وصديقة ايامي "

والدتي الحنونة بلعيد دليلة "

و الى من شدّ الله بهم عضدي " اخواتي واخواني "عبد الله . كوثر . محمد

و لا أنسى رفقاء الروح الذين شاركوني خطوات هذا الطريق، الى من شجعوني على مثابراتي واكمال المسيرة الى رفقاء السنين هديل و اكرام و سارة ممتنة لكم جميعا

هذا التخرج ليس مجرد شهادة بل هو تتويج لكل لحظة كنتم فيا بجانبي ولكل دعوة رفعتموها من أجلي أحبكم جميعا من أعماق قلبي وأهديكم هذا النجاح الذي هو بفضلكم بعد الله

إهداء

الحمد لله رب العالمين وألف صلاة وسلام على رسوله الكريم

قال تعالى في كتابه الجليل:

إلى رمز المحبة والحنان إلى من سهرت على تربيتي إلى من منحتني القوة

والحنان إليك أمي العزيزة حفظك الله وأطال عمرك

إلى الذي رسم لي طريق العلم بحبه وعلمني معنى الحياة بكده وجهده

إلى أبي الغالي

إلى أولادي يوسف، أيوب وألاء الرحمان

إلى كل الأهل وإلى كل من ساهم في هذا العمل من قريب أو بعيد

أهديكم هذا العمل المتواضع

مـــقـــدمة

مقدمة:

شهدت البشرية مرحلة تطور متميزة ارتبطت بتطور التكنولوجيا الهائل ومعالمه الكبرى في الرقمنة المتزايدة والفضاء الافتراضي ،كما ظهر مجتمع المعلومات والمعرفة والذي أدى إلى هيمنة وسائل الإعلام والاتصال فهذه الثورة التكنولوجية برزت كطفرة تطورية غير مسبوقة في فترة زمنية قصيرة والتي أثرت على التكنولوجيا وعلى الأمن الالكتروني مما أصبح الأمن ضرورة حتمية لأن حياتنا مرتبطة ارتباطا وثيقا بوسائل الاتصال الحديثة التي سهلت طرق التواصل بكل أشكالها (السمعية، البصرية والمكتوبة).

ومن هنا فإن الحفاظ على الخصوصية في حياة كل شخص أضحى من المستحيلات لوجود ما يهدد هذه الخصوصية عن طريق ما يسمى بالإرهاب الالكتروني، والذي يعتبر آخر ما توصل إليه العقل الإجرامي في تنامي الثورة التكنولوجية والمعلوماتية وبالتوافر السهل لشبكة الأنترنت وملحقاتها المادية فأصبح العالم دولا وأفرادا يتعرض اليوم لهجمات ارهابية عبر الفضاء الرقمي، وتختلف حدة هذه الهجمات حسب نوعها وهدفها وغايتها فقد تصيب المصالح الأساسية للدول وأمنها أو سيادتها القومية وقد تستهدف سلامة المواطنين وطمأنينتهم فالإرهاب الالكتروني هو أحد الجوانب الأكثر سلبية في استغلال التطور الحاصل في تقنية المعلومات.

1- أهمية الموضوع:

تتجلى أهمية الموضوع أولا في خطورة الارهاب الإلكتروني والتي تعدد ضحاياه بين الأفراد والدول والكيانات الأخرى، وما أصبحت تثيره هذه الجريمة من مخاوف وقلق لدى المجتمع الدولي والمحلي بسبب تهديدها وتطورها المستمرين، ومن الخصائص التي تميز الإرهاب الالكتروني صعوبة اكتشافه وملاحقة مرتكبيه وغيرها.

اضافة لخطورة هذه الظاهرة على البنى التحتية لأنظمة تقنية المعلومات والاتصالات ،وتحديد طبيعة الاختراقات والهجومات المستمرة في شتى المجالات، وذلك

لأنه يتميز عن غيره من أنواع الإرهاب الالكتروني بطريقته العصرية المتمثلة في استخدام موارد المعلوماتية والوسائل الإلكترونية والبنية التحتية المعلوماتية، فهي جريمة تتميز بحداثة الاسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محوا آثارها وتعدد صورها.

2-أسباب اختيار الموضوع:

اخترنا دراسة موضوع جريمة الإرهاب الالكتروني لمجموعة من الأسباب الشخصية والأسباب الموضوعية.

فتنطوي الأسباب الشخصية في الميول الشخصي لدراسة مثل هذه المواضيع وعلاقة موضوع الدراسة بمجال التخصص قانون اعلام الي وانترنت والرغبة في دراسة المواضيع الجنائية الدولية.

أما الأسباب الموضوعية فهي تتجلى في الأهمية العلمية لموضوع جريمة الإرهاب الإلكتروني وما يترتب عنها من آثار، والأليات القانونية لمكافحة هذه الجريمة على المستوى الوطني والدولي .

اضافة إلى حداثة الموضوع خاصة بما يتعلق توضيح كونه من الجرائم المستحدثة والتي هي محل اهتمام الدراسة بمختلف المجالات، ويعكس آثارا سلبية على الأفراد والدول مما يجعل من المهم والمفيد التطرق إليه بالدراسة والتحقيق والتدقيق فيه .

3- إشكالية الموضوع :

تتلخص إشكالية الموضوع في البحث عن مفهوم الإرهاب الإلكتروني ومظاهره المتنوعة والجهود المحلية والوطنية والدولية في مكافحته.

فمن خلال ما سبق يتبادر في ذهننا طرح الإشكالية التالية:

"ماهية الإرهاب الإلكتروني ؟وما مدى نجاعة الجهود الدولية والوطنية في مواجهتها؟" .

4- أهداف الموضوع:

تهدف هذه الدراسة لتسليط الضوء على ظاهرة الإرهاب الإلكتروني بشكل دقيق، وكذا دراسة وتحليل الاطار القانوني الوطني المتعلق بجريمة الإرهاب الإلكتروني، ودراسة ما ورد في الاتفاقيات الدولية والقانونية المقارنة وتوعية الافراد والجماعات باعتباره خطرا مستحدثا، وكيفية تجنبه ومكافحته على الصعيد الوطني والاقليمي والدولي

5- المنهج المتبع:

اعتمدنا في دراستنا هذه على :

- المنهج الوصفي للبحث والتعمق في مفهوم الإرهاب الإلكتروني، من خلال التطرق إلى الاجتهادات والتطبيقات والمفاهيم المتعددة لجريمة الإرهاب الإلكتروني وما عمل به المشرع وما تناوله الفقه في مؤلفاته.
- المنهج التحليلي للإجابة على تساؤلات الدراسة المطروحة من خلال تحليل أحكام العقوبات والتفاقيات والمعاهدات.

6. صعوبات الدراسة:

- موضوع جديد وغير متداول في دراستنا وبالتالي نقص في المراجع بشدة وصعوبة الوصول إليها
- عدم وجود نصوص قانونية صريحة ومبسطة في بعض البلدان ومنها الجزائر تخص الإرهاب الإلكتروني بالتحديد بل يتم ادراجه ضمن الجرائم العامة ما يخلق غموضا تشريعيا.

ولقد حاولنا تقسيم هذه الدراسة إلى فصلين:

الفصل الأول: تناولنا فيه الإطار المفاهيمي للإرهاب الإلكتروني حيث تطرقنا في المبحث الأول: مفهوم الإرهاب الإلكتروني، وأشكاله ومظاهره في المبحث الثاني.

كما تناولنا في الفصل الثاني: الاساس القانوني لجريمة الإرهاب الإلكتروني حيث خصصنا المبحث الأول اركان جريمة الإرهاب الإلكتروني، والمبحث الثاني لسبل مكافحة الإرهاب الإلكتروني.

الفصل الأول:

الإطار المفاهيمي للإرهاب الإلكتروني

مع التطور الاخير الذي شهدته تكنولوجيا المعلومات والاتصالات والاعتماد الكبير على الاجهزة الذكية وما نتج عليها من تطبيقات الانترنت مثل فيسبوك، واتساب وغيرها... مما جعلها جزءا لا يتجزأ من الحياة اليومية وجعل هذا التطور شبكة الانترنت أداة عالمية لتبادل المعلومات مما ألغى كل الحواجز الجغرافية وجعل العالم قرية صغيرة.

غير أن هذا التقدم التكنولوجي لا يخلى من السلبيات إذ جعل العقود الإجرامية أكثر تطورا ودهاء في استغلال الوسائل الحديثة لأساليبهم الاجرامية فظهر ما يسمى بجريمة الإرهاب الإلكتروني.

فهذا النوع من الجرائم يرتكب باستخدام الفضاء الرقمي في تنفيذ أنشطتهم الإرهابية وتحقيق أهدافهم من خلال اختراق الأنظمة الإلكترونية لإلحاق الضرر بالجماعات والافراد.

وعليه خصصنا المبحث الأول للتعريف بمفهوم الإرهاب الإلكتروني وهذا ما سنتناوله من خلال:

- المبحث الأول: مفهوم جريمة الارهاب الالكتروني.
- المبحث الثاني: اشكال الارهاب الالكتروني ومظاهره.

المبحث الأول

الاطار المفاهيمي للإرهاب الإلكتروني

أصبح من السهل لمرتكبي جرائم الإرهاب الإلكتروني تهديد الحياة العامة عن طريق اقتحام المواقع الالكترونية وتدميرها وتغيير محتوياتها أو الدخول على شبكات الاتصال بهدف تعطيلها عن العمل لأطول فترة ممكنة أو تدميرها نهائيا، كما بات عنده من الضروري ابتكار الاف المواقع لنشر أفكارهم ومعتقداتهم والتخطيط والتجهيز لعمليات إرهابية ولتنسيق وتبادل الخبرات الميدانية العلمية فيما بينهم، فالإرهاب الإلكتروني هدفه الحاق الشلل لأنظمة القيادة والسيطرة والاتصالات وكذا تعطيل أنظمة الدفاع واختراق النظام المصرفي وارباك حركات الطيران المدني وشل مخططات الطاقة الحرارية أو النووية فهذا هو الأسلوب الجديد للإرهابيين حاليا في محاولة الوصول الى اغراضهم بكل ارتياح وطمأنينة لذا من الاهمية دراسة مفهوم الإرهاب الإلكتروني ومعرفة أشكاله ومظاهره.

المطلب الأول

تعريف الإرهاب الإلكتروني

أصبح الارهاب الالكتروني من أبرز التهديدات التي تواجه المجتمعات والدول في العصر الرقمي، إذ لم يعد الارهاب مقتصرا على الاساليب التقليدية، بل انتقل الى الفضاء الالكتروني مستغلا التطور التكنولوجي الهائل، ولتحديد مفهوم الارهاب الالكتروني بدقة، لابد من التطرق لتعريفه من جوانب مختلفة: لغة، اصطلاحا، شرعا وقانونا لفهم مختلف جوانبه.

الفرع الأول

تعريف الإرهاب الإلكتروني لغة واصطلاحا

أولا: تعريف الإرهاب الإلكتروني لغة

هو مأخوذ من رهِبَ بالكسر ،يرهب رهبة ورهباناً وبالضم رهبُ، أي خاف ورهب الشيء رهبا ورهبة: خافه.[1]

"وأَرهَبَه ورَهَبَه وإسترهبه: أخَافه وفَزَعَه".[2]

وأطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف "يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم السياسية "[3]

ويعني الإرهاب في اللغات الأجنبية القديمة مثل اليونانية "حركة من الجسد تفزع الاخرين".[4]

وبحسب هذه التعاريف فالإرهاب في اللغة دالُ عن الاخافة والترويع.

ثانيا: تعريف الإرهاب الإلكتروني اصطلاحا.

لم يصل المجتمع الدولي حتى الآن لتعريف جامع مانع متفق عليه للإرهاب الالكتروني وذلك لتنوع أشكاله واختلاف جهات النظر الدولية والسياسية.

وأن المشكلة عدم تحديد المجتمع الدولي لمفهوم الإرهاب دفعت جميع المؤتمرات العربية والإسلامية التي بحثت في موضوع الإرهاب الى تحديد هذا التعريف واستعدادها

---

[1] ابن منظور، ابو فضل جمال الدين محمد بن مكرم ،لسان العرب، ط1 ،دار صادر ،بيروت، 436.1 حرف الباء ،فصل الراء، مادة رهب

[2] المرجع نفسه، 436.1، حرف الباء، فصل الراء، مادة رهب

[3] المعجم الوسيط، صادر عن مجمع اللغة العربية بجمهورية مصر العربية، ط4، مكتبة الشروق الدولية ،1435هـ 2004م ،376، مادة رهبه

[4] صدقي، عبد الرحيم ،الارهاب السياسي والقانون الجنائي، دار النهضة العربية ،القاهرة ،1958م، 81

للتعاون مع المجتمع الدولي لوضع مصطلح محدد له، فعرفته الاتفاقيات الدولية لمكافحة الإرهاب في جنيف 1937، الإرهاب بأنه "الافعال الاجرامية الموجهة من إحدى الدول ضد دولة اخرى والتي يكون هدفها إثارة الفزع والرعب لدى جماعات من الناس ".

كما عرفت الاتفاقات العربية لمكافحة الإرهاب الصادرة بالقاهرة عام 1998بأنه "كل فعل من أفعال العنف أو التهديد أين كانت بواعثه أو أغراضه يقع تنفيذ المشروع إجرامي أو جماعي ويهدف الى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستلاء عليها أو تعريض أحد الموارد الوطنية للخطر".[1]

الفرع الثاني

تعريف الارهاب شرعا

هناك الكثير من التعريفات للإرهاب، ومنها ما وضعه علماء المجامع الإسلامية ومن أفضل هذه التعريفات الاصطلاحية الشرعية للإرهاب تعريف مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فقد عرف الإرهاب بأنه "العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان دينه ودمه وعقله وماله وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الخرابة وإخافة السبيل وقطع الطريق وكل فعل من أفعال العنف أو التهديد يقع تنفيذ لمشروع إجرامي فردي أو جماعي ويهدف الى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حرياتهم أو أمنهم أو اموالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق والإملاك العامة أو الخاصة ،أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر ،فكل هذا من صور الفساد

[1] جاسم محمد جندل ،الارهاب الالكتروني ،دار البداية ،ط1،عمان ،1435هـ.2014م، ص28.30

في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها.[1] في قوله تعالى "**وَلَا تُفْسِدُواْ فِي الأَرْضِ بَعْدِ إِصْلَاحِهَا ذَلِكُم خَيْرٌ لَكُمْ إِن كُنتُم مُؤْمِنِينِ** " سورة الأعراف (56).

كما أصدر مجمع الفقه الإسلامي الدولي قرار في دورت الرابعة عشر المنعقدة في الدوحة في 2003 م ذكر فيه تعريف مصطلح الإرهاب بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا الصادر في الدول أو الجامعات أو الأفراد على الأنسان في دينه أو نفسه أو عرضه أو عقله أو مال بغير حق يثني صنوف وصور الفساد في الأرض.[2] لقوله عز وجل "**إِنمَا جَزَاءُ الذِينَ يُحَارِبُونَ اللهَ وَرَسُولَهُ وَيَسْعَونَ فِي الأَرضِ فَسَادِا أَنْ يُقْتَلَوُا أَوْ يُصَلَبُوا أَوْ تُقْطَعَ أَيْدِيهِمْ وَأَرْجُلُهُمْ مِنْ خِلاَفٍ أَوْ يُنْفَوْا مِنَ الَأَرْضِ** " **(المائدة الآية 33).**

الفرع الثالث

تعريف الارهاب قانونا

بالرغم من الاختلاف في إعطاء تعريف جامع لجريمة الارهاب الالكتروني، إلا أن كانت هناك محاولات تشريعية تعريف جريمة الارهاب الالكتروني، والتي تتمثل في التعريفات التالية:

عرف القانون الدولي الإرهاب بانه " جملة من الأفعال التي حرمتها القوانين الوطنية لمعظم الدول". كما قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب ويكن ذكر أهم التعاريف لهذا المصطلح حيث عرفه الاتحاد الأوروبي عام 2002 بأنه أعمال ترتكب بهدف ترويع الأهالي أو إجبار الحكومة أو هيئة دولية على القيام بعمل أو امتناع عن القيام بعمل ما أو تدمير الهياكل الأساسية السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو لهيئة دولية أو زعزعت استقرارها.

