وزارة التعليم العالي والبحث العلمي
جامعة محمد البشير الإبراهيمي –برج بوعريريج –
كلية الحقوق والعلوم السياسية

جريمة الإرهاب الإلكتروني

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق
تخصص: قانون الإعلام الآلي والأنترنيت

من إعداد الطلبة:
- مهني رمزي
- سبيعة محمود

تحت إشراف الأستاذة:
د. مسعودان فتيحة

الاسم واللقب	الرتبة	الصفة
رمضاني مريم	أستاذ محاضر –ب–	رئيسا
مسعودان فتيحة	أستاذة مساعدة –ب–	مشرفا ومقررا
بن مالك إسمهان	أستاذة مساعدة –ب–	مناقشا

السنة الجامعية: 2022–2023

بسم الله الرحمن الرحيم

قال الله تعالى:

﴿وَإِذْ يَمْكُرُ بِكَ الَّذِينَ كَفَرُوا لِيُثْبِتُوكَ أو يَقْتُلُوكَ أو يُخْرِجُوكَ وَيَمْكُرُونَ وَيَمْكُرُ اللَّهُ وَاللَّهُ خَيْرُ الْمَاكِرِينَ﴾

سورة الأنفال الآية 30

شكر وعرفان

الحمد لله كاشف الغمة، رازق النعمة، ذو الفضل والمنة

الحمد لله حمدا كثيرا طيبا مباركا فيه

الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله

الحمد لله كثيرا الذي وفقنا ويسر لنا إنجاز هذا العمل المتواضع

ولأن شكر العباد من شكر الله، نتقدم بالشكر إلى:

أستاذتنا "الدكتورة مسعودان فتيحة " التي أفادنا بتوجيهاتها ونصائحها ومساعدتها لنا في إنجاز هذا العمل

نشكر كل من ساعدنا من قريب أو من بعيد

«نسأل الله الغفور الشكور أن يثبت الجميع بالأجر العظيم
إنه سميع عليم"

إهـــــــــــداء

انتهت الحكاية، ورفعت قبعتي مودعاً للسنين التي مضت، أهدي الى من وضع المولى سبحانه وتعالى الجنة تحت قدميها، ووقَّرها في كتابه العزيز، تلك الشمعة التي كانت تنير ظلمتي تلك التي لا أجد وصفا يليق بحبها وعطفها وحنانها هي أمي الحبيبة رحمها الله.

إلى من علمني العطاء وإلى من أحمل اسمه بكل افتخار وأرجو من الله أن يمد في عمرك والدي العزيز.

إلى أولادي إياد ومحمد نجيب.

إلى أخي منير التي لم تلدم أمي ولكن ولدته لي الأيام كان سنداً لي.

وإلى من تحلوا بالإخاء وتميزوا بالوفاء والعطاء وإلى من برفقتهم في دروب الحياة السعيدة والحزينة سرت وإلى من كانوا معي على طريق النجاح والخير "أصدقائي الأعزاء" بتوفيق من الله.

إلى جميع أساتذتي الكرام ممن لم يتوانوا في مد يد العون لي.

رمزي

إهـــــــــــداء

إلى صاحب السيرة العطرة، والفكر المستنير؛ فلقد كان له الفضل الأول في بلوغي التعليم العالي (والدي الحبيب)، أطال الله في عمره.

إلى من وضعتني على طريق الحياة، وجعلتني رابط الجأش وراعتني حتى صرت كبيرا أمي الغالية رحمها الله واسكنها فسيح جنانه.

إلى إخوتي من كان لهم بالغ الأثر في كثير من العقبات والصعاب.

إلى جميع أساتذتي الكرام ممن لم يتوانوا في مد يد العون لي.

محمود

قائمة المختصرات

أولا: باللغة العربية

1-ط: طبعة

2-ص: صفحة

3-الو م أ: الولايات المتحدة الأمريكية

4- ق ع ج: قانون العقوبات الجزائري

5- ق إ ج: قانون الإجراءات الجزائية

6- ج ر: الجريدة الرسمية

7-ع: عدد

8-د ط: دون طبعة

ثانيا: باللغة الفرنسية

1- P : PAGE
2- INCC : INSTITUT NATIONAL DE CRIMINALISTIQUE ET DE CRIMINOLOGIE
3- CPLCIC : CENTRE DE PREVENTION ET DE LUTTE CONTRE LA CRIMINALITE INFORMATIQUE ET LA CYBERCRIMINALTIE
4- SCLCO : LE SERVICE CENTRALE DE LUTTE CONTRE LA CRIME ORGANISE

مقدمة

مقدمة

يعتبر الإرهاب من أخطر وأعنف الظواهر التي شهدها العالم خلفت الملايين من الأرواح لم تفرق بين صغير وكبير ومعظم ضحاياها من الأبرياء وخير دليل ما حدث في الجزائر فيما يسمى بالعشرية السوداء ما يحدث في سوريا والعراق واليمن وتطورت هاته الجريمة بالتطور التكنولوجي.

غزت التطورات التكنولوجية الحديثة مجتمعاتنا في شتا مجالات الحياة، خاصة في مجال الإعلام والاتصال وهو ما سهل نقل المعلومة من مكان إلى أخر، وبفضل هذه التكنولوجيا أصبح العالم قرية صغيرة مفتوحة، يمكن من خلالها العبور إلى عوالم أخرى لم يكن لنصل إليها.

برزت بعض الصور الإجرامية المستحدثة التي كان لهذا التطور أثراً في بروزها، ومن هذه الطائفة جرائم الإرهاب، فلقد أسفر التطور الحاصل الى ظهور ما يسمي بجرائم الإرهاب الإلكتروني ، الذي اصبح ظاهرة تسهل تجنيد وتدريب الشباب لا سيما التأثير على أفكارهم ومعتقداتهم، وتشجيعهم على القتل والتخريب والتي لا يتوقف نطاقها عند دولة محددة، بل يمتد اتساعاً ليشمل بطريق مباشر أو غير مباشر عدة دول، وهو ما يثير إشكالية أخري مرتبطة بضرورة المواجهة وضرورة توفير آلياتها لمواجهة جرائم الإرهاب الإلكتروني، التي لا يقتصر نطاقها على دولة دون أخري، بل تمتد آثاره الى عدة دول، وهو ما يوجب بطبيعة الحال تتضافر الجهود على المستوي الدولي لتحقيق فاعلية المواجهة، بل أنه يحتم بالإسراع ببحث النظم القانونية القائمة ومدى قدرتها على مواجهة الصور المستحدثة للإرهاب، لتدارك أوجه النقص والقصور، بما يتطلبه ذلك من تعزيز قدرات الأمن السيبراني، وهو ما عنيت الدراسة بإبراز خطورته.

أهمية الموضوع:

وتكمن أهمية دراسة هذا الموضوع في إلقاء الضوء على الإرهاب الرقمي المعاصر من خلال تحديد مفهومه وخصائصه وحجم مخاطر التي يخلفها وانعكاساته على المجتمعات، وتبيان آليات المكافحة والوقاية منه سواء فنيا/تقنيا/قانونيا على الصعيد الدولي أو الإقليمي، حيث يعتبر من أخطر أشكال الإرهاب أكثرها استحداثا أو انتشارا في ظل التطور التكنولوجي وتنامي استخدام شبكة الأنترنت.

أسباب اختيار الموضوع:

اخترنا دراسة موضوع جريمة الإرهاب الإلكتروني لعده أسباب منها الشخصية والموضوعية، فتنطوي أهم الأسباب الشخصية كون هذا الموضوع في مجال تخصصنا قانون الإعلام الآلي والأنترنت، واهتمامنا الشخصي بموضوع الإرهاب الإلكتروني، وما يرتبط به من استراتيجيات وآليات مكافحته، وكذلك الميول والرغبة في دراسة المواضيع الجنائية.

تتمثل الأسباب الموضوعية في كونه من المواضيع الحديثة التي تستحق بذل الجهود للبحث فيه كونه ظاهرة مستجدة متعددة الأبعاد وما تسببه من مخاطر التي قد تمس كل القطاعات الحيوية والحساسة والبنية التحتية والخسائر التي يحدثها قد تفوق تفجير قنبلة والأمر الذي حفزنا على البحث فيه كونه من المواضيع التي شغلت اهتمام الراي العام العالمي والإقليمي.