[1] سفر ،حسن بن محمد "الارهاب والعنف في ميزان الشريعة الاسلامية والقانون الدولي" بحث مقدم لمجمع الفقه الاسلامي ،ص 9 و11

[2] سفر، حسن بن محمد، مرجع سابق، ص 11

كما اصدر مجتمع البحوث الاسلامية بالأزهر تعريف الإرهاب في سنة 2001 فقال عنه هو ترويع الآمنين ومصالحهم ومقومات حياتهم والاعتداء على اموالهم واغراضهم وحرياتهم وكرامتهم الانسانية بغيا أو افسادا في الأرض.[1]

كما أن هيئة الامم المتحدة عرفت الارهاب الالكتروني، وهذا من خلال شهر أكتوبر سنة 2021 بأنه استخدام الانترنت لنشر أعمال ارهابية.[2]

أما المشرع الجزائري، فقد تناول تعريف الارهاب الالكتروني في نص المادة 87 مكرر 11 الفقرة الرابعة من قانون العقوبات الجزائري، بأنه استخدام تكنولوجيا الاعلام والاتصال من أجل ارتكاب أفعال ارهابية.[3]

المطلب الثاني

خصائص الارهاب الالكتروني

يتميز الإرهاب الالكتروني بعدد من الخصائص والسمات التي يختلف فيها عن بقية الجرائم، وتحول دون اختلاط بالإرهاب العادي، ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يأتي:

- إن الإرهاب الالكتروني لا يحتاج في ارتكابه الى العنف والقوة ،بل يتطلب وجود حاسب آلي متصل بشبكة المعلوماتية ومزود ببعض البرامج اللازمة.
- يتسم الإرهاب الالكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات ،وغير خاضعة لنطاق إقليمي حدودي.

[1] جاسم محمد جندل، مرجع سابق، ص 25. 30

[2] علي مطر، الارهاب الالكتروني في القانون الدولي، مقال منشور على الموقع الالكتروني: https//:www.assakina.com/news/news1/31803.html، تاريخ الاطلاع: 23/05/2025 على الساعة 9:48 صباحا

[3] المادة 87 مكرر 11من القانون رقم 66 – 155 والمتعلق بقانون العقوبات، المعدل والمتمم بالقانون رقم 16 – 02 الصادر بتاريخ 2016/ 06 /19 الجريدة الرسمية، العدد 37 ،الصادرة بتاريخ 2016 / 06 / 22

- صعوبة اكتشاف الإرهاب الالكتروني ،ونقص الخبرة لدى بعض الاجهزة الأمنية والقضائية في التعامل مع هذا النوع من الجرائم.
- صعوبة الإثبات في الإرهاب الالكتروني، نظرا لسرعة غياب الدليل الرقمي ،وسهولة اتلافه ورميه
- يتميز الإرهاب الالكتروني بأنه يتم عادة بتعاون أكثر من شخص على ارتكابه.
- أن مرتكب الإرهاب الالكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات ،أو على الاقل شخص لديه قدرة من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.
- الأثر النفسي يعد من أبرز خصائص الإرهاب الالكتروني ،وما يتصل به من جرائم فالإرهاب الالكتروني لا يعني فقط التسبب في اضرار المادية، بل إنه قد يتسبب في أضرار معنوية تدخل ضمن الحرب النفسية حيث يتم الهجوم على المعتقدات أو الأفكار أو النسيج الاجتماعي والثقافي بهدف خلخلته وتكسير شبكة العلاقات القائمة، وتظل فكرة "الخوف من الإرهاب "هي المسيطرة على فلسفة الإرهاب الالكتروني، فبث المواد والفيديوهات التي تحمل محتوى عنيف أو دموي كالقتل أو التدمير أو غيرها ونشرها على الشبكة العنكبوتية يؤدي بلاشك الى العديد من الآثار النفسية السيئة.
- الإرهاب الالكتروني يعتمد على استراتيجية هجوم ذات دوافع سياسية وعقائدية وأيديولوجية ،فقد يكون هناك عنف ضد أهداف مدنية تقوم بها جماعات دون قومية أو عملاء سريين ،ويختلف الإرهاب الالكتروني عن الأشكال الأخرى من إساءة استخدام الكومبيوتر والتجسس الاقتصادي وحرب المعلومات.
- القائمين على الإرهاب الالكتروني لديم قدرة كبيرة على تغيير اساليب عملهم وأماكنهم ،بحيث يمكنهم الافلات من إمكانية مراقبتهم ،وذلك بإخفاء مواقعهم على الشبكة وإظهارها بثوب جديد.

- القائمين على الإرهاب الالكتروني يسهل التواصل بين بعضم البعض ،دون الحاجة الى اجتماعهم ،وذلك من خلال الرسائل الالكترونية وغيرها من الوسائل التواصل التي تتيحها الشبكة وبهذا يصعب تحديد أماكنهم.
- إن الاعمال الإرهابية التي تتم عبر الأنترنت تتسم بكونها تنتمي الى طائفة الجريمة المنظمة ،أي يخضعون لنظام صارم، بحيث إن المجموعات إن كانت تعمل لغرض واحد لكن لا تعرف بعضها البعض، واستخدامها لشبكة المعلوماتية يجعلها حريصة أكثر على تنظيم نفسها تنظيما محكما ودقيقا، لتحقيق الاستفادة القصوى من الامتيازات التي تُتيحها الشبكة التنظيمات التي تمارس الإرهاب الالكتروني تحرص على إعلان تبنيا لما يقع من أحداث إرهابية تتسبب بها ،وتعلن مسئوليتها عن ذلك ،ولا تحأول إنكاره.[1]

المطلب الثالث

أسباب الإرهاب الالكتروني وأهدافه

للإرهاب الإلكتروني عدة أسباب وأهداف نذكر منها:

الفرع الأول

أسباب الارهاب الالكتروني

أسبابه كثيرة ومتداخلة وسوف نتطرق الى بيان أهم أسباب الإرهاب عموما ثم سنتكلم عن أهم دوافع انتشار الإرهاب الالكتروني بوجه خاص:

[1] حسام فايز، الارهاب الالكتروني والثورة الرقمية، ط1 ،مؤسسة طيبة، القاهرة ،2019 م، ص 92.

أولا: الأسباب العامة للإرهاب:

مما لاشك فيه أن أسباب الإرهاب ودوافعه تختلف في درجة أهميتها وفي مدى تأثيرها باختلاف المجتمعات الدولية تبعا لاختلاف الاتجاهات السياسية والظروف الاقتصادية والاحوال الاجتماعية والاختلاف الديني والعقائدي ،لذا فأن ما يصدق على المجتمع قد لا يصدق بالضرورة على غيره من المجتمعات.

1. أسباب مادية:

هدف المنظمات الارهابية يكمن في السيطرة على مصادر الثروة وعلى المجتمع من أجل استغلالها ماديا ومعنويا، خاصة وأن الخيرات المادية ومصادر تلك الخيرات تعتبر محور الصراع الطبقي منذ انقسام المجتمع الى طبقات مستغلة للخيرات وطبقات محرومة منها ،فالجهات الممارسة للإرهاب تسعى إلى مصادرة حقوق الآخرين للاستفادة من الخيرات المادية عن طريق السيطرة على وسائل الانتاج مما يؤدي الى تسخيرها لصالح الجهات الممارسة للإرهاب لجعلها على المستوى القومي والاممي واستثمار الثروات في الوصول الى السيطرة على المؤسسات المالية والشركات العابرة للقارات، حتى تضمن السيولة الازمة لدعم الإرهاب على أعلى المستويات ونقله الى أي نقطة من العالم عن طريق الشبكة التي تكون لهذا الغرض وتمتد عبر القارات من اجل السيطرة على العالم.

2. **أسباب شخصية:**

تتعدد الدوافع الشخصية المؤدية للإرهاب ويمكن بيان أبرزها هي الرغبة في الظهور وحب الشهرة حيث لا يكون الشخص مؤهلا فيبحث عما يؤهله باطلا فيشعر بالعدوان والتخريب والتدمير والإحباط من عدم تحقيق اهدافه أو رغباته أو يشعر أنه أقل من غيره أو ينظر إليه بازدراء فيلجأ إلى الإرهاب والخروج من النظام ،إضافة إلى أن فقدان الشخص لدوره في الأسرة والمجتمع وفشله في كل جوانب الحياة يكسبه الصفات

السيئة وعدم شعوره بالانتماء والولاء للوطن ،كما أن إخفاقه في تجارب الحياة الاجتماعية والعاطفية يشعره بالفشل ونقمة الشخص على المجتمع الذي يعيش فيه نتيجة ما يراه من ظلم وإهدار لحقوق المجتمع فيتولد لديه الحقد والاستعداد للقيام بأي عمل يضر المجتمع.

3. **أسباب داخلية:**

إن الأوضاع الداخلية للبلدان العربية وغياب الديموقراطيات ،الفوارق الطبقية ،الأزمات الاجتماعية المطبوعة بالفقر والبطالة على وجه الخصوص تلعب دور المحرك للانخراط في أعمال العنف الموجهة نحو الخارج ،لأن للديمقراطية مسارب لإبداء الرأي والرأي الأخر وفي المجتمعات الديكتاتورية لا يوجد طريق للتعبير عن الرأي والرأي الأخر غير العنف والحركات الشعوبية والإرهابية لا تظهر ولا تمثل خطرا على المجتمع إلا عندما تخنق الحريات وتتعطل الاستحقاقات الديمقراطية.

4. أسباب سياسية:

إن ابرز الأسباب والدوافع السياسية لظاهرة الإرهاب هي السياسات غير العادلة التي تنتجها بعض الدول ضد مواطنيها والكبت السياسي الذي تمارسه عليهم وتهميش دور المواطن وتغييبه عن المشاركة السياسية وانتهاك حقوقه وعدم تلبية متطلبات التوازن الاجتماعي وانعدام تفعيل دور مؤسسات المجتمع المدني ،فبعض البلدان تدعي الديمقراطية وحرية الرأي وهذا من شأنه أن يولد المنظمات السرية وردود الافعال الغاضبة التي لا تنتج عنها سوى الإرهاب، غياب العدالة الاجتماعية عدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق الأساسية والاستيلاء على الأموال العامة وانعدام التنمية المستدامة وإهمال الرعية والتقصير في امورهم وانعدام الامانة وحفظ الديانة وتسهيل امورهم المعيشية والإنسانية، وما تعانيه بعض المجتمعات والشعوب الدولية من ظلم واضطهاد واحتلال وسيطرة استعمارية وانتهاك للحقوق وسلب الأموال مما دفع الشعوب الى التشدد والتطرف.

5. أسباب اقتصادية:

إن من أهم الدوافع الاقتصادية المؤدية لتفشي ظاهرة الإرهاب هي تفاقم الازمات الاقتصادية في المجتمعات الدولية بالإضافة الى المتغيرات الاقتصادية العالمية الاستغلال الاجنبي للموارد الطبيعية للدول النامية ،عدم القدرة على إقامة تعاون دولي جدي من قبل الأمم المتحدة ،عدم إيجاد حل لعدد من المشكلات العالمية مثل اغتصاب والنهب والاضطهاد اضافة الى المشكلات المتعلقة بالإسكان والديون والفقر وغلاء المعيشة والتضخم في أسعار الموارد الغذائية والخدمات الأساسية وعدم تحسن دخل الفرد كل هذه العوامل دفعت بعض الشباب الى التطرف والإرهاب ،انتشار البطالة في المجتمع وزيادة العاطلين عن العمل وعدم توفر فرص عمل لهم من أقوى العوامل المساهمة في امتهان الاعتداء والسرقة وتفشي الإرهاب لان المحرك الاساسي لها الجوع والفقر.

التقدم العلمي والتقني للأنظمة المصرفية العالمية ادى الى سهولة انتقال الاموال وتحويلها وتبادلها بين الجميع أرجاء العالم عن طريق الشبكة العالمية للمعلومات مما ساعد المنظومات الإرهابية على استغلال الفرصة من اجل تحقيق أغراضهم غير مشروعة، أصبح الاعتماد على الشبكات الكومبيوتر شل مطلق في مجال المال والاعمال مما جعلها هدفا مغريا للعابثين والهاكرز.

6. أسباب عسكرية:

أصبح يعتمد بشكل كبير على تقنية المعلومات في إدارة الصراع بين مختلف الدول والذي يعتمد اعتمادا كليا على الانترنت والكومبيوتر للقيام بعمليات الاختراق والوصول للمعلومات السياسية والعسكرية والاقتصادية وكذلك التجسس الالكتروني الناتج عن الاختراق والذي لا تكمن خطورته الكبيرة عندما يكون القائمون به منه الهاكر وإنما تكمن خطورته عندما تقوم بيه أجهزة المخابرات ،وتستهدف هذه النوعية من الهجمات عادة الاهداف العسكرية والمرتبطة بشبكات المعلومات وهذا النوع من الهجمات نادر

الحدوث لانها تتطلب معرفة عميقة بطبيعة الهدف وطبيعة المعلومات التي يجب النفاذ اليها وهي معرفة لا تمتلكها إلا الحكومات إضافة الى ان الحكومات تقوم بعزل المعلومات العسكرية الحساسة ولا تقوم بوصلها بالأجهزة التي تحملها بالعالم الخارجي ،ويبقى الحذر واجب من عمليات التخريب الداخلية ومن هنا تأتي ضرورة وضع نظم موثوقة.

7. **أسباب دولية:**

يمثل الفضاء الالكتروني بيئة استراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع وظهور فاعلين جدد على الساحة الدولية ومن ثم يمكن القول ان النظام الدولي قد اصبح امام ظاهرة متعددة في أبعادها ونطاق تأثيرها وملامحها مما فرض المزيد من التعقيد ظاهرة الإرهاب الالكتروني التي تنطوي على استخدام الكومبيوتر كأداة مثل فيروسات الكومبيوتر أو التجسس أو اختراق المواقع أو سرقة المعلومات وغسيل الاموال وغيرها من الاشكال ،ويمكنهم سرقة الهويات الشخصية لإخفاء اعمالهم إشاعة الاخبار الاقتصادية التي تأثر على البورصات العالمية مثل ظهرت حرب الفضاء الالكتروني والاختراق المتبادل بين اسرائيل وحلفائها وما بين غزة ومناصريها في كانون 2009وتعبير لها فقد استطاع متسللون الكترونيون مسلمون اختراق مواقع اسرائيلية معروفة وتغيير ما يعرض فيها من مشاهد ما يحدث من اعتداءات على مدينة غزة وسكانها.[1]

ثانيا: الأسباب الخاصة للإرهاب الالكتروني

1. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق فهي مصممة في الاصل بشكل مفتوح دون قيود أو حواجز أمنية مكثفة عليها رغبة في التوسع وتسهيل الدخول المستخدمين مما يغلق ثغرات يسهل الولوج من خلالها وممارسة الانشطة الإرهابية.

[1] جاسم محمد، مرجع سابق، 67. 93

2. أن غياب الحدود المكانية في الشبكة المعلوماتية ،فعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد فرصة مناسبة للإرهابين لممارسة أنشطتهم

3. سهولة الاستخدام وقلة التكلفة والتي تعتبر دافع للممارسة الأنشطة الإرهابية بشكل افتراضي.

4. الفراغ التنظيمي والقانوني وغياب الجهة المسيطرة على الشبكة المعلوماتية يساهم بشكل كبير في انتشار جرائم الإرهاب الالكتروني وتبادل محتواه ورسائله بسهوله ويسر.[1]

الفرع الثاني

اهداف الارهاب الالكتروني

يهدف الإرهاب الالكتروني الى تحقيق جملة من الاهداف غير المشروعة ويمكن ابراز تلك الاهداف في ضوء النقاط الاتية:

- نشر الخوف والرعب بين الاشخاص والدول والشعوب المختلفة.
- الإخلال بالنظام العام، والأمن المعلوماتي وزعزعة الطمأنينة.
- تعريض سلامة المجمع وامنه للخطر.
- إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات وبالأموال والمنشآت العامة والخاصة.
- تهديد السلطة العامة والمنظمات الدولية وابتزازها.
- الانتقام من الخصوم.
- الدعاية والإعلان ،وجذب الانتباه ،واثارة الرأي العام
- جمع الاموال والاستلاء عليها. [1]

[1] حسام فايز، مرجع سابق، ص 95

المبحث الثاني

أشكال الإرهاب الالكتروني وآثاره

في عصرنا الحالي، اصبحت التكنولوجيا جزءا لا يتجزأ من حياتنا اليومية، لكن مع فوائدها ظهرت أيضا مخاطر جديدة، من ابرزها ما يعرف بالإرهاب الالكتروني. هذا النوع من الارهاب لا يستخدم الاسلحة التقليدية، بل يعتمد على وسائل التكنولوجيا الحديثة مثل الانترنت لنشر الخوف والاضطراب وتهديد أمن الافراد والدول.