إشكالية الموضوع:

وتتلخص إشكالية الموضوع في البحث عن مفهوم الإرهاب الإلكتروني والوسائل التي يستعملها الإرهابيون في تنفيذ أعمالهم، مع عرض الآليات المختلفة لمواجهة هذه الجريمة التي تشكل تهديدا يؤرق الكثير من الدول، ومنها دولة الجزائر التي تبذل جهودا كبيرة من أجل تحقيق أمنها السيبراني.

ومن خلال ما سبق يتبادر الى أذهاننا طرح الإشكالية التالية:

ما المقصود بالإرهاب الإلكتروني؟ وفيما تتمثل آليات مكافحته؟

أهداف الموضوع:

يمكن إجمالها فيما يلي:

تسليط الضوء على تحديد مفهوم الإرهاب الإلكتروني وتبيان اهم خصائصه وأهدافه التي يسمو الهيا ووسائله وكذلك أهم مظاهره وعرض مخاطره بهدف التوعية باعتباره الخطر القادم، بالإضافة الى تحديد الأركان العامة لهذه الجريمة من الناحية القانونية والعقوبات المقررة لها وكذا التطرق الى آليات المكافحة على الصعيد الدولي والإقليمي والوطني.

المنهج المتبع:

تم الاعتماد على المنهج الوصفي التحليلي لوصف جريمة الإرهاب الإلكتروني من خلال تحديد بعض المفاهيم وأهم الخصائص التي تتميز بها هذه الجريمة، والمنهج التحليلي الذي يناسب طريقتنا في الإجابة على تساؤلاتنا وعليه ارتأينا تقسيم هذه الدراسة الى فصلين:

الفصل الأول: تناولنا فيه الإطار المفاهيمي لجريمة الإرهاب الإلكتروني، حيث تطرقنا في المبحث الأول الى: مفهوم جريمة الإرهاب الإلكتروني والأساس القانوني لجريمة الإرهاب الإلكتروني في المبحث الثاني، كما تناولنا في الفصل الثاني مكافحة جريمة الإرهاب الإلكتروني حيث خصصنا المبحث الأول لآليات مكافحة جريمة الإرهاب الإلكتروني والمبحث الثاني الهيئات الخاصة لمكافحة جريمة الإرهاب الإلكتروني.

الفصل الأول:

الإطار المفاهيمي لجريمة الإرهاب الإلكتروني

شهد العالم في الآونة الأخيرة تطوراً هائلاً في استعمال التقنيات التكنولوجية الحديثة والوسائل الإلكترونية في مجال الاتصالات وتقنية المعلومات كاستخدام الحاسوب والهواتف النقالة الذكية ومواقع التواصل الاجتماعي (الفيس البوك، الإنستغرام، التويتر، الإيمو، الفايبر، الواتساب) عبر شبكات الاتصال وشبكة المعلومات الدولية "الأنترنت"، حتى أضحى العالم بفضلها قرية صغيرة لا تفصله عن بعضه الحدود المعروفة بين الدول، كما أصبحت الدول تعتمد عليها في تيسير مختلف قطاعاتها ومؤسساتها الحيوية وبنيتها التحتية ووظائفها وأهدافها، وهذا مما فتح مجال للإرهاب إلى تطوير أساليبه الإجرامية فظهر نوع جديد من الإرهاب وهو "الإرهاب الإلكتروني" (الإرهاب الرقمي) إذ استغلت الجماعات والمنظمات الإرهابية تلك البيئة الإلكترونية (البيئة الرقمية) في توسيع نشاطاتها الإجرامية لتحقيق أغراضها الإرهابية بتخويف وترويع الدول وتدمير بنيتها التحتية التي تدار بالحاسبات الإلكترونية والشبكات المعلوماتية وعلاوة عن الشركات الاقتصادية الكبرى والجماعات والأفراد وإلحاق الضرر المادي والمعنوي بهم أو تهديدهم بالاعتماد على استخدام وسائل الاتصال الحديثة والشبكات المعلوماتية ومن أهم مظاهر الإرهاب الإلكتروني وأشكاله[1] .

وعليه قد تم تخصيص هذا الفصل للحديث عن الإطار المفاهيمي لجريمة الإرهاب الإلكتروني وهو ما سنتناوله من خلال:

المبحث الأول: مفهوم جريمة الإرهاب الإلكتروني

المبحث الثاني: الأساس القانوني لجريمة الإرهاب الإلكتروني

1- حيدر فالح، جريمة الإرهاب الإلكتروني، مقال منشور على الموقع https://www.sjc.iq/view.70721/

تم الاطلاع عليه يوم 04 /06 / 2023 على الساعة 41: 23.

المبحث الأول: مفهوم جريمة الإرهاب الإلكتروني

يعد الإرهاب الإلكتروني من الجرائم التي استغلت الجانب السلبي للتطور الهائل لوسائل الاتصال وثورة الأنترنت والتكنولوجيا التي حولت العالم الى قرية صغيره خالية من الحدود الجغرافية والسياسية وجعلت المعلومات في متناول الجميع، حيث استغل الإرهابيين هذا التطور لتنفيذ أنشطتهم الإرهابية وأعمالهم التخريبية وبذلك ساهمت عوامل التحضر السريع وسهولة استخدام هذا السلاح الذي يعرف بالإرهاب الإلكتروني الى انتشاره الهائل وارتفاع نسبة ضحاياه وشده أثره وضرره.

فالإرهاب الإلكتروني يتميز عن غيره من أنواع الإرهاب في استخدام الموارد المعلوماتية والوسائل الإلكترونية وكذا في طبيعته ونطاقه ووسائله وحتى خصوصيه مرتكبيه[1] .

المطلب الأول تعريف الإرهاب الإلكتروني في الفقه والتشريع

التطور الحاصل في مجال تكنولوجيا الإعلام والاتصال الحديثة أسفر عن نوع جديد من أنواع الإرهاب والذي يعد من الجرائم المستحدثة وهو الإرهاب الإلكتروني أو الإرهاب الرقمي وجاء نتيجة التزاوج بين الإرهاب وتكنولوجيا الإعلام والاتصال [2] .

سنحاول من خلال هذا المطلب تقديم تعريف الإرهاب الإلكتروني في الفرع الأول ثم سنتطرق في الفرع الثاني الى تعريف الإرهاب الإلكتروني في التشريع الجزائري.

1- شاشوه ياسمينة، الإرهاب الإلكتروني بين مخاطره وآليات مكافحته، مذكرة ماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة اكلي محمد أو الحاج، بويرة، 2019 2020، ص 7.

2 -إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة البحرين، 2012، ص 23.

الفرع الأول: تعريف الإرهاب الإلكتروني

عرفه الفقه على انه: خرق للقانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف أثاره اضطراب خطير في نظام العام عن طريق شبكه المعلومات العالمية الأنترنت

كما عرفه عادل عبد الصادق بانه: يعني العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادرة من دول أو جماعات أو الأفراد عبر الفضاء الإلكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له[1].

هناك من عرفه انه: هجمات غير مشروعة أو تهديدات بهجمات ضده الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الانتقام والابتزاز أو الإجبار أو تأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره، لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، وبالتالي كي يلقب الشخص بأنه إرهابي على الأنترنت وليس مخترقا فقط، فلابد من أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب [2].

حيث أن فرنسا عرفت الإرهاب الإلكتروني على انه: كل هجوم الغرض منه الحصول على معلومات مرتبطة بالغير وإمكانياته وإستراتيجيته التي يتخذها للدفاع عن نفسه أو تدمير نظم المعلوماتية أو نشر المعلومات الزائفة من اجل تظليله بتوظيف تكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والأنترنت[3].

1- عادل عبد الصادق، الإرهاب الإلكتروني قوه في العلاقات الدولية نمط جديد وتحديات جديدة، ط1، مركز الأهرام للدراسات السياسية والاستراتيجية، 2009، ص109.

2- علي عدنان الفيل، الإجرام الإلكتروني، ط1، مكتبة زين الحقوقية والأدبية، لبنان،2011 ص60.

3- Peter belly , Hached attacked, abuses digital crime exposés, London, Regan p 2002 p 107

كما عرفته إيطاليا على انه: كل جماعة إرهابية تستعمل الوسائل التكنولوجية الأنترنت من اجل الدعاية لنشاطاتها أو التعريف بأهدافهم أو التنسيق أو التبادل المهارات والخبرات والأساليب أو جمع تبرعات من اجل تمويل عملياتهم الإرهابية[1].