المطلب الأول

اشكال الارهاب الالكتروني

أدى التطور التكنولوجي في مجال الانترنت الى تطور الاعمال الإرهابية بوجه عام وظهور أنماط جديدة على مستوى الوطني والاقليمي والعالمي، فزادت معاناة دول العالم من النشاطات الإرهابية، كما استفادت الجماعات الإرهابية من مكاسب هذه الثروة والمعرفة التقنية لتحسين أهدافها ووظائفها، حيث استغلت هذه الجماعات شبكة الانترنت في تمويل نشاطها بعدة أشكال منها:

- **التهديد الالكتروني:** تعددت الأساليب الإرهابية في التهديد عبر الانترنت من تهديد بالقتل لشخصيات سياسية الى التهديد بتفجير في المراكز السياسية او التجمعات الرياضية، ثم التهديد بإطلاق فيروسات ولإتلاف الانظمة المعلوماتية في العالم. ومثال ذلك ما قام به شاب امريكي يدعى "جاهابر جويل" البالغ 18 عاما حيث قام بتهديد مدير شركة ميكروسوفت اذا لم يدفع له خمس ملايين دولار ،وقد تم القبض

[1] صدام حسين ياسين العبيدي، جرائم الانترنت وعقوباتها في الشريعة الاسلامية والقوانين الوضعية ،ط1 ،المركز العربي، مصر ،2019،ص200

عليه وتفتيش منزله فعثروا على حاسب آلي يحتوي عدة ملفات رقمية تحمل معلومات عن تصنيع القنابل تم إنزالها عبر الانترنت.

- **القصف الالكتروني:** هو أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الالكترونية الى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على استقبال رسائل من المتعاملين معها والذي يؤدي الى وقف عمل الشركة، وهذا ما تقوم بيه المنظمات الإرهابية لتدمير البنية التحتية الخاصة بأنظمة المعلومات في العالم، ومثال ذلك ما تعرض اليه موقع امازون لبيع الكتب على الانترنت، وايضا شركة سي إن أن للأخبار على الانترنت مما أدى الى بطء تدفق المعلومات لمدة ساعتين.
- **تدمير أنظمة المعلومات:** هو محاولة اختراق شبكة المعلومات الخاصة بالأفراد أو الشركات العالمية بهدف تخريب نقطة الاتصال أو النظام، عن طريق خلق نوع جديد من الفيروسات التي تسبب الكثير من الضرر لأجهزة الكومبيوتر والمعلومات المخزنة عليه، ففي استراليا عام 2000م تمكنت منظمة إرهابية من تدمير شبكة الصرف الصحي في إحدى المدن مما نجم عنها اضرار صحية واقتصادية فادحة.
- **التجسس الإلكتروني:** وهو التلصص وسرقة المعلومات من الافراد أو المؤسسات أو الدول أو المنظمات، والتجسس على هذه المعلومات أيا كان نوعها يأخذ أبعادا جديدة، فتعددت أهدافها من معلومات اقتصادية أو سياسية أو عسكرية أو شخصية، ومن أمثلة ذلك ما حدث في صيف 1994 عندما تمكنت جهات إرهابية من سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها الجيوش التابعة لحلف الشمال الاطلنطي من الانظمة الخاصة بسلاح البحري الفرنسي ،مما دفعهم لتصميم برامج جديدة لحماية حاسباتهم الالية.

- **الاختراق الالكتروني:** اختراق البورصة العالمية يهدد الاقتصاد الدولي أو اختراق موقع مطار دولي وتلاعب ببرامج الاتصالات يهدد سلامة ووصول الطائرات، ومثال ما حدث في الولايات المتحدة عندما تمكن احد القراصنة من السيطرة على نظام كومبيوتر لمطار صغير واطفأ مصابيح اضاءة ممرات الهبوط مما هدد بحدوث كارثة.
- **الإرهاب النووي:** وهو الذي بات الخوف منه يتخذ أبعادا بالغة الخطورة منذ بداية عقد التسعينات، ولا سيما مع ما تردد عن إمكانية حصول جهات إرهابية على رؤوس نووية أو مواد نووية من جمهورية الاتحاد السوفياتي السابق في ظل حالة الفوضى التي أصابت الترسانة النووية عقب تفكك الاتحاد السوفياتي.
- **الإرهاب الالكتروني:** يتمثل في استخدام الموارد المعلوماتية والمتمثلة في شبكات المعلومات وأجهزة الكومبيوتر وشبكة الانترنت من اجل اغراض تخويف أو الإرغام لأغراض سياسية، ويرتبط هذا الإرهاب الى حد كبير بالمستوى المتقدم للغاية الذي باتت تكنولوجيا المعلومات تلعبه في كافة مجالات الحياة في العالم، ويمكن أن يتسبب الإرهاب المعلوماتي بالحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصالات بين الوحدات والقيادات المركزية وتعطيل أنظمة الدفاع الجوي أو اخراج عن مسارها أو شل محطات الطاقة الكبرى[1].

المطلب الثاني

آثار الإرهاب الالكتروني

يتبلور جوهر الارهاب الالكتروني حول فكرة توظيف التكنولوجيا واستخدامها على نحو من التطرف باستخدام التخويف والعنف أو التهديد به بهدف تحقيق أغراض سياسية،

[1] جاسم محمد، مرجع سابق، ص105

وتقاس أهميته من الناحية العلمية بمدى ما يمكن أن يحدثه العنف من تأثير نفسي على الطرف المستهدف به وإجباره على تغيير سلوكه وإبدال موقفه اتجاه قضية معينة، وعلى هذا يمكن ان نستعرض ابرز أثار الارهاب الالكتروني على النحو التالي:

- **الاثر النفسي للإرهاب الالكتروني (التخويف، الذعر والحرب النفسية):** عندما يوجه الارهاب ضرباته في أوقات وأماكن مختلفة، فهو يكون قد أرسل إلى الحكومات والجمهور رسالة مفادها أنه قادر على توجيه ضرباته أينما شاء ووقتما شاء. وأن الحكومات ستكون عاجزة عن إيقافه. فمن خصائص الأعمال الإرهابية الإلكترونية أنها ترمي إلى إيجاد حالة من الذعر، وأنها تُرتكب بوسائل تتعدى نتائجها حالة الذعر والخوف، ويلتقي عنصر الخوف والذعر مع الحرب النفسية، والتي هي بمثابة عمليات لتمرير معلومات منتقاة للتأثير على العواطف والمعتقدات ودوافع وتبريرات الآخرين الموضوعية وسلوكياتهم، خاصةً سلوك الحكومات والمنظمات والجماعات والأفراد وتساعد العمليات النفسية التأثير على النفسيات وإضعاف الروح المعنوية وتخفيض فاعلية الخصم، وهي بذلك جزء من النشاط السياسي والمعلوماتي، وبالتالي فإن العمليات النفسية قد تكون وسيلة من وسائل العمليات الإرهابية والعكس صحيح فالإرهاب قد يستعمل الحرب النفسية لتحقيق عنصر التخويف والذعر والهلع في النفوس.
- نظرا لكون وقائع وجرائم الإرهاب الإلكتروني ذات طابع عالمي فهذا يجعل آثارها كذلك، مما يؤدي لوجود حالة من عدم الاستقرار في معظم أرجاء العالم، ومع هذا يشعر الانسان بالأمن والسلام
- قد تتسبب جرائم الإرهاب الإلكتروني في الإصابة بالأمراض العصبية والنفسية وهذه الأمراض تؤثر بشكل مباشر على تركيبة المجتمع وأخلاقه وسلوكه.

- تؤدي الافعال والجرائم الإرهابية الإلكترونية إلى أصداء دولية وتوابع سلبية خطيرة يتضرر منها أغلب أناس أبرياء، ففي أعقاب أحداث 11 سبتمبر 2001 اجتاحت القوات الأمريكية أفغانستان، وعانت ومازالت تعاني الجاليات الإسلامية في الولايات المتحدة وأوروبا من التضييق الأمني وانعزال واتخذت بعدها الدول الأوربية كثيرة العديد من المحاذير والتضييقات على مرور العرب والمسلمين في أوروبا.
- وللإرهاب الالكتروني آثار اقتصادية أيضا قد تتحقق عبر أكثر من طريقة من بينها، التهديد بانتقاء المعلومات لأغراض سياسية أو عسكرية أو اقتصادية وإستغلالها في بعض المجالات وتدميرها أو التهديد بتدمير معلومات ومكونات البناء المعلوماتي التحتي الحساس ذات تأثير كبير على الإقتصاد والأمن الوطني، ولاشك أن انتشار مثل هذه الأفعال على شبكة الإنترنت من شأنه أن يؤثر على السمعة الدولية للبلدان المستهدفة بمثل هذه التصرفات، الأمر الذي يعود على السياحة.
- حينما تمارس الإرهاب الإلكتروني أو تدعمه الدول فليس من الضرورة أن تكون إثارة في صورة استيلاء على أرض أو اغتيال أشخاص فقط، بل قد ينال النواحي النفسية للأفراد بشكل مباشر كما يفعل الكيان الصهيوني بممارسته للإرهاب الالكتروني على الشباب الفلسطيني، فالمواقع الفلسطينية على شبكة الانترنت تتعرض وبصفة مستمرة ومن الإسرائيليين إلى الاقتحام والعبث بمحتوياتها وازالة ما فيها من معلومات، وعرض صور العلم الاسرائيلي على الصفحة الرئيسية [1]

[1] حسام فايز، مرجع سابق، ص 103، 104

المطلب الثالث

الجهات الممارسة للإرهاب الالكتروني

الارهاب لا يحدث في الواقع دون وقوف جهة معينة ورائه، والجهات التي تقف ورائه هي الجهات التي من مصلحتها ممارسة الارهاب لإقصاء الاخر أو اخضاعه أو تصفيته جسديا أو فكريا أو عقائديا أو إيديولوجيا، والجهات الممارسة للإرهاب يمكن تصنيفها في:

الفرع الأول

الدولة

باعتبارها أداة السيطرة، فهي من تخلق الطبقات في المجتمع، وعدم المساواة في ما بينهم في اطار دولة القانون بانحيازها دائما الى الطبقة المسيطرة وعدم القضاء على الامية، كما تحدُ من الحريات العامة والفردية مما يحرم المواطنين من التعبير عن رأيهم، وقوف أجهزة الدولة وراء تزوير ارادة المواطنين في مختلف الانتخابات حتى لا تعمل ارادة الشعب في الخريطة السياسية، عدم العمل على تعميم الحماية الاجتماعية لجميع المواطنين وفي مختلف القطاعات حتى لا تتم مصادرة الحق في الحياة بسبب العجز عن العلاج بسبب الفقر وهذا ما يؤدي الى ظهور جريمة الارهاب الالكتروني.

الفرع الثاني

الجماعات المنظمة

وهي جماعات إرهابية مغلفة باللباس الديني، تهدف الى الترويج للعقائد المختلفة والخاطئة وتمارس هذه الجماعات ضد جماعات أو افراد ضد المجتمع. ومن هذه المنظمات المتطرفة حول عالم الانترنت لخدمة اغراضها منظمة حركة "إيتا" الانفصالية بإسبانيا، ومنظمة "توباك أمارو" ومنظمة "لاشكالاتوبيا" في أفغانستان. إضافة للعديد من

الكيانات الاخرى في المنطقة العربية والشرق الأوسط "موقع النداء" و"موقع البتار "وهي مجلة العلمية المتخصصة والتي فيها تنظيم أساسي يختص بالمعلومات العسكرية والمدنية.

الفرع الثالث

الافراد

هناك ارهاب الافراد الذين يلجؤون الى ممارسات تقود بطريقة مباشرة او غير مباشرة الى مصادرة حقوق الاخرين في السلامة الجسدية وفي الحياة وحماية الممتلكات وضمان رواج الافكار والقيم وحق التنقل والعمل وغيرها من الحقوق التي يلجأ بعض الأفراد الى مصادرتها اعتمادا على الامتيازات التي يتمتعون بها وبدعم من السلطة القائمة وبتزكية منها. [1]

[1] جاسم محمد، مرجع سابق، ص 229

خلاصة الفصل

يعدّ الارهاب من الجرائم التي اتفقت الدول من خلال التعريفات والاتفاقيات على مدى عنفه وتنوعه، ومنه الارهاب الالكتروني الذي يقوم على استغلال تكنولوجيا الاتصال والانترنت استغلالا سلبيا، مثل تحقيق أعمالهم التخريبية والحاق الضرر بالأفراد والمؤسسات، وهذا ما قمنا بدراسته في الفصل الأول من خلال تعريفه وذكر اهم خصائصه واسباب ارتكاب هذه الجريمة والاهداف التي يسمو اليها، كما ختمنا الفصل بأهم أشكال ومظاهرة جريمة الارهاب الالكتروني.

الفصل الثاني:

الأساس القانوني لجريمة الإرهاب الإلكتروني.

أصبح الارهاب الالكتروني من أخطر التهديدات التي تواجه الدول والمجتمعات في العصر الرقمي، حيث يستغل الارهابيون الفضاء السبيراني لنشر أفكارهم المتطرفة، وتنسيق العمليات، وإستهداف البنى التحتية الحيوية [1].

ويعد تجريم هذا النوع من الافعال ضرورة قانونية لحماية الامن القومي والسلم العام، مما أدى الى تدخل المشرع الوطني والدولي لوضع أسس قانونية تحدد ماهية ووسائل مكافحته.[2]

[1] سامي منصور، الارهاب الالكتروني: التحديات القانونية والامنية، مجلة العلوم القانونية، جامعة الجزائر 1، ع 19، 2020، ص 97

[2] فتحية سرور، الوسيط في قانون العقوبات، القسم العام، دار الشروق ' القاهرة، 2004، ص 412

المبحث الأول

أركان جريمة الارهاب الالكتروني

لا تكون جريمة الارهاب الالكتروني كاملة الا اذا تحقق فيها اركان خاصة بها، فهي تعتبر كالجرائم الاخرى والتي لا بد من الوقوف على أركانها التي تكون البنية القانونية اللازمة لقيام المسؤولية الجنائية: وهي الركن الشرعي، والركن المادي، والركن المعنوي[1].

المطلب الأول

الركن الشرعي لجريمة الارهاب الالكتروني

الركن الشرعي يقصد به بوجود نص قانوني يجرم الفعل ويقرر له عقوبة، عملا بمبدأ "لا جريمة ولا عقوبة إلا بنص " المنصوص عليه في المادة 1 من قانون العقوبات الجزائري[2]. ويعد هذا الركن أساسا ضروريا لأي متابعة جزائية.

الفرع الأول

تعريفة الشرعية الجنائية

يقصد بمبدأ الشرعية الجنائية أو الركن الشرعي للجريمة وجود نص يجرم الفعل ويقدر عقوبته قبل وقوعه، وعدم تمتع الفعل بسبب من أسباب الاباحة. والركن الشرعي للجريمة هو النص الذي يجرم الفعل المرتكب والمنصوص عليه في قانون العقوبات، حيث ينص هذا الاخير على أن لا جريمة ولا عقوبة ولا تدبير أمن الا بنص، وبالتالي

[1] سامي منصور، مرجع سابق، ص 102

[2] الجمهورية الجزائرية الديمقراطية الشعبية، قانون العقوبات الجزائري، المادة 1، الجريدة الرسمية، ع 14، 2006

فكل فعل غير مجرم في قانون العقوبات يعتبر فعل مباح حتى ولو أنكرته اخلاق العادات والاعراف. [1]

وفيما يتعلق بجريمة الارهاب الالكتروني، لم يخصص المشرع الجزائري نصا صريحا تحت هذا المسمى لكنه تناولها من خلال تلاقي نصوص قانونية في قانون مكافحة الارهاب وقانون مكافحة جرائم المتصلة بتكنولوجيا الاعلام والاتصال. حيث نص القانون رقم 04. 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون رقم 95. 11 على توسيع مفهوم العمل الارهابي يشمل أفعال التي ترتكب على وسائل التكنولوجيا لأغراض ارهابية.

كما صدر القانون رقم 09. 04 المؤرخ في 5 اوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، والذي يجرم أفعالا مثل: الدخول غير مشروع الى انظمة المعلومات، التحريض عبر الانترنت، ونشر محتوى يهدف الى زعزعة الامن العام.[2] وعند اجتماع هذه الافعال مع القصد الارهابي نكون امام جريمة ارهاب الكتروني يستند تجريمها الى تضافر النصوص المذكورة.

وعمد المشرع الجزائري على تحديد الركن الشرعي لظاهرة الارهاب والمتمثلة في النصوص القانونية التي تجرم كافة السلوكيات لهذه الظاهرة سواءا في قانون العقوبات عامة وفي القوانين الخاصة على ظاهرة الارهاب في قانون العقوبات في المواد 87 مكرر الى 87 مكرره 10 ولم يقف على تجريمه الارهاب التقليدي بل الثغرة القانونية في سنة 2016 لمسايرة التطورات الحاصلة لارتكاب الجرائم باستعمال التكنولوجيا الحديثة من الانترنت ونظام المعلوماتية وما يسمى بتجريم الارهاب الالكتروني في قانون 16. 02 الذي يتمم الامر 66. 156 المتضمن قانون العقوبات بموجب المادة 87 مكرر 11

[1] بلعيات ابراهيم، اركان الجريمة وطرق اثباتها، دار الخلدونية، ط 1، الجزائر، 2007، ص 94

[2] القانون رقم 09. 04 المؤرخ في 5 اوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية الجزائرية، ع 50

و87 مكرر 12 في القسم الرابع مكرر من الفصل الأول في الكتاب الثالث تحت عنوان الجرائم الموصوفة بأفعال ارهابية تخريبية. [1]

الفرع الثاني

العقوبات المقررة لجريمة الارهاب الالكتروني وفقا للقانون رقم 02.16

تترتب على جريمة الارهاب الالكتروني مجموعة من الاثار منا توقيع العقوبة على مرتكبيها، وبتحليل مواد قانون رقم 16.01 المتمم لقانون العقوبات يتبين أن العقوبات المقررة لجرائم الارهاب الالكتروني تتراوح ما بين العقوبات السالبة للحرية والغرامة المالية، [2] وهذا ما سنراه في الفقرة الاتية:

أولا: السجن المؤقت

كل جزائري أو أجنبي_مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر الى دولة اخرى بغرض ارتكاب أفعال ارهابية أو تدبيرها أو الاعداد لها أو المشاركة فيا أو التدريب على ارتكابها أو لتلقي تدريب عليها، وكل من يوفر أو يجمع أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال ارهابية أو تدبيرها أو الاعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، وكل من قام عمدا بتمويل أو تنظيم سفر أشخاص الى دولة أخرى بغرض ارتكاب أفعال ارهابية أو تدبيرها أو الاعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي تدريب عليها أو تسهيل ذلك السفر ،و كان ارتكاب الافعال المذكورة باستخدام تكنولوجيا

[1] المواد 87 مكرر الى 87 مكرر 12 من القانون 16. 02، المؤرخ في 14 رمضان 1437هـ الموافق ل 19 يونيو 2016، يتمم الامر رقم 66. 156 المؤرخ في 18 صفر 1386هـ الموافق ل8 يونيو 1966م والمتضمن قانون العقوبات، ج.ر.ع.4 مؤرخ في 17 رمضان 1437هـ الموافق ل 22 يونيو 2016.

[2] مهني رمزي، سبيعة محمود، جريمة الارهاب الالكتروني، مذكرة لنيل شهادة ماستر، قانون اعلام الي والانترنت، جامعة برج بوعريريج ،الجزائر، 2023 ،ص 24

الاعلام والاتصال لارتكاب الافعال السالفة الذكر، بالسجن المؤقت من خمس (5) سنوات الى عشر (10) سنوات، وهو ما نصت عليه المادة 87 مكرر 11من القانون 02.16.

ويعاقب بنفس العقوبة مستخدم تكنولوجيا الاعلام والاتصال من أجل تجنيد الاشخاص لصالح إرهابي أو جمعية أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو بدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة، وهو مانص عليه المشرع الجزائري بموجب المادة 87 مكرر 12 من القانون رقم 02.16.[1]

ثانيا: عقوبة الحبس

يمكن التوقيع بصدد جرائم الارهاب الالكتروني بعقوبة الحبس وهي عقوبة مقررة لمقدمي خدمات الانترنت، حيث عرفت المادة 2 فقرة د من القانون رقم 04.09 مقدمو خدمات الانترنت على أنهم أي كيان كان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات أو أي كيان اخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعمليها.[2]

فمقدم خدمات الانترنت الذي لا يقوم رغم اعذاره من الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته، أو صدور أمر، أو حكم قضائي بتدخل الفوري بسحب أو تخزين محتويات التي يتيح الاطلاع عليها، أو جعل الدخول اليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص

[1] المواد 87 مكرر الى 87 مكرر 12، مرجع سابق

[2] القانون رقم 09 – 04، مؤرخ في 14 شعبان عام 1430 الموافق ل5 غشت 2009 ،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،الجريدة الرسمية ،ع 47 ،مؤرخ في 25 شعبان 1430هـ، الموافق ل16 غشت 2009م.

عليها قانونا أو لجعل الدخول اليها غير ممكن قانونا، يعاقب بالحبس من سنة الى ثلاث سنوات.[1]

ثالثا: الغرامة المالية

اضافة الى توقيع العقوبة على الشخص المرتكب لجريمة الارهاب الالكتروني بسلب حريته بالحكم عليه بالسجن المؤقت والحبس المؤقت، يمكن علاوة على ذلك أن يقوم القاضي بالحكم المجني عليه بغرامة مالية تتراوح ما بين 100.000 دج الى 5000.000 دج، وهذه العقوبة توقع على كل جزائري أو أي شخص أجنبي مقيم بالجزائر سواء بطريقة شرعية أو غير شرعية يسافر أو يحأول السفر الى دولة اخرى بغرض ارتكاب افعال ارهابية أو الاعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تدبيرها أو المشاركة فيها، كما تطبق أيضا على كل من قام عمدا بتمويل أو تنظيم سفر أشخاص الى دولة أخرى بغرض ارتكاب افعال ارهابية أو تدبيرها أو الاعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي التدريب عليها أو تسهيل السفر من أجل القيام بها، كما تطبق على كل من يوفر أو يجمع عمدا أموالا بأي وسيلة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بانها تستخدم في تمويل سفر أشخاص الى دولة اخرى بغرض إرتكاب أفعال ارهابية أو الاعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تدبيرها أو المشاركة فيها، وعلى كل من يستخدم تكنولوجيات الاعلام والاتصال لتجنيد الاشخاص لصالح إرهابي أو جمعية أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة.[2]

[1] المادة 394 مكرر من 8 الى 11، قانون العقوبات، الامر رقم 66 – 156المؤرخ في 8جوان 1966 المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 76، 2021.

[2] المادة 87 مكرر 11 ،المرجع السابق

وقد تكون العقوبة المالية تتراوح من 2.000.000 دج الى 10.000.000 دج، تطبق هذه العقوبة على مقدمي خدمات الانترنت الذين يمتنعون عن القيام بالتدخل الفوري بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول اليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو الامتناع عن وضع ترتيبات تقنية تسمح بسحب أو تخزين محتويات التي تتعلق بالجرائم المنصوص عليها قانونا أو لجعل الدخول اليها غير ممكن رغم إعذارهم من طرف الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، أو صدور أمر أو حكم قضائي يلزمه بذلك وهو ما نصت عليه المادة 394 مكرر 8 من القانون رقم 02.16.[1]

المطلب الثاني

الركن المادي لجريمة الارهاب الالكتروني

يعتبر الركن المادي جسم الجريمة حسب مبدأ لا جريمة دون ركن مادي، وهو ذلك الفعل المحظور الذي يخرج الى العالم الخارجي ويشكل إعتداءا على الحق الذي يحميه القانون ويهدد النظام والامن العام. ويتكون الركن المادي من ثلاثة عناصر أساسية مترابطة فيما بينها تتمثل في:

1. السلوك الاجرامي من المجرم
2. النتيجة الاجرامية المتحققة في العالم الخارجي
3. العلاقة السببية بين المجرم والنتيجة الحاصلة [2]

[1] المادة 394 مكرر 8، المرجع السابق

[2] خليفة عبد الرحمان، محاضرات في القانون الجنائي العام ،دار الهدى ،عين مليلة، الجزائر ،2012، ص 101

الفرع الأول

السلوك الاجرامي

السلوك الإجرامي في جرائم الارهاب بصورتها التقليدية يقوم على افعال التخريب والقتل والتدمير، وكذلك خلق حالة من الذعر والرعب في صفوف الناس، والمواد المستخدمة في هذه الجرائم هي المواد المتفجرة والاسلحة المختلفة وما الى ذلك، أما في الارهاب الالكتروني فان الامر يختلف عن ذلك حيث يكون السلوك الاجرامي متمثلا بإنشاء المواقع على شبكة الانترنت أو احدى وسائل تقنية المعلومات لجماعات ارهابية تحت مسميات تمويهية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الاجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الاعمال الارهابية أو نشر أفكار ومبادئ التنظيم الارهابي والدعوة له أو في تمويل العمليات الارهابية والتدريب عليها أو تسهيل الاتصال بين التنظيمات الارهابية أو بين أعضائها وقيادتها. وهذا السلوك الاجرامي للإرهاب الالكتروني الذي تكون أدواته ووسائله الحاسب الالي والانترنت ووسائل تقنية المعلومات يختلف عن السلوك الاجرامي في الارهاب التقليدي الذي يقوم على التخريب والتدمير والقتل وبث الرعب والذعر بين الناس.[1]

فالسلوك الاجرامي هو ذلك النشاط الصادر من الجاني بصفة اختيارية ويحدث أثر في العالم الخارجي ويعاقب عليه القانون، وهو نوعان: أما سلبي أو سلوك ايجابي، فالأول يتحقق في حالة الامتناع عن الفعل أو قول يأمر عليه القانون، أما الثاني هو القيام بفعل يجرمه القانون ويؤدي الى احداث نتيجة في الجرائم ذات النتيجة وكذلك يعتبر سلوكا اجراميا في ذاته في الجرائم الشكلية ولا يعتد القانون بالوسيلة المستعملة سواء كانت مادية أو معنوية في ارتكاب سلوك الاجرامي بما أن المشرع الجزائري جرم فعل الارهاب

[1] صدام العبيدي، مرجع سابق، ص 233

الالكتروني في نص المادتين 87 مكرر 11 و87 مكرر 12، ومن هاتين المادتين يمكن استخلاص السلوكيات الاجرامية المكونة للركن المادي لهذه الجريمة.[1]

أولا: السلوك الاجرامي الوارد في نص المادة 87 مكرر 11 قانون العقوبات الجزائري.

تنص المادة 87 مكرر 11:"كل جزائري واجنبي مقيم بالجزائر، بطريقة شرعية أ، غير شرعية، يسافر أو يحاول السفر من دولة لأخرى بغرض ارتكاب أفعال ارهابية او تدريبها أو الإعداد له أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

و يعاقب بنفس العقوبة كل من:

- يوفر صمت جمع عمدا اموالا باي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو علم بأنها ستستخدم في تمويل سفر أشخاص الى دولة اخرى بغرض ارتكاب الافعال المذكورة في الفقرة الأولى من هذه المادة.
- كل من قام عمدا بتمويه أو تنظيم سفر أشخاص الى دولة اخرى بغرض ارتكاب أفعال إرهابية أ، الاعداد لها أو المشاركة فيها أو التدريب علي ارتكابها أو لتلقي تدريب عليها أو لتسهيل ذلك السفر.
- يستخدم تكنولوجيا الاعلام والاتصال لارتكاب الافعال المذكورة في المادة 87 مكرر من الامر رقم 66 / 156 متضمن قانون العقوبات المعدل والمتمم.[2]

ومن خلال هذه المادة نجد أن المشرع الجزائري جرم جملة من الافعال المتمثلة في:

1. **فعل السفر لغرض إرهابي باستخدام تكنولوجيا الاعلام والاتصال:** من خلال قراءتنا للمادة نجد أنها تجرم فعل السفر على الجزائريين والاجانب المقيمين بالجزائر بصفة شرعية او غير شرعية إذا كان الهدف منه القيام بعمليات إرهابية أو التدريب عليها أو

[1] منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006، ص 98 و99

[2] المادة 87 مكرر، مرجع سابق

الاعداد لا أو التدريب على ارتكابها أو لتلقي تدريب عليها، باستخدام تكنولوجيا الاعلام والاتصال لارتكاب الافعال الارهابية.[1]

2. **فعل التمويل باستخدام تكنولوجيا الاعلام والاتصال:** تجرم الفقرة الثانية من نص المادة 87 مكرر 11 السالفة الذكر فعل التمويل ويظهر ذلك من خلال مصطلح: يوفر أو يجمع عمدا أموالا وقام عمدا بتمويل وقد عرف المشرع الجزائري فعل التمويل بموجب قانون 15 / 06 المتعلق بالوقاية من تبييض الاموال وتمويل الارهاب 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 اجل ارتكاب الجرائم الموصوفة بأفعال ارهابية أو تخريبية المنصوص والمعاقب عليها بالمواد 87 مكرر الى 87 مكرر 10 من قانون العقوبات. [2]

اشترط المشرع الجزائري استخدام تكنولوجيا الاعلام والاتصال للحصول على التمويل عن طريق انشاء حسابات ومواقع الكترونية خاصة بالتنظيمات الارهابية والتي تتخذها كأداة لتوفير وجمع الاموال بصورة مباشرة عن طريق اختراق الحسابات البنكية أو تحديد الاشخاص عبر البريد الالكتروني واجبارهم على تحويل مبالغ الى حساباتهم الخاصة أو بصورة غير مباشرة كالادعاء بوجود نشاطات خيرية أو اجتماعية أو ثقافية أو عن طريق أنشطة غير مشروعة كجريمة تبييض الاموال والاتجار بالمخدرات والاسلحة وتزوير العملة أو اختطاف الرهائن وطلب فدية منهم أو السرقة واستغلالها لتمويل السفر اشخاص الى دولة اخرى بغرض ارتكاب اعمال ارهابية. [3]

---

[1] مهني رمزي، سبيعة محمود، مرجع سابق، ص28

[2] المادة 3 من القانون رقم 06.15 المؤرخ في 15 فيفري 2015 المعدل والمتمم لقانون رقم 05.01 المؤرخ في 6 فيفري 2005 والمتعلق بالوقاية من تبييض الاموال وتمويل الارهاب ومكافحتهما، المعدل والمتمم.

[3] مهني رمزي، مرجع سابق، ص 29

ثانيا: فعل التجنيد الوارد في نص المادة 87 مكرر 12 قانون العقوبات الجزائري.

تنص المادة 87 مكرر 12 من قانون العقوبات الجزائري على: كل من يستخدم تكنولوجيا الاعلام والاتصال لتجنيد الاشخاص لصالح ارهابيين أو جمعية أو تنظيم أو جماعة ومنظمة يكون غرضها ان تقع انشطتها تحت طائلة احكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة.