كما عرفته المملكة العربية السعودية: على انه أي فعل يرتكب متضمن استخدام الحاسب الآلي أو الشبكة المعلوماتية أو استخدام تقنيه الرقمية المخالفة لأحكام النظام ومن أنواعه السب، تشهير، الابتزاز، والإباحة وكذلك الشائعات وما يتعلق بأمور المالية كالاعتداء على البطاقات البنكية بأشكالها واختلاسها[2].

وعرفه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي بانه : العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دينه ودمه وعقله وماله وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف الى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو امنهم أو أموالهم للخطر، ومن صنوفه الحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها[3].

1- شاشوه ياسمينة، المرجع السابق، ص14.

2 – نجاري بن حاج، علي فايزة، الآليات القانونية للإرهاب الإلكتروني، مذكرة ماستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص، 28 29.

3- راجع بيان مكة المكرمة الصادر عن المجمع الفقهي الإسلامي التابع لرابطة العالم الإسلامي في دورته 16 مكة المكرمة يوم 01-11-2002.

الفرع الثاني: تعريف الإرهاب الإلكتروني في التشريع الجزائري

المشرع الجزائري لم يعرّف الإرهاب الإلكتروني إلاّ أنّه قام بتعريف فعل الإرهاب وكذلك جريمة تمويل الإرهاب حيث عرف الإرهاب بموجب المادة 87 مكرر من الأمر رقم 95 – 11 المؤرخ في 25 فيفري 1995 المعدل والمتمم للأمر رقم 66 – 156 المتضمن قانون العقوبات، حيث نصت المادة السالفة الذكر على أنّه: «يعتبر فعلا إرهابيا أو تخريبيا، في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي:

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم أو المس بممتلكاتهم،
- عرقلة حركة المرور أو حرية التنقل في الطريق والتجمهر أو الاعتصام في الساحات العمومية
- الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والتنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.
- الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في الباطن أو إلقاءها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.
- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.

عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات" [1] .

1- الأمر رقم 95 – 11 مؤرخ في 25 رمضان 1415 الموافق 25 فبراير 1995 يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، ج.ر.ع.11، مؤرخة في 29 رمضان 1415 هـ.

فالمشرع الجزائري قد عرّف بموجب هذه المادة المقصود من الإرهاب وما هي صوره وحالته إلا أنّه لم يتطرق إلى ذكر الإرهاب الإلكتروني، إلاّ أنّ ما يمكن قوله وهو إسقاط هذه المادة على الإرهاب الإلكتروني بمعنى أنّه كلما ارتكبت هذه العمليات بواسطة وسيلة نكون أمام جريمة الإرهاب الإلكتروني، حيث تختلف فقط الجريمة من حيث طريقة ارتكابها.

وعلى ضوء تعريفات الواردة أعلاه وبعد عقد مقارنة فيما بينهما نميل إلى أن تعريف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي مناسب لتعريف الإرهاب اصطلاحا لقصر ألفاظه وإيجاز عبارته وشموله لمختلف مظاهر وأنواع الإرهاب وأشكاله وأهدافه

وعلى إثر ما سبق من تعريفات يمكن أن نخرج بتعريف لجرائم الإرهاب الإلكتروني ونقول إنها كل عدوان أو تخويف أو تهديد مادي أو معنوي يحدث من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام التقنية المعلوماتية والوسائل الإلكترونية بشتى أنواع العدوان ومظاهر الفساد[1] .

المطلب الثاني: خصائص وأهداف الإرهاب الإلكتروني

أحدثت الثورة التكنولوجية في الاتصالات والمعلومات ثورة فكرية في مفاهيم الحرب والعدوان وفي مضامين القانون الدولي والوسائل أيضا، فلم يعد هناك مجال لإعلان الحرب بين الدول أو بين الجماعات، بل شملت الحرب الدخول لأنظمة المعلومات وتدميرها أو التأثير في كيفية عملها مما يكون له الأثر الكبير في ظل الاعتماد المتزايد للدول على التكنولوجيا في الاقتصاد والسياسة وفي شتى مجالات الحياة[2].

1- محمد الطيب عبد الله خالد، (الإرهاب الإلكتروني)، مجلة كلية الشريعة والقانون، جامعة أم درمان الإسلامية، المجلد الثالث عشر 2020 ص 100.

2- عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة مطبوعات مركز الدراسات السياسية والاستراتيجية، ط 1، القاهرة، 2009، ص 118.

الفرع الأول: خصائص الإرهاب الإلكتروني

يتميز الإرهاب الإلكتروني بعدد من الخصائص والسميات التي يختلف فيها عن بقية الجرائم، وتحول دون اختلاطه بالإرهاب العادي، ومن الممكن إيجاز اهم تلك الخصائص فيما يلي:

1. أن الإرهاب الإلكتروني لا يحتاج ارتكابه الى العنف والقوه، بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية والمزود ببعض البرامج اللازمة.
2. حيث يعتبر الإرهاب الإلكتروني جريمة، عابرة للقارات وغير خاضع بنطاق إقليم محدود [1].
3. صعوبة اكتشاف جرائم الإرهاب الإلكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.
4. صعوبة الإثبات في الإرهاب الإلكتروني نظرا بسرعه غياب الدليل الرقمي وبسهولة إتلافه وتدميره.
5. وتميز الإرهاب الإلكتروني لأنه يجري عاده بتعاون أكثر من شخص على ارتكابه.
6. إن مرتكب الإرهاب الإلكتروني يكون في العدم من ذوي الاختصاص في مجال تقنيه المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسوب والشبكة المعلوماتية[2].

الفرع الثاني: أهداف الإرهاب الإلكتروني

يهدف الإرهاب الإلكتروني الى تحقيق جمله من الأهداف الغير مشروعه ويمكننا بيان أبرز تلك الأهداف في النقاط الأتية:

1. نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة
2. الإخلال بالنظام العام، والأمن المعلوماتي، وزعزعة الطمأنينة
3. تعريض سلامه المجتمع وأمنه للخطر

1- نسرين فوزي، تجريم الانفلات الإلكتروني، ط 1، دار الأهرام للنشر، مصر، 2019، ص 82.

2 حسن طاهر داود، جرائم نظم المعلومات، ط 1، مطبعة جامعة نايف العربية للعلوم الأمنية، الرياض،2000، ص 120.

4. الحاق الضرر بالبنا المعلوماتية الأساسية وتدميرها والأضرار بوسائل الاتصالات وتقنيه المعلومات، أو بالأموال والمنشئات العامة والخاصة
5. تهديد السلطات العامة والمنظمات الدولية وابتزازها
6. الدعاية والإعلام، وجذب الانتباه، وأصاله للرأي العام
7. جمع الأموال والاستيلاء عليها[1]

المطلب الثالث: مظاهر الإرهاب الإلكتروني وأشكاله ووسائله

من الصعب تحديد أشكال أو مظاهر الإرهاب الإلكتروني فطبيعة هذا النوع من الجرائم تتطلب التصنيف نظرا لأنها تستخدم تكنولوجيا تتطور يوما بعد يوم، فالإرهاب الإلكتروني يرتبط بالمستوى المتقدم الذي تحتله وسائل الاتصال وتقنية المعلومات في جميع مجالات الحياة، وفي العالم باسره، ومن خلال الأنظمة الإلكترونية والشبكات المعلوماتية اتخذ الإرهاب أبعادا جديدة وازدادت خطورته على المجتمع الدولي[2].

الفرع الأول: مظاهر الإرهاب الإلكتروني وأشكاله ووسائله

يعتبر الإرهاب حسب ما عرفته اتفاقية جنيف الخاصة بقمع الإرهاب لعام 1391 على أنه " الأعمال الإجرامية الموجهة ضد الدولة، والتي يكون من شأنها إثارة الفزع والرعب لدى شخصيات معينة أو جماعات من الناس أو لدى الجمهور"[3].

يتخذ الإرهاب الإلكتروني أشكال وطرق عديدة على حسب الأهداف المرجوة من العملية الإرهابية، فهي تتغير بتطور الوسائل التكنولوجية وهذا ما سيتم تناوله في هذا الفرع.

1- حسنين شفيق، المرجع السابق، ص 191.

2- شعنبي صابرة، "الإرهاب الإلكتروني، الأشكال والدوافع، مجلة العلوم الاجتماعية والإنسانية، العدد 10، جوان 2015 ، جامعة تبسة، ص443.

3- عبد الرحمن بن سالم بن فهاد الطريف، اتجاهات الطلاب الجامعيين نحو ظاهرة الإرهاب، دراسة ميدانية على طلاب الجامعات في الرياض، مذكرة لنيل شهادة الماجستير في العلوم الاجتماعية، تخصص تأهيل ورعاية اجتماعية، قسم العلوم الاجتماعية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2006، ص 21.

أولا: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب وتبادل الآراء في الأفكار والمعلومات صعبا في الواقع، فانه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيرا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين، ويتبادلون أطراف الحديث والاستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمع لهم أتباعا وأنصار عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية[1].

وعلى الرغم من أن البريد الإلكتروني (E-MAIIL) اصبح من اكثر الوسائل استخداما في مختلف القطاعات، و خاصة قطاع الأعمال , لكونه أكثر سهولة وأمننا وسرعة لإيصال الرسائل، إلى أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، بل ان كثيرا من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية ومخططين لها، والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية[2].

فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراضهم الغير مشروعة، والتي تتعارض مع مصلحة المجتمع ويستخدموا الإرهابيون الشبكة

1- محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها، الإرهاب الإلكتروني وطرق مواجهته، ملتقى الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية، كلية العلوم والدراسات الاستراتيجية، المملكة الأردنية الهاشمية 2013، ص 17.

2 – أمير فرج يوسف، المرجع السابق، ص 234،235 .

العالمية للمعلومات بشكل يومي لنشر أفكارهم الهدامة وتحقيق أهدافهم السيئة، ويمكن إبراز أهم استخدامهم للشبكة فيما يلي:

1- الاتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة للشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم، نظرا لقلة تكاليف الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال والتخفي، وذلك عن طريق البريد الإلكتروني أو مواقع المنتديات وغرف الحوار الإلكتروني، حيث يمكن وضع رسائل مشفرة تأخذ طابعا لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته كما أنها لا تترك أثر واضحا يمكن أن يدل عليه[1].

2- جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفره المعلومات الموجودة فيها، كما أنها تعتبر موسوعة الكرتونية شامله متعددة الثقافات، ومتنوعة المصادر، وغنيه بالمعلومات الحساسة التي يسعى الإرهابيين الحصول عليها.

بالتأكيد فان الأنترنت عالم كبير ومن خلال التقنيات والبرامج المتاحة في الحواسيب يمكن لتلك التنظيمات من أن تستثمر تلك البرامج لصالحها وعلى سبيل المثال لا الحصر برنامج Google Earthالذي يتيح لك خرائط مجانية عن كل المواقع الأمنية و المنشآت النووية ومواعيد إقلاع الطائرات وهبوطها ... الخ[2].

1- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والأنترنيت، مكتبة الوفاء القانونية، الطبعة الأولى، 2011، ص 233.

2- حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، كلية العلوم القانونية والسياسية، جامعة ديالي، عدد خاص، ص 318.

3 – التخطيط والتنسيق بالعمليات الإرهابية

العمليات الإرهابية عمل على جانب من التعقيد والصعوبة، فهي تحتاج الى تخطيط محكم، وتنسيق شامل، وتعتبر الشبكة العالمية للمعلومات وسيله اتصال بالغه الأهمية للجماعات الإرهابية، حيث تتيح لهم حريه التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيدا عن أعين الناظرين، مما يسهل على الإرهابيين ترتيب تحركاتهم، وتوقيت هجماتهم[1].

4-الحصول على التموين

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية سكانيه منتقاة من المعلومات الشخصية التي يدخلها المستخدمين على الشبكة المعلوماتية من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات ماليه لأشخاص اعتباريين يكونون واجهه لهؤلاء الإرهابيين، ويتم ذلك بواسطه رسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية ،بطريقه ذكيه وأسلوب مخادع، بحيث لا يشك المتبرع بانه سيساعد أحد التنظيمات الإرهابية[2].

6 –إصدار البيانات الإلكترونية

تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتهم الإرهابية المختلفة، وذلك عن طريق المواقع الإلكترونية أو بواسطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وساحاتها، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفه انتشار تلك البيانات، ووصولها الى مختلف شرائح المجتمع وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية

1- أمير فرج يوسف، المرجع السابق، ص 234.

2 – حسنين شفيق، المرجع السابق، ص 195.

اتجاهات متنوعة، فتارة ترسم أهدافا وخططا عامة للتنظيم الإرهابي، وأحيانا تكون للتهديد والوعيد بشن هجومات إرهابيه معينه، في حين تصدر معلنه عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار صادرة من جهات أخرى[1].

ثانيا: إنشاء المواقع الإرهابية الإلكترونية

يقوم الإرهابيون بأنشاء وتصميم مواقع لهم على الشبكة العالمية الأنترنت لبث أفكارهم الضالة، والدعوة الى مبادئهم المنحرفة، ولإبراز قوة التنظيم الإرهابي، والتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الإلكتروني، وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بالشم هجمات إرهابية، فقد أنشئت مواقع إرهابية الكرتونية لبيان كيفية صناعه القنابل المتفجرات، والأسلحة الكيماوية الفتاكة، ولشرح طرق اختراق البريد الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول الى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ونحو ذلك وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا بالنسبة للإرهابيين، فان إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات , لخدمة أهدافهم وترويج أفكارهم الضالة اصبح سهلا وممكنا، ولذا فان معظم التنظيمات الإرهابية لها مواقع الإلكترونية، وهي بمثابه المقر الافتراضي لها[2] و لقد أصبح من السهل قيام الإرهابيين بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات لاستغلالها في البث والدعوة لأفكارهم الظل و مبادئهم المنحرفة لإبراز قوة التنظيم الإرهابي والتعبئة الفكرية وتجنيد إرهابيين جدد وإعطاء التعليمات والتلقين والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية فقط أنشئت مواقع إرهابية الكرتونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية،

1- حسنين شفيق، المرجع السابق، ص 192- 195.

2 -عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، ص 32.

ولشرح طرق اختراق البريد الإلكتروني كيفية اختراق وتدمير المواقع الإلكترونية، الدخول الى المواقع المحجوبة وتعليم طرق نشر الفيروسات[1].

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع بصورة كبيرة، فاذا ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الإلكتروني غدا، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان الكرتوني مختلف، بل تجد لبعض المنظمات الإرهابية في آلاف المواقع، حتى يضمنوا انتشار أوسع للمعلومات، وحتى لو جرى منع دخول على بعض هذه المواقع أو تعرضت بعضها لتدمير وفق المواقع الأخرى ويمكن الوصول إليها[2].

ومن الأمثلة على بعض المواقع الإلكترونية نذكر على سبيل المثال بعض المواقع الإلكترونية التي قام بأنشائها وتصميمها بعض تنظيمات الإرهابية، فمن حيث المواقع الغربية نذكر موقع المقاومة الأريانية البيضاء، التي أسسها توم ميتزقر Tom metzgy المتطرف الأمريكي , حيث أسس مجموعة بريدية إلكترونيه لبث أفكاره المتطرفة والتواصل مع أتباعه، امثله المواقع الإلكترونية العربية، موقع النداء وهو الموقع الرسمي لتنظيم القاعدة، ومن خلاله تصدر البيانات الإعلامية، وصوت الجهاد وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب ، وهي تصدر بصيغتي WORLD,PDF ، تتضمن مجموعة من البيانات والحوارات مع قادة التنظيم الفضاء الإلكتروني[3].

ولقد وجد الإرهابيون غايتهم في تلك الموارد المعلوماتية لوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات وأصبح للمنظمات الإرهابية العديد من المواقع عبر الشبكة العالمية للمعلومات وصارت تلك المواقع من أبرز مظاهر أشكال الإرهاب الإلكتروني.

1- فايز بن عبد الله الشهري، بحث بعنوان استخدام شبكة الأنترنت في مجال الإعلام الأمني العربي، مجلة البحوث الأمنية، مركز الدراسات، كلية الملك فهد الأمنية، الرياض، المجلد 10، العدد 19، نوفمبر 2001، ص 182.

2- حسنين شفيق، المرجع السابق، ص196.

3 - حسن مظفر الروزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، بيروت، ط 1، 2007، ص 23.