نص المشرع الجزائري في هذه المادة على فعل التجنيد من خلال مصطلح تجنيد الاشخاص ويقصد به استقطاب أعضاء جدد بغرض ادخالها في التنظيمات والجماعات الارهابية واستمراريتها فقد اصبح الاعلام الالكتروني المنظر المفضل للتنظيمات الارهابية لصيد أعضاء جدد وخاصة مع استخدام الفضاء السبيراني الذي يجعل التفاعل عابر للحدود الجغرافية، مما يسهل نقل المعلومات بين الاشخاص حول العالم.[1]

ومنه تسهيل عملية التجنيد وجذب أكبر عدد ممكن من الاشخاص، ويعتبر فئة الشباب المراهقين أكثر استهدافا في هذه العملية باعتبارهم الاكثر تواجدا في منصات التواصل الاجتماعي، كما أدركت التنظيمات الارهابية أهمية هذه المواقع واعتبرتها الاداة العلمية والتكنولوجية المهمة لنشر أفكارها وتنفيذ مشروعها الايديولوجي، سواء بصورة مباشرة عن طريق استعمال القوة واجبار مستخدمي الانترنت للانضمام اليها، أو بصورة غير مباشرة بأسلوب الترغيب والاغراء عن طريق التدعيم بالعواطف واستخدام عبارات حماسية عبر غرف الحوارات والدردشة. [2]

ثالثا: الشرط الخاص المشترك في الركن المادي لجريمة الارهاب الالكتروني:

لقد اشترط المشرع الجزائري من خلال نص المادتين 87 مكرر 11 و87 مكرر 12، انه في حالة وإذا تم ارتكاب هذه السلوكيات الاجرامية باستعمال الوسيلة المتماثلة

[1] مهني رمزي، مرجع سابق ص 30

[2] سامي علي حامد عياد ،استخدام تكنولوجيا المعلومات في مكافحة الارهاب، دار الفكر الجامعي، الاسكندرية، 2007.

في تكنولوجيا الاعلام والاتصال نكون اما جريمة الارهاب الالكتروني وإذا تم ارتكابها دون هذه الوسيلة نكون امام جريمة الارهاب التقليدي، فهذه الوسيلة تعتبر العنصر المشترك بين المادتين السالفتين الذكر كونها شرط جوهري ومهم لاعتبار جريمة الارهاب الالكتروني جريمة الكترونية. [1]

الفرع الثاني

النتيجة الاجرامية في جريمة الارهاب الالكتروني

تعد النتيجة العنصر الثاني للركن المادي للجريمة ، ويراد بها الاثر المترتب عن السلوك الاجرامي والمرتبط به برابطة سببية والذي يحدث في العالم الخارجي أو المادي، وبالرغم من ارتباط النتيجة بالسلوك الاجرامي فانهما قد ينفصلان احيانا عن بعضهما، بحيث يمكن تصور حصول السلوك دون تحقق النتيجة، وخير دليل على ذلك أن المشرع يعاقب على الشروع دون أن تتحقق النتيجة.

للنتيجة الاجرامية مفهومان احدهما مادي، والاخر قانوني:

- ويقصد بالمفهوم المادي للنتيجة الاجرامية التغيير والتعديل الذي يطرأ على العالم الخارجي كأثر للسلوك الاجرامي كالوفاة في جرائم القتل والاذى في جرائم الايذاء
- أما بالنسبة للمفهوم القانوني للنتيجة الاجرامية فيقصد به الاعتداء على المصلحة التي يحميها القانون، سواء أدى الاعتداء الى الاضرار بالمصلحة المحمية أو هددها بالخطر. [2]

جريمة الارهاب الالكتروني تأخذ حكم الجريمة المعلوماتية فهي بذلك تعد من الجرائم الشكلية الذي يفترض فيها الضرر مستقبلا والمتمثل في النتيجة الاجرامية، فبمجرد استخدام تكنولوجيا المعلومات والاتصال والقيام بالسلوكيات الواردة في نص المادتين 87

[1] مهني رمزي، نفس المرجع، ص 31

[2] موسى مسعود ارحومة، الاحكام العامة لقانون العقوبات الليبي، مرجع سابق، ص 288

مكرر 11 و87 مكرر 12 من قانون العقوبات الجزائري [1] من فعل السفر أو تمويل او تجنيد لأغراض ارهابية تقوم الجريمة حتى ولو لم تتحقق هذه الافعال كونا جريمة خطر وليست ضرر وذلك بالنظر الى الوسيلة المعتمدة عليها في تنفيذ السلوك الاجرامي. [2]

الفرع الثالث

العلاقة السببية لجريمة الارهاب الالكتروني

لا يوجد مجرم مقبل على ارتكاب أفعال اجرامية بدون أهداف، لذا فإن سلوك المجرم مرتبط دائما بأهداف أو نتائج يطمح أو يتوقع حدوثها عقب ارتكاب الجريمة، والعلاقة السببية هي الصلة التي تربط بين السلوك الاجرامي والنتيجة الضارة.[3]

تعرف العلاقة السببية على أنها العنصر الثالث والاخير من عناصر الركن المادي لجريمة الارهاب الالكتروني فهي الرابطة بين العنصرين السابقين، أي توافر السببية بين السلوك والنتيجة، وإذا انتفت العلاقة السببية فإن مسؤولية مرتكب الفعل تقتصر على الشروع إذا كانت الجريمة مقصودة فإذا كانت غير مقصودة فلا مسؤولية عنها، فالعلاقة السببية عنصر من عناصر الركن المادي وشرط أساسي لقيام المسؤولية الجزائية. [4]

ولا تثير علاقة السببية صعوبة في مدى توافرها واثباتها في جرائم الارهاب بصورتها التقليدية حيث أنها تأخذ صورة الجرائم المادية التي تستلزم تحقق نتيجة اجرامية ترتبط بالسلوك ويكون من السهل اثباتها، ولكن المشكلة تثور في جرائم الارهاب الالكتروني حيث انه يكون من الصعب اثبات علاقة السببية في الجرائم المرتكبة عبر

[1] المواد 87 مكرر 11 و87 مكرر 12، نفس المرجع السابق

[2] مهني رمزي، مرجع سابق، ص 31

[3] حسن المبروك سعد، جريمة الارهاب الالكتروني "دراسة مقارنة" ،رسالة مقدمة لنيل شهادة الماجستير، الاكاديمية الليبية، القسم الجنائي، 2023، ص 70

[4] عبود السراج ،شرح قانون العقوبات القسم العام ،الجزء الاول، منشورات جامعة دمشق، دمشق، 2007، ص 118.

الانترنت، فهي تعتمد على استخدام امكانات الحاسب الالي في ترويع واكراه الآخرين، فهو يتم عن بعد دون اللجوء الى العنف المادي والجسدي.[1]

إن جرائم الارهاب الالكتروني البعض منها يأخذ صور الجرائم المادية التي تستلزم تحقق نتيجة اجرامية ترتبط بالسلوك والبعض الاخر يأخذ صور الجرائم الشكلية التي يكفي فيها توافر السلوك دون وقوع النتيجة، وهنا تقدير السببية يكون بناء على تقدير احتمالي سابق على تحقيق النتيجة، فإذا كان تقييم السلوك يؤدي الى القول بإحداث النتيجة الضارة اكتمل الركن المادي للجريمة، لأنه بذلك يحقق الخطر المعاقب عليه والمتمثل في امكانية تحقيق النتيجة الضارة.[2]

المطلب الثالث

الركن المعنوي لجريمة الارهاب الالكتروني

لا تقوم الجريمة بمجرد تحقق الركن المادي، حيث يلزم لها ايضا بتوفر الركن المعنوي، ويعد الركن المعنوي الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويطلق عليه الركن الادبي او الركن الشخصي، فهذا الركن يتمثل في الاصول الارادية لماديات الجريمة والسيطرة عليها، فلا محل لمسائلة الشخص عن جريمة ما لم تقم صلة أو علاقة بين ماديات الجريمة وإرادتها.[3]

جريمة الارهاب الالكتروني جريمة عمدية تتطلب توافر القصد الجنائي العام بعنصريه العلم والارادة، فيجب ان يعلم الجاني ان سلوكه يعد سلوكا اجراميا يعاقب عليه القانون، ويجب ان تتجه ارادته نحو ارتكاب الفعل المكون للجريمة من اجل تحقيق النتيجة

---

[1] حسن المبروك سعد، نفس المرجع

[2] ياسر فيصل الامين امين، جرائم الارهاب عبر الوسائل الالكترونية "دراسة مقارنة"، مجلة مصدر المعاصرة، العدد 547، 2022، ص 539.

[3] علي حمودة، شرح الاحكام العامة لقانون العقوبات الاتحادي، النظرة العامة للجريمة، الجزء الاول، مطبعة الفجيرة الوطنية، الامارات ،2008، ص 431

الاجرامية في بعض صور جرائم الارهاب الالكتروني التي تتطلب تحقق هذه النتيجة.[1] وهذا ما نصت عليه المادة 87 مكرر 11 من قانون العقوبات الجزائري

وتعد جريمة الارهاب الالكتروني من الجرائم القصدية التي يتمثل فيها الركن المعنوي في صورة القصد الجنائي، فهي لا تقع بطريقة الخطأ إلا أن القصد الجنائي العام لا يكفي لقيام هذه الجريمة، بل لا بد من توافر القصد الجنائي الخاص المتمثل في ايجاد حالة من الذعر بين الناس أو الاخلال بالأمن العام أو الاضرار بالبنية التحتية، وهذا القصد الخاص الذي يميز العمل الارهابي عن غيره من الجرائم التي قد ترتكب بالأفعال والوسائل نفسها.[2]

الفرع الأول

القصد الجنائي العام

القصد الجنائي العام في جريمة الارهاب الالكتروني يعد من العناصر الاساسية لقيام الجريمة

ويتمثل في ارادة الجاني بالقيام وهو يعلم أن القانون ينهى عنه، ويتمثل القصد الجنائي العام في جريمة الارهاب الالكتروني في علم الجاني أو المجرم بارتكاب سلوك مجرّم قانونا والمتمثل في التجنيد والسفر والتمويل باستعمال تكنولوجيا الاعلام والاتصال مع اتجاه الإرادة الى استخدام هذه الوسيلة لتنفيذ الجريمة لأغراض ارهابية. [3]

[1] صدام العبيدي، مرجع سابق، ص 235

[2] حسن المبروك، مرجع سابق، ص 71

[3] احسن بو سقيعة، الوجيز القانون الجزائي العام، ط 7، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2008، ص 109.

الفرع الثاني

القصد الجنائي الخاص

والقصد العام لا يكفي وحده لقيام الجريمة، بل يتطلب الامر اقتران بالقصد الخاص، كأن يكون هدف الجاني من وراء أفعاله هو التأثير على قرارات الدولة وزعزعة استقرارها أو بث الرعب بين السكان أو عرقلة عمل المؤسسات العمومية. فإن القصد الخاص يتجاوز مجرد ارتكاب الفعل الغير مشروع، ليصل الى نية استعمال الوسائل الالكترونية كوسيلة لتنفيذ مشروع ارهابي، وهو ما يضفي على الفعل خطورته حقيقية.[1]

وقد أكد الفقه أن اثبات القصد الخاص في الجرائم الارهابية عموما، ومنها الالكترونية، يعد مسالة دقيقة ومعقدة لأنه يتعلق بالنوايا الداخلية للفاعل والتي غالبا ما تستكشف من الظروف الجريمة وطبيعة الوسائل المستعملة وطبيعة الاهداف التي استهدفتها العملية الالكترونية، مثل استهداف البنى التحتية الحيوية أو المؤسسات الامنية والسياسية للدولة.[2]

ومن الناحية التشريعية، فان المادة 87 مكرر من قانون العقوبات الجزائري، التي تعرف بالأفعال الارهابية، تضع ضمن شروطها قصد جنائي في " الاضرار بمؤسسات الدولة أو الامن العام "، مما يعني أن القصد الخاص عنصر لا غنى عنه لقيام الجريمة الارهابية، سواء ارتكبت بالوسائل التقليدية أو عبر الفضاء الالكتروني. ونص المشرع في نفس المادة على الافعال التي تعد إرهابا والمستهدفة لأمن الدولة واستقرارها وتتمثل في:

- عرقلة حركة المرور وحرية التنقل في الطريق والتجمهر والاعتصام في الساحات العمومية والاعتداء على رموز الامة والجمهورية ونبش أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.

---

[1] بن حدو عبد الكريم، الركن المعنوي في الجرائم الارهابية ،مجلة الدراسات القانونية والسياسية، العدد 12 ،2022، ص 73

[2] بو عافية ليلى، الجرائم المعلوماتية ذات الطابع الارهابي، مجلة السياسية الجنائية، العدد 6، 2021، ص 111

- بث الرعب في أوساط السكان وخلق جو انعدام الامن من خلال الاعتداء المعنوي أو الجسدي على الاشخاص وتعريف حياتهم أ، حريتهم أو أمنهم للخطر أو المساس بممتلكاتهم.
- الاعتداء على المحيط وإدخال مادة أو تسريبها في الجو أو باطن الارض أو إلقاءها عليها أو في المياه الاقليمية من شأنها جعل صحة الانسان أو الحيوان أو البيئة الطبيعية في خطر.
- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادات 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 الى أي وسيلة اخرى من وسائل النقل.
- اتلاف منشئات الملاحة الجوية أو البحرية أو البرية.
- تخريب أو اتلاف وسائل الاتصال.
- احتجاز الرهائن.
- الاعتداء باستعمال متفجرات أو مواد بيولوجية أو كيماوية أو نووية أو المشعة
- تمويل ارهابي او منظمة ارهابية [1]

[1] المادة 87 مكرر، مرجع سابق

المبحث الثاني

سبل مكافحة الارهاب الالكتروني

يعد الارهاب من اخطر الظواهر التي تواجه المجتمع الدولي في القرن الحادي والعشرين، حيث لم تعد آثاره محصورة في الجانب الامني فقط، بل اصبحت تمتد الى ابعاد سياسية، اقتصادية، اجتماعية وثقافية. وقد فرض هذا الواقع على الدول ضرورة تبني مقاربات شاملة ومتكاملة تهدف الى مكافحة هذه الافة بشكل فعال، خصوصا مع تطور أشكالها ووسائلها، واعتمادا على التكنولوجيا الحديثة لنشر أفكارها وتنفيذ عملياتها.[1]

كما تلعب التشريعات الوطنية دورا مهما في مكافحة الارهاب، من خلال سن قوانين صارمة تجرم الاعمال الارهابية وتحدد العقوبات المناسبة لها. [2]

المطلب الأول

الجهود الدولية والاقليمية في مكافحة جريمة الارهاب الالكتروني

لقد عانت الدول والمجتمعات من الاستخدام السلبي لتكنولوجيا الاتصال والانترنت من طرف الارهاب الالكتروني ،مما دفع الدول لفرض جملة من الاتفاقيات والتشريعات لمواجهة هذا الخطر والقضاء عليه.

[1] بوجمعة لطفي، الاجراءات الخاصة لمكافحة الجرائم الارهابية في التشريع الجزائري، مجلة العلوم الانسانية، جامعة باجي مختار، عدد خاص، 2018، ص 55

[2] تازير آمنة، جهود المنظمة القانونية الجزائرية في مكافحة جريمة الارهاب، مجلة الاستاذ الباحث، المجلد 4، ع 1، 2019، ص 63

الفرع الأول

مكافحة الارهاب الالكتروني في المنظمات الدولي

أولا: منظمة الامم المتحدة.

مع تزايد خطر الارهاب الدولي وظهور وانتشار نوع جديد من الجريمة المرتبطة بالحاسوب الالي بفعل تسارع وتيرة التطور التقني في أنظمة المعلومات والاتصالات وما أفرزه ذلك التهديد من أضرار ومخاطر على البلدان والافراد، ولا سيما بعد دخول الشبكة الدولية للمعلومات بوسائلها المتنوعة والمتطورة على خطر الارهاب الدولي ومواجهته تزايدت الحاجة الى تضافر الجهود الدولية وتعاضدها تحت مضلة المنظمات الدولية والاقليمية لمواجهة هذا التهديد، وكانت الامم المتحدة المحفل العالمي الاهم لترجمة هذه الجهود واستثمارها الامثل في مثل هذه المواجهة، لما تتمتع به هذه الاخيرة من مصداقية في مجال تعزيز التعاون الدولي لتحقيق مقاصدها في ضمان الامن والسلم الدوليين في مواجهة مختلف التهديدات بضمنها خطر الارهاب الالكتروني.[1]

أصدرت الامم المتحدة عبر جمعيتها العامة ومجلس الامة مجموعة من القرارات الدولية التي اعتمدت عليها بموجب الصلاحيات الواردة في الفصل السابع من ميثاق الامم المتحدة.[2] ففي 22نوفمبر من عام 2002 اتخذت قرار بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي، وفي ديسمبر من نفس السنة اتخذت قرار ارساء ثقافة عالمية لأمن الفضاء الالكتروني. [3] والذي اعتبر هذا القرار من بين اهم القرارات التي استهدفت العمل على حماية البنية التحتية

[1] محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005 ،ص253

[2] الدليل التشريعي لنظام القانون العالمي لمكافحة الارهاب، اعداد مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينا ،2008.