ثالثا: التهديد والترويع الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتنوع طرقه، وذلك من اجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن اجل الحصول على التمويل المالي ولإبراز قوة التنظيم الإرهابي من ناحية أخرى. والمقصود بالتهديد الوعيد بالشر وزرع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضررا ما سيلحقه أو سيلحق أشخاصا وأشياء له بها صله وقد يلجأ إرهابي الإرهاب الإلكتروني الى التهديد وترويع الأخرين عن طريق الاتصالات والشبكات المعلوماتية، بغيت تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية لتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة للتهديد وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية[1].

ولقد تعددت الأساليب الإرهابية بالتهديد، فتارة يكون التهديد بالقتل شخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير المنشآت الوطنية، ويكون تارة أخرى بنشر فيروسات من اجل الحاق الضرر والدمار بشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية الأساسية المعلوماتية[2].

رابعا: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجمات الكرتونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالبا، وهي الأهداف العسكرية، والسياسية، والاقتصادية، وفي عصر ثوره من المعلومات تجد

1 – حسنين شفيق، المرجع السابق، ص 198.

2 – رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة، 1985، ص 23.

الأهداف الثلاثة نفسها، وعلى راسها مراكز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه ، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة شعوب والمجتمعات الدولية[1].

وقد بات من شبه المؤكد أنه لا تتوافر حتى الآن تقنيه أو نظام أو تطبيق يمكن أن تحول كاملا دون تدمير المواقع أو اختراقها أو سرقه البيانات بشكل دائم المتغيرات التقنية، إلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس تصميم المفتوح للأجزاء سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة تجعل الحيلولة دون حصول القرصنة أمرا غير ممكن، اضافتا الى أن المنظمات الإرهابية من ضمن أهدافها الرغبة في الاختراق وتدمير المواقع بما لديها من الإمكانيات والقدرات التي لا تتوافر للأفراد[2].

الفرع الثاني: مظاهر وصور جريمة الإرهاب الإلكتروني وفقا للقانون رقم 16- 02

نستنتج من خلال تحليل المواد 87 مكرر 11 والمادة 87 مكرر 12 والمادة 394 مكرر 8 من القانون رقم 16 – 302 [1]بعض الصور والمظاهر الّتي تكيف على أنّها جريمة إرهاب الكرتوني وتتمثل في الآتي:

أولا: ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها

تأتي جريمة الإرهاب الإلكتروني في عدّة صور ومن بينها ارتكاب الفعل الإرهابي أو التدبير له أو التدريب على ارتكابه أو المشاركة في ارتكابه، حيث يعاقب كل من قام بارتكاب

1- أمير فرج يوسف المرجع السابق ص 238

2 -علي عسيري، الإرهاب والأنترنت، جامعة نايف للعلوم الأمنية الطبعة الأولى الرياض 2006 ص 43

3- المواد 87 مكرر 11و 394 مكرر 8 من القانون رقم 16 – 02، مؤرخ في 14 رمضان 1437 هـ الموافق 19 يونيو 2016 م، يتمم الأمر رقم 66 – 156 المؤرخ في 18 صفر 1386 هـ الموافق 8 يونيو 1966 م والمتضمن قانون العقوبات، ج.ر.ع.4 مؤرخة في 17 رمضان 1437 هـ الموافق 22 يونيو 2016م.

فعل من الأفعال المذكورة سواء كان مرتكب الجريمة جزائري أو أجنبي مقيم في الجزائري بطريقة شرعية أو غير شرعية وكان ارتكابها ذلك باستخدام تكنولوجيات الإعلام والاتصال بالعقوبة المقررة للإرهاب الإلكتروني[1].

ثانيا: السفر أو محاولة السفر من أجل ارتكاب الأفعال الإرهابية المذكورة في الفقرة الأولى من المادة 87 مكرر 11

وتعتبر جريمة إرهاب الكرتوني كل شخص جزائري أو أجنبي مقيم في الجزائر بصورة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها[2].

ثالثا: توفير أو جمع أموالا في تمويل سفر أشخاص للقيام بأعمال إرهابية

يعتبر من مظاهر أو من صور الإرهاب الإلكتروني توفير أو جمع الأموال بصورة عمدية وبأية وسيلة كانت وسواء كان ذلك بصورة مباشرة أو غير مباشرة بقصد استعمالها أو مع علمه بأنّها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بهدف ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها[3] كما تعتبر أيضا القيام بصورة عمدية بتنظيم أو تمويل سفر أشخاص إلى دولة أخرى ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر مظهر من مظاهر الإرهاب الإلكتروني.

رابعا: استخدام تكنولوجيات الإعلام والاتصال في تجنيد الأشخاص لتحقيق أعمال إرهابية

يعتبر من جرائم الإرهاب الإلكتروني وفقا لقانون العقوبات الجزائري استخدام تكنولوجيات الإعلام والاتصال في سبيل تجنيد أشخاص لصالح إرهابي، أو جمعية، أو تنظيم، أو جماعة، أو منظمة يكون الغرض منها أو تقع أنشطتها تحت أعمال إرهابية وفقا لقانون العقوبات المعدل سنة 2016 أو ينظم شؤونها، أو يدعم أعمالها أو أنشطتها، أو ينشر أفكارها بصورة مباشرة أو غير مباشرة.

1- المادة 87 مكرر 11 من القانون رقم 16 – 02، المرجع السابق.

2- المادة 87 مكرر 2/11، المرجع نفسه.

3- المادة 87 مكرر 11، المرجع نفسه.

حيث تجند الجماعة الإرهابية من خلال الأنترنيت عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإرهابية، وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر فتعلن الجماعة الإرهابية عبر مواقعها على الأنترنيت حاجاتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الاستشهاد في سبيل الفوز بالجنة[1].

وإضافة إلى الصور المذكورة أضاف المشرع الجزائري صورة أخرى تعتبر مظهرا من المظاهر المعاقب عليها بصدد جرائم الإرهاب الإلكتروني، وهي معاقبة مقدمو خدمات الأنترنيت في حالة الامتناع رغم اعذراهم من طرف الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته أو عن طريق صدور أمر أو حكم قضائي عن التدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو الامتناع عن وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بجرائم الإرهاب المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن[2].

1- محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، 2004، ص.13.

2 – المادة 394 مكرر 8 من القانون رقم 16 – 02، المرجع السابق.

المبحث الثاني: الأساس القانوني لجريمة الإرهاب الإلكتروني

إن تحقق الجريمة على الواقع الميداني لا يقوم إلا بتحقيق كافة الأركان الخاصة بها وهي التي تحدد نطاق الجريمة وتفصلها عن غيرها من الجرائم وتنطوي على تبيان اهم أركانها, و يقسم الفقهاء أركان الجريمة إلى ثلاثة أركان, الركن الشرعي للجريمة يعني وجود نص يجرم الفعل ويقدر عقوبته قبل وقوعه و ركن مادي يتمثل في النشاط الإجرامي للجاني ونتيجة محققة بالفعل, تصل بينهما رابطة سببية, بينما يتمثل الركن المعنوي في تلازم الإرادة والعلم بتجريم القانون للفعل لدى الجاني, واتجاه إرادة الجاني لتحقيق النتيجة هو ما يحدد القصد الجنائي . جريمة الإرهاب الإلكتروني كغيرها من الجرائم الأخرى لها ثلاث أركان تقوم عليهم الركن الشرعي، الركن المادي، الركن المعنوي وسنتناولها في ثلاث مطالب.

المطلب الأول: الركن الشرعي لجريمة الإرهاب الإلكتروني

يتمثل الركن الشرعي في جريمة الإرهاب الإلكتروني بوجود نص قانوني يجرم الفعل فلا جريمة ولا عقوبة إلا بنص قانوني، كما نصت علية المادة 01 من ق ع ج «لا جريمة ولا عقوبة أو تدابير أمن بغير قانون»[1].

الفرع الأول: تعريف الشرعية الجنائية

يقصد بمبدأ الشرعية الجنائية أو الركني الشرعي للجريمة وجود نص يجرم الفعل ويقدر عقوبته قبل وقوعه، وعدم تمتع الفعل بسبب من أسباب الإباحة والركن الشرعي للجريمة هو النص الذي يجرم الفعل المرتكب والمنصوص عليه في قانون العقوبات، حيث ينص قانون العقوبات على أن لا جريمة ولا عقوبة ولا تدبير أمن إلا بنص وبالتالي فكل فعل غير مجرم في قانون العقوبات يعتبر فعل مباح حتى ولو أنكرته الأخلاق والعادات والأعراف[2].