[3] ناصر العلي، الجهود الدولية في مكافحة الارهاب الالكتروني، مجلة الباحث للدراسات الاكاديمية، ع 01، 2021، ص 35.

للمعلومات، وحث الدول والمنظمات الدولية على تكثيف جهود التعاون لمواجهة الارهاب الالكتروني. [1]

الى جانب هذه القرارات أُدرجت استراتيجية شاملة لمكافحة الارهاب واعتمدتها الجمعية العامة سنة 2006، والتي نصت على ضرورة اتخاذ تدابير قانونية وتقنية للحد من استخدام الانترنت لأغراض ارهابية، مع التركيز على احترام حقوق الانسان أثناء مكافحة هذا التهديد[2]، وفي سبيل ذلك اعتمدت الدول الاعضاء في 8 سبتمبر 2006 هذ الاستراتيجية والتي هي بمثابة قرار وخطة عمل في نفس الوقت. وهذه هي المرة الأولى التي اتفقت فيها الدول الاعضاء جميعها على نهج استراتيجي موحد لمكافحة الارهاب بجميع اشكاله وأنواعه، وتنص هذه الاستراتيجية على اتخاذ خطوات عملية فرديا وجماعيا لمنعه ومكافحته، وتلك الخطوات العملية تشمل طائفة واسعة من التدابير التي تتراوح من تعزيز قدرة الدول على مكافحة التهديدات الارهابية الى تحسين تنسيق أنشطة منظومة الامم المتحدة في مكافحة الارهاب.[3]

ثانيا: الاتحاد الدولي للاتصالات.

يلعب الاتحاد الدولي للاتصالات دورا محوريا في تعزيز الأمن السبيراني العالمي، من خلال وضع أطر تنظيمية ومبادرات تهدف الى الحد من استغلال الفضاء الرقمي في أعمال ارهابية. وقد أطلق الاتحاد في سنة 2007 الاجندة العالمية للأمن السبيراني كإطار عمل استراتيجي يرتكز على خمسة محاور أساسية: التدابير القانونية، التقنية،

---

[1] شفيق نوران أثر، التهديدات الالكترونية على العلاقات الدولية، طبعة 1، المكتب العربي للمعارف، القاهرة، مصر، 2015، ص108.

[2] الامم المتحدة، الاستراتيجية العالمية لمكافحة الارهاب، الجمعية العامة للأمم المتحدة ،2006، متاح على الرابط: https://www.un.org/counterterrorism/ar/un-global-counter-terrorism-strategy تاريخ الزيارة: 19/ 05/2025 على الساعة 11:06 مساءا

[3] حسن المبروك سعد، مرجع سابق، ص 89.

التنظيمية، بناء القدرات، والتعاون الدولي، وكلها موجهة لمواجهة التهديدات السبيرانية بما فيها الارهاب الالكتروني. [1]

كما وضع الاتحاد الدولي للاتصالات مخططا لتعزيز الأمن السبيراني العالمي، يتكون من سبعة أهداف رئيسية، وهي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا، بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.
- وضع استراتيجيات لتهيئة الارضية الوطنية والاقليمية المناسبة لوضع الهيكليات التنظيمية والسياسية المتعلقة بجرائم الانترنت.
- وضع استراتيجية لتحديد الحد الادنى المقبول عالميا في موضوع معايير الامن ونظم تطبيقات البرامج والأنظمة.
- وضع استراتيجيات لوضع آلية عملية للمراقبة والانذار والرد المبكر، مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.
- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي المجالات المعلوماتية
- تقديم مشورة بشأن امكانية اعتماد اطار استراتيجي عالمي لأصحاب المصلحة، من أجل التعاون الدولي والحوار والتنسيق في جميع المجالات التي سبق ذكرها. [2]

[1] الاتحاد الدولي للاتصالات، الاجندة العالمية للامن السبيراني، جنيف، 2007، ص 5

[2] تقرير الاتحاد الدولي للاتصالات في مجال تكنولوجيا المعلومات والاتصالات عن حالة التعاون بين البلدان النامية، المتاحة على الرابط: HTTPS://WWW.G77.ORJ/SSHLCST/ITU_ARABIC . تاريخ الزيارة 20/05/2025 على الساعة: 20:56

ثالثا: المنظمة العالمية للملكية الفكرية:

تأسست المنظمة العالمية للملكية الفكرية بموجب اتفاقية استكهولم في 14 يوليو 1967م، تحت عنوان اتفاقية "إنشاء المنظمة العالمية للملكية الفكرية"، وكان لها دور كبير في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها (المصنفات الادبية والفنية والعلمية والاختراعات)، ومع تزايد الحاجة العالمية لحماية البرامج، شكلت هذه المنظمة مجموعة من الخبراء بهدف حماية برامج الحاسب الالي.[1]

وتلعب المنظمة العالمية للملكية الفكرية دورا مهما في مكافحة الارهاب الالكتروني، من خلال حماية حقوق الملكية الفكرية في الفضاء الرقمي وتعزيز التشريعات ذات الصلة والتعاون الدولي. وتتمثل إحدى أهم مبادرات هذه المنظمة في اعتمادها لاتفاقيتي الانترنت سنة 1996 م أحدهما بشأن حق المؤلف والاخرى بشأن التسجيل الصوتي، حيث تهدفان الى تعزيز حماية المصنفات الرقمية وحقوق المؤلفين ما يقلل من احتمالات استغلالها في أنشطة ارهابية كالدعاية والتحريض عبر الانترنت. [2]

اضافة الى ذلك، تساهم المنظمة العالمية للملكية الفكرية في دعم التعاون الدولي من خلال التنسيق مع المنظمات كالإنتربول، وتبادل المعلومات حول الجرائم المتربطة بالملكية الفكرية التي قد تكون لها صلة بالإرهاب الالكتروني، ما يسمح بوضع استراتيجيات مشتركة للوقاية والمواجهة.[3]

رابعا: الولايات المتحدة الامريكية:

تلعب الولايات المتحدة الامريكية دورا محوريا ومتقدما في مواجهة الارهاب الالكتروني، باعتباره من أخطر التهديدات المعاصرة التي تواجه الامن القومي والمجتمع الدولي عموما، فقد تصاعدت وتيرة الاعتماد على التكنولوجيا والفضاء السيبراني من قبل

---

[1] حسن مبروك سعد، مرجع سابق، ص 90

[2] احمد بن محمد بن عبد الله، الملكية الفكرية في البيئة الرقمية ودورها في مكافحة الجرائم الالكترونية، مجلة العلوم القانونية، جامعة محمد الخامس، ع 12، 2020 ،ص88

[3] المنظمة العالمية للملكية الفكرية، تقرير التعاون الدولي لمكافحة الجرائم المرتبطة بالملكية الفكرية، متاح على الموقع الرسمي: HTTPS://WWW.WIPO.INT تم الاطلاع عليه في 20/05/2025 على الساعة: 22:33

الجماعات الارهابية سواء في التجنيد أو نشر الدعاية أو حتى في التنسيق والتخطيط لهجمات فعلية. مما دفع الولايات المتحدة الى وضع استراتيجيات شاملة للأمن السبيراني تركز على الوقاية والاستجابة الفعالة لأي تهديدات محتملة.[1]

فاعتمدت السلطات الامريكية على مجموعة من الوكالات المتخصصة، ابرزها وكالة الامن القومي ووزارة الامن الداخلي وكذلك القيادة السيبرانية الامريكية التي تتولى تنفيذ عمليات هجومية ودفاعية في الفضاء الالكتروني سواء داخل الولايات المتحدة أو خارجها.[2]

على الصعيد الدولي، سعت الولايات المتحدة الى ارساء تعاون أمني الكتروني واسع يشمل الدول الحليفة خاصة أعضاء حلف الناتو، فضلا عن التعاون مع شركات التكنولوجيا الكبرى مثل شركة مايكروسوفت، أمازون، وغوغل التي تعتبر طرفا اساسي في مراقبة الفضاء الرقمي ومنع استغلاله من طرف الجماعات الارهابية.[3]

كما اتخذت الولايات الامريكية عدة خطوات لمكافحة الجريمة والارهاب الالكتروني منها:

- إصدار قانون تعزيز أمن المعلومات.
- وضع الاستراتيجية الوطنية لتأمين الفضاء الالكتروني.
- إنشاء لجنة مكافحة الارهاب الالكتروني من قبل وزارة العدل الامريكية.
- إنشاء لجنة حماية البنية التحتية الحساسة في الولايات المتحدة والتي أسست مجموعة خاصة تتناول جوانب الارهاب الالكتروني وأطلقت عليا اسم: مرك حرب المعلومات.

---

[1] المركز المصري للفكر والدراسات الاستراتيجية، استراتيجية امريكية هجومية ضد التهديدات السيبرانية ،القاهرة، 2018 ،ص3.

[2] معهد واشنطن لسياسات الشرق الادنى، التعامل مع المشهد الديناميكي للتهديدات الداخلية في الولايات المتحدة ،ترجمة وحدة الدراسات الامنية، واشنطن، 2021، ص5.

[3] معهد واشنطن لسياسات الشرق الادنى، التعاون في الامن السيبراني:تجربة الولايات المتحدة، 2022، ص20 الى23

- إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات والبرامج.[1]

الفرع الثاني

مكافحة الارهاب الالكتروني في المنظمات الاقليمية

أولا: دور الاتحاد الاوروبي في مكافحة الارهاب الالكتروني.

يولي الاتحاد الاوروبي اهتماما بالغا لمكافحة الارهاب الالكتروني نظرا لتزايد التهديدات السيبرانية التي تستهدف أمن دول الاعضاء ومواطنيها، وقد تبنى الاتحاد سياسات واستراتيجيات شاملة لتعزيز قدراته في هذا المجال من خلال تطوير الاطر القانونية وتعزيز التعاون بين الدول الاعضاء وتكثيف الشراكات مع الجهات الدولية، ومن أبرز الهيئات التي أنشأها الاتحاد الاوروبي لمواجهة التهديدات الالكترونية هي وكالة الاتحاد الاوروبي للتعاون في مجال إنفاذ القانون ومركز الاستخبارات الاوروبي، اللذان يعملان على تنسيق الجهود الاستخبارية وتبادل المعلومات بين الدول الاعضاء.[2]

وعلى الصعيد الدولي، يعمل الاتحاد الاوروبي على تعزيز التعاون مع شركائه، مثل مجلس التعاون لدول الخليج العربية من خلال برامج عمل مشتركة تهدف الى مكافحة الارهاب والامن السيبراني، وقد تم الاتفاق على تنفيذ برنامج العمل المشترك (2022-2027) بين الاتحاد الاوروبي ومجلس التعاون.[3] كما يشارك الاتحاد الاوروبي في تعزيز

[1] صباح كزيز، أمال كزيز، الارهاب الالكتروني وانعكاساته على الامن الاجتماعي، مجلة التراث، رقم 1، ع 08، 2008، ص 03.

[2] المركز الاوروبي لدراسة مكافحة الارهاب والاستخبارات، مكافحة الارهاب داخل الاتحاد الاوروبي وكيفية التعاون الامني، ألمانيا، 2023، ص 5 ;7

[3] الامانة العامة لمجلس التعاون لدول الخليج العربية، البيان الرئاسي المشترك لاجتماع الدورة السابعة وعشرون للمجلس الوزاري المشترك بين مجلس التعاون والاتحاد الاوروبي، الرياض، 2023، ص 3 و4.

الأمن السيبراني من خلال التعاون مع منظمة الانتربول حيث يعملان معا على تبادل المعلومات والخبرات في مجال الامن ومكافحة الجريمة والارهاب.[1]

ثانيا: دور الجامعة العربية في مكافحة الارهاب الالكتروني.

تلعب جامعة الدول العربية دورا متناميا في مكافحة الارهاب الالكتروني وذلك نظرا لتزايد التهديدات الرقمية وتأثيرها على الامن القومي العربي، وقد تجسدت هذه الجهود في تبني استراتيجيات قانونية وأمنية وتعزيز التعاون بين الدول الاعضاء وتطوير القدرات المؤسساتية والبشرية في هذا المجال. فقد أطلقت الجامعة العربية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في 21 ديسمبر 2010، بهدف تعزيز التعاون بين الدول العربية في مواجهة الجرائم الالكترونية بما في ذلك الارهاب الالكتروني، من خلال وضع إطار قانوني مشترك لتجريم هذه الافعال وتبادل المعلومات والخبرات بين الاجهزة المعنية في الدول الاعضاء.[3]

كما أصدرت الجامعة العربية توصيات بإنشاء مراكز وطنية للأمن السيبراني في الدول الاعضاء، وتطوير استراتيجيات وطنية لمكافحة الارهاب الالكتروني وتحديث التشريعات الوطنية لتتوافق مع الاتفاقيات الدولية والاقليمية ذات الصلة.[2]

ثالثا: دور المشرع الجزائري في مكافحة الارهاب الالكتروني.

لطالما كان موقف الجزائر تجاه مسألة الارهاب واضحا منذ البداية، حيث تمثل موقفها في مثل هذه القضية في مجموعة القرارات والمواقف الدولية والمحلية تجاه هذه المسألة الخطيرة التي تهدد أمن المجتمع والدولة على حد سواء، وتعتبر الجزائر من الدول التي عانت بشكل خاص من مشكلة الارهاب مع بداية التسعينات أين عرفت أزمة أمنية

[1] منظمة الشرطة الجنائية، الانتربول والاتحاد الاوروبي: تعزيز التعاون في مجالات الامن ومكافحة الجريمة والارهاب، ليون، 2023، ص 2 و3.

[2] جامعة الدول العربية، توصيات المؤتمر العربي حول الامن السيبراني ومكافحة الارهاب الالكتروني، بيروت، 2022 ،ص6.

حادة تخللتها فترة تعد طويلة من الارهاب، وهو الأمر الذي سمح لها باكتساب خبرة التعامل مع هذه المسألة الخطيرة.[1]

لم تعرف الجزائر قبل سنة 2004 قوانين تطبق على تكنولوجيا الاعلام والاتصال، لكن تزايد الجريمة الالكترونية أَجبر المشرع الجزائري على وضع إطار قانوني مناسب يمنع الاعتداء على هذه النظم أو الاستعمال المسيء لها لسد الفراغ القانوني.[2]

ولتأمين الفضاء المعلوماتي لكل الناشطين فيه سواء كانوا أفراد أو مؤسسات عمومية، ركزت منظومة الدفاع الوطني على النص القانوني من خلال إصدار القانون 04 /15 المتضمن تعديل قانون العقوبات تماشيا مع التطور التكنولوجي والذي نص على حماية جزئية نسبية لأنظمة المعلومات. [3] حيث خصص القسم السابع مكرر بأحكام المساس بأنظمة المعالجة الآلية للمعطيات وقد تضمن ثمانية مواد ركزت في مجملها على معاقبة المتورطين في عمليات المساس بأنظمة المعالجة الآلية للمعلومات كما جاء في المادة 394 مكرر 1، فنصت على كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، ونصت المادة 394 مكرر 2 على معاقبة كل من يقوم عمدا عن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في المعطيات المخزنة أو معالجة أو المراسلة عن طريق المنظومة المعلوماتية يمكن أن ترتكب بما الجرائم المنصوص عليها في القسم الأول
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم

[1] كواشي عتيقة، تداعيات الارهاب السيبراني على الامن القومي الجزائري، المجلة الجزائرية للأمن والتنمية، جامعة باتنة 1 ،المجلد 12، ع 03، 2023، ص 211

[2] بوزنون سعيدة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الانسانية، ع 47، 2019، ص 49.

[3] بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، 2017، ص246.

أما المادة 394 مكرر 3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم إذ استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد، وفي المادة 394 مكرر 4 شددت المشرع الجزائري على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة مالية تعادل خمسة مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي.[1]

وفي اطار الوقاية من الجريمة الالكترونية والارهاب السيبراني باشر المشرع الجزائري اجراءات جديدة للمواجهة تضمنت اصدار قانون 09 / 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها في المادة 4 على أنه: " يمكن القيام بعلميات المراقبة المنصوص عليها في المادة الثالثة منه:

"... للوقاية من الأفعال الموصوفة بجرائم الارهاب **والتخريب أو الجرائم الماسة بأمن الدولة في حالة توافر معلومات عن حالة اعتداء على منظومة معلوماتية**".[2]

كما أنشأت السلطات الجزائرية الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال بموجب المرسوم الرئاسي رقم 15–261 المؤرخ في 8 اكتوبر 2015، حيث حدد هذا المرسوم تشكيلة وتنظيم وكيفيات سير هذه الهيئة[3].