1- المادة 01 من القانون 16-02، المرجع السابق.

2- بلعليات إبراهيم، أركان الجريمة وطرق إثباتها دار الخلدونية، ط 1 ,الجزائر، 2007، ص 94.

و عمد المشرع الجزائري على تحديد الركن الشرعي لظاهره الإرهاب والمتمثلة في النصوص القانونية التي تجرم كافه السلوكيات لهذه الظاهرة سواء في القانون عقوبات عامه وفي قوانين خاصة على ظاهره الإرهاب في قانون العقوبات في المواد 87 مكرر الى 87 مكرره 10 ولم يقف على تجريمه الإرهاب التقليدي بل تبارك الثغرة القانونية في سنة 2016 لمسايره التطورات الحاصلة في ارتكاب الجرائم باستعمال التكنولوجيا الحديثة من أنترنت ونظام المعلوماتية وما يسمى بتجريم الإرهاب الإلكتروني في القانون 16-02 الذي يتمم الأمر رقم 66-156 المتضمن قانون العقوبات بموجب المادة 87 مكرر 11 و 87 مكرر 12 في القسم الرابع مكرر من الفصل الأول في الكتاب الثالث تحت عنوان الجرائم الموصوفة بالأفعال الإرهابية والتخريبية[1].

كما عملت على تجفيف منابع تمويل إرهابيين من خلال القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها[2], المعدل والمتمم بالقانون رقم: 15 -06 ولم يكتفي بهذا القدر بل استحدث بموجب قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكرس من خلاله تدابير وقائية لمنع وقوع الجريمة وآليات خاصه لمكافحه ومتابعه هذه الظاهرة بالإضافة الى الإجراءات العامة الواردة في قانون الإجراءات الجزائية المستخدمة في كشف الجريمة والجمع أدلتها, كما نجد القانون رقم 04-15 المتضمن تعديل قانون العقوبات المتعلقة أساسا بالمساس بأنظمة المعالجة الآلية للمعطيات الواردة في المواد 394 مكرر الى غايه مكرر7 نلاحظ أن المشرع الجزائري لم ينص صراحه في هذه المواد على جريمة الإرهاب الإلكتروني ولكن يفهم ضمنيا بأنه اعتبرها جريمة معلوماتية.

---

1 – المواد من 87 مكرر الى 87 مكرر 12 من القانون 16-02، المرجع السابق.

2-الأمر رقم 12-02، مؤرخ في 13 فبراير 2012، يعدل ويتمم القانون رقم 05-01، المؤرخ في 27 ذي الحجة عام 1425 الموافق 6 فبراير سنة 2005، والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية عدد 8 صادرة في 15 فبراير، 2012.

الفرع الثاني: العقوبات المقررة لجريمة الإرهاب الإلكتروني وفقا للقانون رقم 16 – 02

تترتب على جريمة الإرهاب الإلكتروني مجموعة من الآثار منها توقيع العقوبة على مرتكبيها، وبتحليل مواد قانون رقم 16 – 01 المتمم لقانون العقوبات يتبين أنّ العقوبات المقررة لجرائم الإرهاب الإلكترونية تتراوح ما بين العقوبات السالبة للحرية والغرامة المالية، وهذا ما سنراه من خلال هذه الفقرة في الآتي:

أولا: السجن المؤقت

كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الأعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، و كل من يوفر أو يجمع عمدا 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 إرهابية أو تدبيرها أو الأعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، وكل من قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي تدريب عليها أو تسهيل ذلك السفر، وكان ارتكاب الأفعال المذكورة باستخدام تكنولوجيات الإعلام والاتصال لارتكاب الأفعال السالفة الذكر، بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات، وهو ما نصت عليه المادة 87 مكرر 11 من القانون 16 – 02 .

ويعاقب بنفس العقوبة مستخدم تكنولوجيات الإعلام والاتصال من أجل تجنيد الأشخاص 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، وهو ما نص عليه المشرع الجزائري بموجب المادة 87 مكرر 12 من القانون رقم 16 – 02 .[1]

1- المواد 87 مكرر الى 87 مكرر 12، المرجع السابق.

ثانيا: عقوبة الحبس

يمكن التوقيع بصدد جرائم الإرهاب الإلكتروني بعقوبة الحبس وهي عقوبة مقررة لمقدمي خدمات الأنترنيت، حيث عرفت المادة **2** فقرة د من القانون رقم 09 – 04 مقدمو خدمات الأنترنيت على أنّهم أي كيان كان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها [1].

فمقدم خدمات الأنترنيت الّذي لا يقوم رغم اعذراه من الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، أو صدور أمر، أو حكم قضائي بالتدخل الفوري بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها، أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن قانونا، يعاقب بالحبس من سنة إلى ثلاثة سنوات[2].

ثالثا: الغرامة المالية

إضافة إلى توقيع العقوبة على الشخص المرتكب لجريمة الإرهاب الإلكتروني بسلب حريته بالحكم عليه بالسجن المؤقت والحبس المؤقت، يمكن علاوة على ذلك أن يقوم القاضي بالحكم على المجني بغرامة مالية تتراوح بين 100.000 دج إلى 5000.000 دج ، وهذه العقوبة توقع على كل جزائري أو أي شخص أجنبي مقيم بالجزائر سواء بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد 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 إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي تدريب عليها

1- القانون رقم 09 – 04، مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ع.47 مؤرخة في 25 شعبان 1430هـ، الموافق 16 غشت 2009 م.

2- المادة 394 مكرر 8 من القانون رقم 16 – 02، المرجع السابق.

أو تسهيل السفر من أجل القيام بها، كما تطبق على كل من يوفر أو يجمع عمدا 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 إرهابية أو الإعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تدبيرها أو المشاركة فيها، وعلى كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص 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"[1].

وقد تكون العقوبة المالية تتراوح من 2.000.000 دج إلى 10.000.000 دج، وتطبق هذه العقوبة على مقدمي خدمات الأنترنيت الذين يمتنعون عن القيام بالتدخل الفوري بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو الامتناع عن وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن رغم اعذراهم من طرف الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، أو صدور أمر أو حكم قضائي يلزمه بذلك وهو ما نصت عليه المادة 394 مكرر 8 من القانون رقم 16 – 02 [2].

1- المادة 87 مكرر 11، المرجع السابق.

2- المادة 394 مكرر 8، المرجع السابق.

المطلب الثاني: الركن المادي لجريمة الإرهاب الإلكتروني

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

1- السلوك الإجرامي من المجرم.

2- النتيجة الإجرامية المتحققة في العالم الخارجي.

3- العلاقة السببية بين المجرم والنتيجة التي حصلت[1].

الفرع الأول: السلوك الإجرامي

هو ذلك النشاط الذي الصادر من الجاني بصفه اختيارية ويحدث اثر في العالم الخارجي ويعاقب عليه القانون وهو نوعان: أما سلبي أو سلوك إيجابي، فالأول يتحقق في حاله الامتناع عن الفعل أو قول يأمر عليه القانون, أما الثاني هو القيام بفعل يجرمه القانون ويؤدي الى إحداث نتيجة في الجرائم ذات النتيجة وكذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية ولا يعتد القانون بالوسيلة المستعملة سواء كانت ماديه أو معنويه في ارتكاب سلوك الإجرامي بما أن المشارع الجزائري جرم فعل الإرهاب الإلكتروني في نص المادتين 87 مكرر 11 و 87 مكرر 12, ومن هاتين المادتين يمكن استخلاص السلوكيات الإجرامية المكونة للركن المادي لهذه الجريمة [2].

1- خلفيه عبد الرحمن، محاضرات في القانون الجنائي العام، دار الهدى، عين مليلة، الجزائر, 2012, ص 101-102.

2- منصور رحماني، الوجيز في قانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006، ص 98 99.

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

تنص المادة 87 مكرر 11 ...كل جزائري وأجنبي مقيم بالجزائر، بطريقه شرعيه أو غير شرعيه، يسافر أو يحاول السفر من دوله لأخرى بغرض ارتكاب أفعال إرهابية أو تدريبها أو الإعداد له أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

ويعقب بنفس العقوبة كل من:

– يوفر صوت جمع عمدا أموالا باي وسيله وبصوره مباشره أو غير مباشره بقصد استخدامها أو علم بانها ستستخدم في تمويل سفر أشخاص الى دوله أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة.