اذا تعد الهيئة سلطة ادارية ومستقلة لدى وزير العدل وتضم أعضاء من الحكومة ومسؤولي مصالح الامن والقضاة من المحكمة العليا يعينهم المجلس الاعلى للقضاء.[4]

كما وضعت الجزائر فرقا أمنية تقنية متخصصة في الجريمة الالكترونية مهمتها مراقبة الانشطة المشبوهة على مدار الساعة والتعامل بفعالية مع البلاغات التي تصلها

---

[1] قانون رقم 156/66 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، المادة 394 مكرر 1 الى4، الجريدة الرسمية الجزائرية.

[2] المواد من 02. 03. 04، من القانون رقم 09 – 04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

[3] المرسوم الرئاسي رقم 15 – 261 المؤرخ في 8اكتوبر 2015، المحدد لمهمة الوكالة الوطنية للامن المعلوماتي وتنظيمها وسيرها، الجريدة الرسمية، ع 55، سنة 2015

[4] بوزنون، نفس المرجع، ص 53

بشكل سمح بإفشال نشاط عشرات الخلايا الارهابية في ضرف قياسي. [1] اذ قررت القيادة العليا للأمن الوطني استحداث مخابر وخلايا مختصة في مكافحة الجريمة الالكترونية، فقد تدعمت المديرية العامة للأمن الوطني سنة 2010 بما يقارب 23 خلية لمكافحة الجريمة الالكترونية بكل أنواعها. [2] حيث يعتبر الهدف الاساسي من اطلاق هذه الخلايا الامنية المتخصصة هو العمل على تعزيز اجراءات الرقابة لحماية المواطن الجزائري وخاصة عنصر الشباب من هذه الجرائم التي أصبحت تهدد استقرار البلاد. [3]

المطلب الثاني

آليات القضاء على الارهاب الالكتروني

مع تحالف الجهود الدولية والاقليمية لإبرام اتفاقيات ومعاهدات فيما بينهم للقضاء على جريمة الارهاب الالكتروني توصلوا لآليات مكافحتها والقضاء على تهديداتها، وهذا ما خصصناه في مطلبنا من خلال دراسته من عدة جوانب:

الفرع الأول

مكافحة الارهاب قانونيا

سنت العديد من دول العالم قوانين مكافحة الجرائم الالكترونية بعد أن جليا مدى سرعة انتشارها وقداحة الخسائر الناتجة عنها وأجمع أغلب هذه القوانين أن هذه الجرائم ماهي إلا تعدي على الاخرين وعلى الممتلكات العامة والانظمة بواسطة استخدام

---

[1] الارهاب الالكتروني يهدد الجزائر، جريدة البلاد، 13 ماي 2017 متاحة على الرابط:
https://www.elbilad.net/article/detail?id=70386، تاريخ الاطلاع: 2025 / 05 / 23، على الساعة: 10 :57

[2] حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، ملتقى وطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، 2015، ص 8.

[3] كواشي عتيقة، مرجع سابق، ص 211

الوسائل التقنية وخصص جزءا كبيرا من هذه القوانين لعقوبات رادعة لجرائم الارهاب الالكتروني الذي يمتد أثره ليس على دولة معينة بحد ذاتها بل يمتد ليشمل المجتمع الدولي بأسره وفيما يلي بيان أسماء بعض الدول العالم التي سنت القوانين لمكافحة هذه الجريمة.[1]

السويد، الولايات المتحدة، استراليا، كندا، الصين، مقاطعة هونج كونج التابعة للصين، مملكة الدنمارك، فرنسا، المانيا، جهورية ايرلندا، الهند، اليابان، وغيرها العديد من دول العالم التي أضافت لقانونها الجزائي ملحقا خاص لمكافحة الجرائم الالكترونية ومنها لبنان، البحرين، الجزائر، المغرب، تونس، الاردن، مصر، السودان وغيرها. وهناك ثلاث دول عربية فقط هي السعودية والامارات وعمان التي سنت قوانين مستقلة لمكافحة الجرائم المعلوماتية. [1]

ولقد سعت معظم هذه الدول الى مكافحة ومواجهة الارهاب الالكتروني بشتى الطرق حيث:[2]

- قام الانتربول بأعضائه 178 بعمل جبار لمحاربة جرائم الارهاب الالكتروني خاصة والجرائم الالكترونية عامة، وتقييم عديد من الدورات لأعضائه وكذلك العديد من مجالات التدريب.
- مجلس أوروبا في إطار سعيه لمواجهة الجرائم الالكترونية سن القانون الاسترشادي لمكافحة جرائم الحاسب الآلي، وهو إطار يجمع 45 دولة ولم يقتصر على الدول الاوروبية بل شمل أمريكا وكندا واليابان وعدد من الدول الافريقية وأمريكا الجنوبية.
- منظمة جنوب شرق آسيا وضعت خطوط عريضة لتبادل المعلومات والخبرات بخصوص مواجهة الجرائم الالكترونية عامة وجرائم الارهاب الالكتروني خاصة، بل وقعت على إنشاء وحدة إقليمية لهذه الدول لمكافحة الجرائم الالكترونية.

[1] حسن بن أحمد الشهري، الارهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، ع 8، 2015، ص 20

[2] المرجع نفسه، ص 20

- موافقة الجامعة العربية على اعتماد قانون دولة الامارات العربية المتحدة كقانون استرشادي لقانون مشابه للقانون الاسترشادي لدول أوروبا لمكافحة جرائم الارهاب الالكتروني.[1]
- جامعة نايف العربية للعلوم الامنية انطلاقا من تخصص الجامعة كجامعة تهتم بالامن الشامل والتخصص كذلك بتنفيذ الجانب العلمي من الخطط والاستراتيجيات الامنية العربية لمكافحة الارهاب، التي أقرت من وزراء الداخلية في الدول العربية وتم الانتهاء من تنفيذ الخطة المرحلية الرابعة الاستراتيجية في عام 2009، وتنفذ الجامعة العديد من المناشط العلمية المعتمدة ضمن الخطط ، كما نفذ تعدد أمن الدورات التدريبية والندوات العلمية والمحاضرات العلمية والدراسات والابحاث الميدانية، وتمكنت من الاستفادة من الخبرات الدولية حيث نضمت العديد من الانشطة العلمية في مجال مكافحة الارهاب في كل من فرنسا وألمانيا واسبانيا والنمسا وايطاليا وهولندا والتشيك والصين كما ضمت مناهجها العلمية العديد من المقررات الدراسية التي تنأولت مشاكل وانواع الارهاب وطرق مواجهته.[2]

الفرع الثاني

مكافحة الارهاب فنيا

الارهاب الالكتروني يعتبر تحديا أمنيا تعمل الدول على مواجهته والحد منه وذلك عن طريق استخدام مجموعة من الاجراءات الفنية التقنية والتدابير الاحترازية الوقائية التي يمكن لها أن تقلل بشكل كبير من مخاطر هذا الارهاب وذلك من خلال[3]:

[1] حسن بن احمد الشهري، مرجع سابق، ص 20

[2] حسن بن أحمد الشهري، مرجع سابق، ص 20

[3] شاوشة ياسمينة، الارهاب الالكتروني بين مخاطره وآليات مكافحته، مذكرة تخرج لنيل شهادة الماستر في الحقوق، جامعة أكلي محمد أولحاج، بسكرة، 2019، ص 102

أولا. التدريب والتوعية.

تتطلب مكافحة الارهاب الالكتروني في الفضاء الالكتروني مواجهته من خلال تدريب المسؤولين عن مكافحة الارهاب على استيعاب السياسات الامنية الالكترونية، والتركيز على دحض أفكار الارهابيين وعزلهم عن المجتمع، مع بث أفكار مضادة لما يروجون له من خلال إنشاء مواقع التوعية العديدة وعد ترك الساحة الاعلامية ساحة حرة لهم.[1]

فلا بد أن يكون رجال القضاة والنيابة العامة على درجة كبيرة من الالمام بالحوسبة الرقمية والكفاءة والمعرفة والقدرة على متابعة الجرائم الالكترونية والارهاب الالكتروني واستخلاص الادلة منها، وهذا لا يتم إلا بالتدريب الذي يشمل جوانب الجرائم الالكترونية كلها.[2]
كما أن للجماعات الارهابية مواقع متعددة على شبكة الانترنت التي تبث من خلالها كل أفكارها السامة وتعمل على استقطاب أكبر عدد ممكن من الشباب وبالتالي لا بد من عدم ترك الساحة الاعلامية حرة لهم كما قلنا سابقا، من خلال إيجاد البديل القوي والمنافس في الشبكة المعلوماتية، والبدء بإنشاء مواقع ومنتديات تخدم المجتمع وتنير أفكار الشباب وتحارب الجماعات الارهابية وتكشف ما يروجون له من كذب وأفكار هدامة، ونشر الوعي التكنولوجي بكيفية التعامل مع الانترنت والحاسوب.[3]

ثانيا: تفعيل المراقبة الالكترونية

لا بد من الدول فرض رقابة على كل ما يقدم على شبكة الانترنت لمنع الدخول للمواقع التي يتضمن محتواها مواد تتعلق بالإرهاب، فضلا عن مراقبة الاتصالات عبر شبكة الانترنت والبريد الالكتروني بهدف ضبط المجرمين وتفتيشهم وجمع الأدلة لإدانتهم

---

[1] نور الله تله، الارهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي، كلية الحقوق، جامعة دمشق، 2015 -2016، ص164

[2] فراس طحان، الارهاب الالكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، ع2، 2011، ص 379.

[3] شاوشة ياسمينة، مرجع سابق، ص 104

وتقديمها للمحاكمة. ويجب أ، تكون هذه المراقبة مشروعة وتحقق التوازن بين حق الافراد في الخصوصية وحق المجتمع في مكافحة الجريمة.[1]

ولا تعني الرقابة المنع من استخدام شبكة الانترنت لكنها عبارة عن تدبير وقائي لمنع وقوع الجريمة، من خلال التحكم في النشر والوصول الى المعلومات عبر الانترنت، وتستخدم الرقابة تقنية تعتمد على الجدار الناري أو البروكسي ويتم ذلك عن طريق إجبار المتعاملين مع الشبكة على المرور عبر خوادم البروكسي قبل الوصول الى الشبكة.[2]

ويوجد برامج عدة للمراقبة الالكترونية وبرامج متخصصة لجمع الادلة والقرائن من رسائل البريد الالكتروني، فعلى سبيل المثال توظف الصين مليوني شخص لمراقبة الانشطة على شبكة الانترنت، حيث تعد شبكة الانترنت هناك من أكثر الشبكات التي تشهد سيطرة ورقابة حكومية صارمة في العالم وتكون المواقع الالكترونية تحت الرقابة الجبرية الدائمة، بل وصل الامر الى حد التدخل لحذف التعليقات ذات الحساسية بصورة روتينية على مواقع التواصل الاجتماعي. [3]

ثالثا: تفعيل أنظمة الحجب

قد جاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم، ويعني ذلك حجب المواقع الضارة التي تدعو الى الفساد، ومنها المواقع التي تعلم وتحث على الارهاب والعدوان والاعتداء على الاخرين بغير حق، والقيام بالإجراءات كلها بما في ذلك تشريح المحتوى.[4]

---

[1] نفس المرجع، ص 105

[2] نفس المرجع، ص 106

[3] نور الله تله، مرجع سابق، ص 168

[4] عبد الرحمن بن عبد الله سند، وسائل الارهاب الالكتروني وحكمها في الاسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الاسلام من الارهاب، الجزء الاول، الرياض، 2004، ص 23

رابعا: أنظمة الحماية الفنية من الاعتداءات الالكترونية.

تتم الحماية الفنية من الاعتداءات الالكترونية سواء كانت ارهابية أو غيرها، بوسائل فنية عدة منها: [1]

- تشفير البيانات المهمة المنقولة عبر الانترنت، سواء كانت منقولة عبر وسائل الاتصالات أو عبر الالياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها الى وضعها السابق عند وصولها للطرف المستقبل، ويتم اللجوء الى تشفير البيانات والمعلومات اذا كانت مهمة، لان عملية التشفير مكلفة.
- ايجاد نظام أمني متكامل ليقوم بحماية البيانات والمعلومات.
- توفير برامج الكشف عن الفيروسات لحماية الحاسب الالي والبيانات والمعلومات من الضرر بها.
- عدم استخدام شبكات الحاسب الالي المفتوحة لتداول المعلومات الامنية.
- عمل نسخ احتياطية من بيانات تخزن خارج مبنى المنظمة.
- استخدام وسائل حديثة تضمن دخول أشخاص مصرح لهم فقط الى أقسام مركز الحاسب الالي، كاستخدام أجهزة التعرف على بصمة العين أو اليد أو الصوت.
- استخدام كلمة المرور، حيث تعد كلمة المرور من أبسط أشكال الحماية ويفضل اختيار كلمة مرور ذات بنية قوية، ويجب مراعاة تغييرها الدوري.

الفرع الثالث

مكافحة الارهاب فكريا

اذا كانت مشكلات التنظيمات الارهابية والجرائم الالكترونية مشكلات فكرية فيجب أن تعتمد الاجراءات المحلية والاقليمية والدولية على وسائل الفكرية والفنية

[1] نفس المرجع، ص 29

والقانونية في مواجهة هذه المشكلات وأن تقتصر الاجراءات الامنية على الخارجين على القانون فقط لأن الاعتماد على الاجراءات الامنية وحدها الى نتائج عكسية فعندها انطلقت الطائرات الامريكية لضرب أفغانستان انطلقت معها حركة تنظيم القاعدة على الانترنت والمنظمات الاخرى الحليفة لها. واكتملت تلك الحلقة باحتلال العراق وليكتسب تنظيم قاعدة أرضا جديدة لبث أفكاره التنظيمية المعادية للولايات المتحدة وللغرب بوجه عام، من هنا فقد زادت المواقع الارهابية تنظيم القاعدة على الانترنت من 13 موقع عام 2001م لتصل الى ما يقارب 2000 موقع في عام 2006م وفق بعض التقديرات. السبيل الامثل لمواجهة هذه الظاهرة يمكن في:

- للاستخدام الامثل لوسائل الاعلام من خلال نشر أفكار المعتدلة وتجنب نشر أعمال العنف أو أفكار متطرفة.
- كشف مواقع المتطرفين ومناقشة أفكاره وبيان ما تشتمل عليه من مخلفات.
- التوسع في إنشاء المواقع البديلة لنشر الوسطية والاعتدال ومحاربة الافكار المتطرفة.
- تشكيل لجان وطنية لحماية الشباب وتحصينهم من الافكار المتطرفة.
- إعداد وتنفيذ برامج إعادة تأهيل المتطرفين فكريا وعلميا.
- اتخاذ الاجراءات الفنية المناسبة لحماية المواقع المعتدلة واختراق المواقع المتطرفة وتغذيتها بالأفكار المعتدلة.
- وضع معايير دولية لأمن المعالجة الالية للبيانات.
- التدابير الملائمة لحل المشكلات للاختصاص القضائي التي تثيرها جرائم معلوماتية العابرة للحدود أو ذات الطبيعة الدولية.

- الاتفاقية الدولية تنطوي على نصوص وتنظيم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الانظمة المعلوماتية المتصلة فيما بينها والاشكال الاخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه للحقوق الدولي. [1]

الفرع الرابع

مكافحة الارهاب عسكريا

تتم المواجهة العسكرية للإرهاب الالكتروني:

أولا: بتقوية ودعم أجهزة جمع المعلومات والاستخبارات:

تستطيع الدولة للمحافظة على أمن مواطنيها بتسخير الاموال لتقوية أجهزة جمع المعلومات عن الارهابيين والجماعات الارهابية ليس هذا فحسب فلا بد من تجنيد عناصر ذو الخبرة في مجال أنظمة المعلومات وإنشاء المواقع الالكترونية وبرمجة الحاسب الالي وغيرها من التقنيات المختلفة.