– كل من قام عمدا بتمويه أو تنظيم سفر أشخاص الى دوله أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر.

– يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في المادة 87 مكرر من الأمر رقم 66/ 156 متضمن قانون العقوبات المعدل والمتمم[1] .

ومن خلال هذه المادة نجد أن المشرع الجزائري جرم جمله من الأفعال وتتمثل في:

1– فعل السفر لغرض إرهابي باستخدام تكنولوجيا الإعلام والاتصال:

من خلال قراءتنا للمادة نجد أنها تجرم فعل السفر على الجزائريين والأجانب المقيمين بالجزائر بصفه شرعيه أو غير شرعيه إذا كان الهدف منه القيام بعمليات إرهابية أو التدريب عليها أو الإعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها، باستخدام تكنولوجيا الإعلام لارتكاب الأفعال الإرهابية.

1– المادة 87 مكرر 11، المرجع السابق.

2- فعل التمويل باستخدام تكنولوجيا الإعلام والاتصال

تجرم الفقرة الثانية من نص المادة 87 مكرر 11 السالفة الذكر فعل التمويل ويظهر من خلال مصطلح: يوفر أو يجمع عمدا أموالا وقام عمدا بتمويل وقد عرف المشرع الجزائري فعل التمويل بموجب قانون 15/ 06 المتعلق بالوقاية من تبويض الأموال وتمويل الإرهاب ومكافحتهما في نص المادة 3 منه : كل فعل يقوم به كل شخص بأية وسيله كانت مباشره أو غير مباشره وبشكل غير مشروع وبإرادة الفاعل من خلال تقديم أو جمع أموال بنيه استخدامها كليا أو جزئيا من اجل ارتكاب الجرائم الموصوفة بأفعال إرهابية أو تخريبيه المنصوص والمعاقب عليها بالمواد 87 مكرر الى 87 مكرر 10 من قانون العقوبات [1].

اشترط المشرع الجزائري استخدام تكنولوجيا الإعلام والاتصال للحصول على التمويل عن طريق إنشاء حسابات ومواقع الكرتونية خاصه بالتنظيمات الإرهابية والتي تتخذها كأداة لتوفير والجمع الأموال بصوره مباشره عن طريق اختراق الحسابات البنكية أو تحديد الأشخاص عبر البريد الإلكتروني وإجبارهم 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 الأموال والاتجار بالمخدرات والأسلحة وتزوير العملة أو اختطاف الرهائن وطلب فديه منهم أو السرقة واستغلالها لتمويل السفر أشخاص الى دول أخرى بغرض ارتكاب أعمال إرهابية .

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

تنص المادة 87 مكرر 12 من قانون العقوبات الجزائري على: كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابيين أو جمعيه أو تنظيم أو جماعه ومنظمه

1 - المادة 3 من القانون رقم 15- 06 المؤرخ في 15 فبراير 2015 المعدل والمتمم للقانون رقم 01-05المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم.

يكون غرضها أن تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصوره مباشرة أو غير مباشرة.

نص المشرع الجزائري في هذه المادة على فعل التجميل من خلال مصطلح تجنيد الأشخاص ويقصد به استقطاب أعضاء جدد بغرض إدخالها في التنظيمات والجماعات الإرهابية واستمراريتها فقد أصبح الإعلام الإلكتروني المنظر المفضل للتنظيمات الإرهابية لصيد أعضاء جدد وخاصه مع استخدام الفضاء السيبراني الذي يجعل التفاعل عابر للحدود الجغرافية، مما يسهل نقل المعلومات بين الأشخاص حول العالم[1].

ومنه تسهيل عمليه التجنيد وجذب اكبر عدد ممكن من الأشخاص, ويعتبر فئه الشباب المراهقين اكثر استهدافا في هذه العملية باعتبارهم الأكثر تواجدا في منصات التواصل الاجتماعي, كما ادركت التنظيمات الإرهابية أهمية هذه المواقع اعتبرتها الأداة العلمية والتكنولوجية المهمة لنشر أفكارها وتنفيذ مشروعها الأيديولوجي, سواء بصوره مباشره عن طريق تهديد والتر, أو استعمال القوه وإجبار مستخدمي الأنترنت للانضمام إليها, أو بصوره غير مباشره بأسلوب الترغيب والإغراء استماله المشاعر عن طريق التدعيم بالعواطف واستخدام عبارات حماسية عبر غرف الحوارات والدردشة[2].

ثالثا: الشرط الخاص المشترك في الركن المادي لجريمة الإرهاب الإلكتروني

لقد اشترط المشرع الجزائري من خلال نص المادتين 87 مكرر 11، 87 مكرر 12 انه في حالة وإذا تم ارتكاب هذه السلوكيات الإجرامية باستعمال وسيله المتماثلة في تكنولوجيا

---

1 –أماني مهدي توظيف التنظيمات الإرهابية لشبكات التواصل الاجتماعي في استقطاب الشباب "الاستراتيجيات وآليات المواجهة 2018 متاح على الرابط

cs.google.com/document/d/1y2xU5kTJaruolcwhk3o40nOYEkAQG1_Qc9QIOTkiVKI/edit

تم الاطلاع عليه يوم 2023/04/02 على الساعة 22:20.

2– سامي علي حامد عياد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية, 2007, ص 62.

الإعلام الاتصال نكون أمام جريمة الإرهاب وإذا تم ارتكابها دون هذه الوسيلة نكون أمام جريمة إرهاب تقليديه، فهذه الوسيلة تعتبر العنصر المشترك بين المادتين السالفتين الذكر كونها شرط جوهري ومهم لاعتبار جريمة الإرهاب جريمة الكرتونية.

الفرع الثاني: النتيجة الجرمية في جريمة الإرهاب الإلكتروني

يقصد بها الأثر الطبيعي المترتب على السلوك الإجرامي، والذي يحدث تغييرا في العالم الخارجي سواء كان ماديا أو معنوي، وليس لكل جريمة نتيجة فهناك جرائم يقوم ركنها المادي على السلوك المجرد بغض النظر عن النتيجة.

جريمة الإرهاب الإلكتروني تأخذ حكم الجريمة المعلوماتية فهي بذلك تعد من الجرائم الشكلية الذي يفترض فيها الضرر مستقبلا المتمثل في نتيجتها الجرمية، فبمجرد استخدام تكنولوجيا الإعلام الاتصال والقيام بالسلوكيات الواردة في نص المادتين 87 مكرر 11 و87 مكرره 12 من قانون العقوبات الجزائري[1] من فعل السفر أو تمويل أو تجنيد لأغراض إرهابية تقوم الجريمة حتى وان لم تتحقق هذه الأفعال كونها جريمة خطر وليست ضرر وذلك بالنظر الى الوسيلة المعتمدة عليها في تنفيذ هذا السلوك الإجرامي.

الفرع الثالث: العلاقة السببية في جريمة الإرهاب الإلكتروني

العلاقة السببية هي الرابطة التي تصل بين السلوك والنتيجة فاذا انقطعت العلاقة السببية انتفت المسؤولية الجنائية باعتبارها احد عناصر الركن المادي, وتقتصر على فئه واحده من الجرائم وهي الجرائم ذات النتيجة أو جرائم المادية بينما تستثنى الجرائم الشكلية من هذه العلاقة, كون لا يدخل في ركنها المادي ضرورة توافر نتيجة إجرامية معينه وعدم وجود نتيجة للفعل بطبيعته لا يترك محلا للبحث عن العلاقة السببية وبما أن جريمة الإرهاب الإلكتروني من جرائم الشكلية فانه لا يثور في شانها العلاقة السببية حيث لم يستلزم المشرع في نموذجها الإجرامي تحقيق النتيجة الجرمية لقيام ركنها المادي, وبمجرد استخدام البيئة الافتراضية وإنشاء

1- المواد 87 مكرر 11 و87 مكرر 12 نفس المرجع السابق.

مواقع حسابيه واستخدام البريد الإلكتروني لتسهيل عمليه السفر أو تمويل منظمه إرهابية واستقطاب أشخاص الى الجماعات المسلحة من اجل ارتكاب أعمال إرهابية فهي تشكل جريمة تامه حتى وان لم تتحقق النتيجة أي عدم وصول المجرم الإرهابي الى تحقيق السلوكيات الواردة في نص المادتين 87 مكرر 11 و 87 مكرر 12 من قانون العقوبات الجزائري .