ثانيا: الردع واستخدام القوة:

هو خيار صعب تقوم به الدول ضد قواعد إرهابية، باغتيال قياداتهم وتصفيتهم والتضييق عليهم، وتجفيف منابع مصادرهم البشرية والمالية. إن اللجوء لهذا الخيار يكون عندما ينشر ويتوسع الارهاب الالكتروني بشكل كبير، ومرتكبو هذا النوع من الارهاب يصعب جدا الوصول اليه بسبب استعمالهم لأسماء مستعارة وصعوبة تحديد أماكنهم.[2]

[1] حسن بن احمد الشهري، مرجع سابق، ص 20

[2] نفس المرجع، ص 19 و20

خلاصة الفصل

بعد أن أصبح الارهاب الالكتروني هاجس يخيف العالم وأصبح الافراد فيه عرضة لمختلف هجمات ونشاطات الارهابيون عبر الانترنت، ومع تفاقم هده المخاطر بمرور الايام، ولان التقنية الحديثة هي التي تقوم بحماية الناس من الارهاب الالكتروني مما دفع الدول لسن التشريعات والاتفاقيات وانشاء منظمات دولية واقليمية التي من شأنها مكافحة الارهاب الالكتروني وتطوير وسائل للتصدي لتهديدات جريمة الارهاب الالكتروني.

الخاتمة

الخاتمـــة:

وفي ختام دراستنا نستخلص أن جريمة الارهاب الالكتروني من أخطر وأعنف الجرائم المعلوماتية الموجودة حاليا في العصر الرقمي، ويعود ذلك لتعدد أساليب تنفيذ جريمة الارهاب الالكتروني وتطور أدواتها وانتشار تنظيماتها والاهم من ذلك سهولة ارتكابها وصعوبة في إثبات دليل عليها لسهولة إتلافه ومحوه ، وهو الامر الذي دفع المجتمع الدولي لمكافحته والتصدي له بالعمل مع الافراد والمؤسسات التي تساهم في تطور آليات ووسائل الحماية على المستوى الدولي والاقليمي والوطني ، وعليه سجلنا مجموعة من النتائج والتوصيات من دراستنا ، منها ما يلي :

أولا: النتائج.

- لم يكن هناك تعريف محدد لجريمة الارهاب الالكتروني ، وذلك راجع لنظرة كل دولة له.
- أن جريمة الارهاب الالكتروني جريمة متعدية الحدود.
- صعوبة الإثبات في جريمة الارهاب الالكتروني ، نظرا لسهولة إتلاف الدليل وحذفه.
- الاثر النفسي الذي يحدثه الارهاب الالكتروني ، فهو يهاجم المعتقدات والافكار والثقافات التي هي أساس المجتمعات.
- تنوع أهداف ودوافع ممارسة الارهاب الالكتروني ، ولكن الهدف الرئيسي منه كسب المال السهل.
- التعاون الدولي والاقليمي لمكافحة جريمة الارهاب الالكتروني عن طريق إبرام المعاهدات والاتفاقيات.

ثانيا: المقترحات.

وفي هذا السياق يمكننا وضع مجموعة من التوصيات لمواجهة الارهاب الالكتروني فنذكر منها:

- تثقيف الافراد والمجتمعات بمسألة الارهاب الالكتروني عن طريق تعزيز التربية الرقمية في المدارس والجامعات.
- تطوير البنى التحتية الرقمية للحكومات والمؤسسات الحيوية.
- تجريم الارهاب الالكتروني في التشريعات الوطنية والقوانين الدولية والاقليمية.
- تعزيز التعاون الدولي لتبادل المعلومات والخبرات بشأن الارهاب الالكتروني ، اضافة الى ابرام المعاهدات والاتفاقيات حول تسليم المجرمين في مختلف الدول.
- تفعيل دور المنظمات الدولية مثل الانتربول ومجلس الامن في التصدي للتهديدات السبيرانية.
- انشاء وحدات مختصة لمراقبة النشاطات الارهابية على الانترنت والشبكة المظلمة.
- تعزيز اجراءات التحقق من هوية المستخدمين خاصة على حسابات التواصل الاجتماعي.
- عدم مشاركة معلومات خاصة مثل الحسابات المالية أو كلمات السر في مواقع التواصل الاجتماعي أو أي جهات غير مؤمنة.
- عدم الضغط على أي روابط مشبوهة أو مرسلة مجهولة الهوية.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

1- الأوامر والمراسيم القانونية:

- المرسوم الرئاسي رقم 15 – 261 المؤرخ في 8اكتوبر 2015، المحدد لمهمة الوكالة الوطنية للامن المعلوماتي وتنظيمها وسيرها، الجريدة الرسمية، ع 55، سنة 2015

2- المواد والقوانين:

- الجمهورية الجزائرية الديمقراطية الشعبية، قانون العقوبات الجزائري، المادة 1، الجريدة الرسمية، ع 14، 2006
- القانون رقم 09 – 04، مؤرخ في 14 شعبان عام 1430 الموافق ل5 غشت 2009 ،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ،الجريدة الرسمية ،ع 47 ،مؤرخ في 25 شعبان 1430ه، الموافق ل16 غشت 2009.
- القانون رقم 09. 04 المؤرخ في 5 اوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية الجزائرية، ع 50
- قانون رقم 156/66 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، المادة 394 مكرر 1 الى4، الجريدة الرسمية الجزائرية.
- المادة 3 من القانون رقم 06.15 المؤرخ في 15 فيفري 2015 المعدل والمتمم لقانون رقم 05.01 المؤرخ في 6 فيفري 2005 والمتعلق بالوقاية من تبييض الاموال وتمويل الارهاب ومكافحتهما، المعدل والمتمم.

- المادة 394 مكرر من 8 الى 11، قانون العقوبات، الامر رقم 66 – 156المؤرخ في 8جوان 1966 المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 76، 2021.
- المادة 87 مكرر 11من القانون رقم 66 – 155 والمتعلق بقانون العقوبات، المعدل والمتمم بالقانون رقم 16 – 02 الصادر بتاريخ 2016/ 06 /19 الجريدة الرسمية، العدد 37 ،الصادرة بتاريخ 2016 / 06 / 22
- المادة 87 مكرر.
- المواد 87 مكرر الى 87 مكرر 12 من القانون 16. 02، المؤرخ في 14 رمضان 1437ه الموافق ل 19 يونيو 2016، يتمم الامر رقم 66. 156 المؤرخ في 18 صفر 1386ه الموافق ل8 يونيو 1966م والمتضمن قانون العقوبات، ج.ر.ع.4 مؤرخ في 17 رمضان 1437ه الموافق ل 22 يونيو 2016.
- المواد من 02. 03. 04، من القانون رقم 09 – 04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

ثانيا: المراجع

1- المعاجم

- ابن منظور، ابو فضل جمال الدين محمد بن مكرم ،لسان العرب، ط1 ،دار صادر ،بيروت، 436.1 حرف الباء ،فصل الراء، مادة رهب
- المعجم الوسيط، صادر عن مجمع اللغة العربية بجمهورية مصر العربية، ط4، مكتبة الشروق الدولية ،1435ه 2004م ،376، مادة رهبه.

2- الكتب:

- احسن بو سقيعة، الوجيز القانون الجزائي العام، ط 7، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2008.
- بلعيات ابراهيم، اركان الجريمة وطرق اثباتها، دار الخلدونية، ط1، الجزائر، 2007.
- جاسم محمد جندل ،الارهاب الالكتروني ،دار البداية ،ط1،عمان ،1435هـ.2014م.
- حسام فايز، الارهاب الالكتروني والثورة الرقمية، ط1 ،مؤسسة طيبة، القاهرة ،2019.
- خليفة عبد الرحمان، محاضرات في القانون الجنائي العام ،دار الهدى ،عين مليلة، الجزائر ،2012.
- الدليل التشريعي لنظام القانون العالمي لمكافحة الارهاب، اعداد مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينيا،2008.
- سامي علي حامد عياد ،استخدام تكنولوجيا المعلومات في مكافحة الارهاب، دار الفكر الجامعي، الاسكندرية، 2007.
- شفيق نوران أثر، التهديدات الالكترونية على العلاقات الدولية، طبعة 1، المكتب العربي للمعارف، القاهرة، مصر، 2015
- صدام حسين ياسين العبيدي، جرائم الانترنت وعقوباتها في الشريعة الاسلامية والقوانين الوضعية ،ط1 ،المركز العربي، مصر ،2019.
- صدقي، عبد الرحيم ،الارهاب السياسي والقانون الجنائي، دار النهضة العربية، القاهرة، 1958م.

- عبد الرحمن بن عبد الله سند، وسائل الارهاب الالكتروني وحكمها في الاسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الاسلام من الارهاب، الجزء الاول، الرياض، 2004.
- عبود السراج ،شرح قانون العقوبات القسم العام ،الجزء الاول، منشورات جامعة دمشق، دمشق، 2007.
- علي حمودة، شرح الاحكام العامة لقانون العقوبات الاتحادي، النظرة العامة للجريمة، الجزء الاول، مطبعة الفجيرة الوطنية، الامارات ،2008.
- فتحية سرور، الوسيط في قانون العقوبات، القسم العام، دار الشروق ' القاهرة، 2004
- محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005.
- المركز المصري للفكر والدراسات الاستراتيجية، استراتيجية امريكية هجومية ضد التهديدات السبيرانية ،القاهرة، 2018.
- منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006.

3- الأطروحات والرسائل الجامعية:

- حسن المبروك سعد، جريمة الارهاب الالكتروني "دراسة مقارنة" ،رسالة مقدمة لنيل شهادة الماجستير، الاكاديمية الليبية، القسم الجنائي، 2023.
- سفر، حسن بن محمد "الارهاب والعنف في ميزان الشريعة الاسلامية والقانون الدولي" بحث مقدم لمجمع الفقه الاسلامي.
- شاوشة ياسمينة، الارهاب الالكتروني بين مخاطره وآليات مكافحته، مذكرة تخرج لنيل شهادة الماستر في الحقوق، جامعة أكلي محمد أولحاج، بسكرة، 2019.

- مهني رمزي، سبيعة محمود، جريمة الارهاب الالكتروني، مذكرة لنيل شهادة ماستر، قانون اعلام الي والانترنت، جامعة برج بوعريريج ،الجزائر، 2023.
- نور الله تله، الارهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي، كلية الحقوق، جامعة دمشق، 2015 –2016.

4- المجلات والمقالات العلمية:

- الاتحاد الدولي للاتصالات، الاجندة العالمية للأمن السبيراني، جنيف، 2007.
- احمد بن محمد بن عبد الله، الملكية الفكرية في البيئة الرقمية ودورها في مكافحة الجرائم الالكترونية، مجلة العلوم القانونية، جامعة محمد الخامس، ع 12، 2020.
- بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني، 2017.
- بن حدو عبد الكريم، الركن المعنوي في الجرائم الارهابية ،مجلة الدراسات القانونية والسياسية، العدد 12 ،2022.
- بو عافية ليلى، الجرائم المعلوماتية ذات الطابع الارهابي، مجلة السياسية الجنائية، العدد 6، 2021.
- بوجمعة لطفي، الاجراءات الخاصة لمكافحة الجرائم الارهابية في التشريع الجزائري، مجلة العلوم الانسانية، جامعة باجي مختار، عدد خاص، 2018.
- بوزنون سعيدة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الانسانية، ع 47، 2019.
- تازير آمنة، جهود المنظمة القانونية الجزائرية في مكافحة جريمة الارهاب، مجلة الاستاذ الباحث، المجلد 4، ع 1، 2019.
- حسن بن أحمد الشهري، الارهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، ع 8، 2015.

- حملاوي عبد الرحمن، دور المديرية العامة للامن الوطني في مكافحة الجرائم الالكترونية، ملتقى وطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، 2015.
- سامي منصور، الارهاب الالكتروني، التحديات القانونية والامنية، مجلة العلوم القانونية، جامعة الجزائر 1، ع 19، 2020.
- صباح كزيز، أمال كزيز، الارهاب الالكتروني وانعكاساته على الامن الاجتماعي، مجلة التراث، رقم 1، ع 08، 2008.
- فراس طحان، الارهاب الالكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، ع2، 2011.
- كواشي عتيقة، تداعيات الارهاب السيبراني على الامن القومي الجزائري، المجلة الجزائرية للأمن والتنمية، جامعة باتنة 1 ،المجلد 12، ع 03، 2023
- ناصر العلي، الجهود الدولية في مكافحة الارهاب الالكتروني، مجلة الباحث للدراسات الاكاديمية، ع 01، 2021.
- ياسر فيصل الامين امين، جرائم الارهاب عبر الوسائل الالكترونية "دراسة مقارنة"، مجلة مصدر المعاصرة، العدد 547، 2022.

5- المؤتمرات العلمية:

- الامانة العامة لمجلس التعاون لدول الخليج العربية، البيان الرئاسي المشترك لاجتماع الدورة السابعة وعشرون للمجلس الوزاري المشترك بين مجلس التعاون والاتحاد الاوروبي، الرياض، 2023.
- جامعة الدول العربية، توصيات المؤتمر العربي حول الامن السيبراني ومكافحة الارهاب الالكتروني، بيروت، 2022.
- المركز الاوروبي لدراسة مكافحة الارهاب والاستخبارات، مكافحة الارهاب داخل الاتحاد الاوروبي وكيفية التعاون الامني، ألمانيا، 2023.

- معهد واشنطن لسياسات الشرق الادنى، التعامل مع المشهد الديناميكي للتهديدات الداخلية في الولايات المتحدة ،ترجمة وحدة الدراسات الامنية، واشنطن، 2021.
- معهد واشنطن لسياسات الشرق الادنى، التعاون في الامن السيبراني: تجربة الولايات المتحدة، 2022.
- منظمة الشرطة الجنائية، الانتربول والاتحاد الاوروبي: تعزيز التعاون في مجالات الامن ومكافحة الجريمة والارهاب، ليون، 2023.

6- المواقع الإلكترونية

- https://www.un.org/counterterrorism/ar/un-global-counter-te
- https//:www.assakina.com/news
- https://www.elbilad.net/article/detail?id=70386
- HTTPS://WWW.G77.ORJ/SSHLCST/ITU_ARABIC
- المنظمة العالمية للملكية الفكرية، تقرير التعاون الدولي لمكافحة الجرائم المرتبطة بالملكية الفكرية، متاح على الموقع الرسمي:

  HTTPS://WWW.WIPO.INT

فهرس المحتويات

فهرس المحتويات:

الفصل الثاني: الأساس القانوني لجريمة الإرهاب الإلكتروني

ملخص الدراسة

إن الإرهاب الالكتروني وليد التطور العلمي الهائل ومن مفجرات الثورة التكنولوجيا حيث يعد من الجرائم المستحدثة الذي يعتمد على الموارد المعلوماتية على عكس الإرهاب التقليدي، وهو إرهاب المستقبل والهاجس الأكبر لدول التي أصبحت عرضة لهجمات الإرهابيين والجمعات المتطرفة الذين يمارسون نشاطهم التخريبي في أي مكان وزمان فهو عالمي لا تربطه أي حدود جغرافية، ورغم قصر تاريخه إلا انه انتشر بسرعة النار في الهشيم ويتعالى مؤشر مخاطره يوم بعد يوم لان التقنية وحدها غير قادرة على حماية الناس من العمليات الإرهابية الالكترونية والتي سببت أضرار جسيمة على الأفراد والدول، مما يستدعي تضافر الجهود الدولية وإقليمية والوطنية لوضع استراتيجيات هادفة لمكافحة هذا الخطر الداهم أو التقليل من حدة أثره وضرره.

الكلمات المفتاحية: الجريمة، الارهاب الإلكتروني، الأمن السيبراني.

Abstract :

Cyberterrorism is the product of tremendous scientific developments and one of the triggers of the technological revolution. Unlike traditional terrorism, it is a newly emerging crime that relies on information resources. It is the terrorism of the future and the greatest concern for countries that have become vulnerable to attacks by terrorists and extremist groups who engage in destructive activities anywhere, anytime. It is global, unbound by geographical borders. Despite its short history, it has spread like wildfire, and its risk index is rising day after day. Technology alone is incapable of protecting people from cyberterrorist operations, which have caused significant harm to individuals and countries. This calls for concerted international, regional, and national efforts to develop targeted strategies to combat this imminent threat or mitigate its impact and harm.

Keywords: Crime, cyberterrorism, cybersecurity.