تعتبر جريمة الإرهاب الإلكتروني من جرائم الشكلية لا يمكن أن تكون موقوفة أو خائبة لأن الجرائم الشكلية تتحقق بمجرد البدء بتنفيذها ولا يشترط لحصول النتيجة فيها[1] .

المطلب الثالث: الركن المعنوي لجريمه الإرهاب الإلكتروني

الوقائع المادية في الجريمة لا تكفي وحدها لقيام الجريمة, لابد من وجود بعث نفسي يحمل المجرم للقيام بالسلوكيات الإجرامية والمعبر عنه بالركن المعنوي لأنه به تتحدد وتكتمل المسؤولية الجنائية للجاني العناصر النفسية لماديات الجريمة تأخذ صورتين إما اتجاه الجاني الى إتيان أفعال إرادية غير مشروعه مع إرادة هذا الأخير في تحقيق النتيجة الجرمية وهو ما يعني بالقصد الجنائي وفي هذه الحالة نكون أمام جريمة عمديه, إما في الصورة الثانية تتمثل في اتجاه الإرادة الى إتيان الفعل دون الرغبة في تحقيق النتيجة وهنا نكون أمام صوره الخطأ الغير العمدي وجريمة الإرهاب الإلكتروني من الجرائم التي لا يتصور فيها الخطأ فهي تعد من الجرائم العمدية, ونجد أن المشرع أورد في المادة 87 مكرر 11 قانون عقوبات الجزائري[2] عباره تفيد القصد العمدي لهذه الجريمة من خلال العبارة التالية يوفر أو يجمع عمدا, قام عمدا وهذه العبارة تؤكد عدم تصور الخطأ في جريمة الإرهاب الإلكتروني .

الفرع الأول: القصد الجنائي العام

القصد العام يتمثل في انطلاق إرادة الجاني نحو القيام بفعل وهو يعلم أن القانون ينهي عنه ويتمثل القصد الجنائي في العام في جريمة الإرهاب الإلكتروني في علم الجاني أو المجرم

1- خلفيه عبد الرحمن، محاضرات في القانون الجنائي العام، دار الهدى، عين مليله، الجزائر, 2012, ص 101-102.

2- المادة 87 مكرر 11 من الأمر رقم66 156 المرجع السابق.

بارتكاب سلوك مجرم قانو المتمثل في التجنيد والسفر والتمويل باستعمال وسائل التكنولوجيا الإعلام والاتصال مع اتجاه إرادة الى استخدام هذه الوسيلة لتنفيذ الجريمة لأغراض إرهابية[1].

الفرع الثاني: القصد الجنائي الخاص

القصد الجنائي الخاص حيث يتمثل في الغاية التي يقصدها الجني من ارتكاز الجريمة فضلا عن إرادته الواعية لمخالفه القانون الجزائري وهكذا يشترط القانون بالإضافة الى القصد العام المتمثل في إرادة الجاني الواعية مخالفه القانون، إما نية إزهاق الروح كما في جريمة قتل عند المنصور المعاقب عليها بالمادة 254 من قانون العقوبات الجزائري[2].

القصد الخاص في جريمة الإرهاب الإلكتروني هو الغاية أو الغرض الذي يرمي إليه الجاني من ارتكاب السلوكيات السالفة الذكر باستخدام وسيله مستحدثه المتمثلة في وسائل التكنولوجيا الإعلام والاتصال لارتكاب الأفعال الإرهابية ونص المشرع الجزائري على الأفعال التي تعد إرهابا في نص المادة 87 مكرر والتي تستهدف امن الدولة واستقرارها وتتمثل في:

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص وتعريف حياتهم أو حريتهم أو امنهم للخطر أو المساس بممتلكاتهم.
- عرقله حركه المرور وحريه التنقل في الطرق والتجمهر والاعتصام في الساحات العمومية والاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور.
- الاعتداء على وسائل مواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.
- الاعتداء على المحيط وإدخال ماده أو تسريبها في الجو أو باطن الأرض أو إلقائها. عليها أو في المياه بما فيه المياه الإقليمية من شانها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.

---

1 –أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 7، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2008 ص 109.

2– أحسن بوسقيعة، نفس المرجع ص 110.

- عرقله عمل السلطات العمومية أو حريه ممارسه العبادات والحريات العامة وسير المؤسسات المساعدة للمرفق العام.
- عرقله سير المؤسسات العمومية أو الاعتداء على حياه أعوانها وممتلكاتهم أو عرقله تطبيق القوانين والتنظيمات.
- تحويل الطائرات أو السفن أو أي وسيله أخرى من وسائل النقل.
- إتلاف منشئات الملاحة الجوية أو البحرية أو البرية.
- تخريب أو إتلاف وسائل الاتصال.
- احتجاز الرهائن.
- الاعتداء باستعمال المتفجرات أو المواد البيولوجية أو الكيمياوية أو النووية أو المشعة
- تمويل إرهابي أو منظمه إرهابية[1].

1- المادة 87 مكرر المرجع السابق.

ملخص الفصل:

الإرهاب من المصطلحات التي كثر الخلاف في بيان معناها وتحديد مدلولها، علما بأنها من أكثر الكلمات استخداما في متخلف وسائل الإعلام العالمية في السنوات الأخيرة، ورغم ذلك فانه لم تتفق كلمة الباحثين على التعريف الدقيق والمحدد لهذا المصطلح بالنظر لطبيعة الأعمال الإرهابية واختلاف وجهات النظر لمثل هذه الأعمال لذلك قمنا في هذا الفصل باستعراض جريمة الإرهاب الإلكتروني، بدء من التعريف والتعرف على أهم الخصائص التي يتميز بها والأهداف التي يسمو إليها وكذلك مظاهر وأركان جريمة الإرهاب الإلكتروني.

الفصل الثاني:

مكافحة جريمة الإرهاب الإلكتروني

التقدم الهائل في المجال التكنولوجي وما يشهده العالم من قفزات نوعية في شتى المجالات ما جعل الأنترنيت تساهم و بشكل كبير في انتشار الجريمة بسرعة كبيرة الأمر الذي يصعب مواجهته نظرا لتداخل القوانين و احتكام كل دولة إلى اختصاصها القانوني كان لازما على الدول التكاتف من اجل مكافحة هذه الجريمة و ذلك عن طريق إبرام اتفاقيات و معاهدات فيما بينها للمساعدة على مكافحة جريمة الإرهاب الإلكتروني, الأمر الذي أدى بالتشريعات الحديثة إلى مواكبة التطورات و السعي إلى سن قوانين من شانها مكافحة هذه الجريمة واسعة الانتشار, كما تهدف أيضا إلى حماية الفضاء الإلكتروني من التهديدات الإرهابية في هذا المجال .

وعليه قد تم تخصيص هذا الفصل للحديث عن آليات مكافحة جريمة الإرهاب الإلكتروني على الصعيد الدولي والإقليمي والوطني وكذلك الهيئات الخاصة بمكافحة الإرهاب الإلكتروني.

المبحث الأول: آليات مكافحة جريمة الإرهاب الإلكتروني

تتعدد الآليات وطرق مكافحة الإرهاب الإلكتروني على المستويات الدولية والإقليمية وكذلك الوطنية باعتبار أن هذه الظاهرة تعد سلوك إجرامي مرتكب لأسباب مختلفة منها سياسية اقتصادية أو اجتماعية ضد النظام ألمعلوماتي بأنواعه لتحقيق أغراض إرهابية تنطوي على العنف أو التهديد أو الاستغلال الذي يهدف حياة الأشخاص وسلامتهم وزرع الخوف وتعطيل الأداء الطبيعي أنظم السيطرة والرقابة الإلكترونية[1].

ومع رغبة المشرع الجزائري في توفير الحماية القانونية ضد هذا النوع من الجرائم ومحاولة التصدي لها ومواجهتها وتدارك الفراغ التشريعي القائم في هذا المجال بحيث عمل على تعديل العديد من القوانين وعلى رأسها قانون العقوبات لجعله يتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال وكذلك صدور قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات جديدة خاصة بمكافحة هذه الظاهرة [2].

المطلب الأول: الجهود الدولية لمكافحة جريمة الإرهاب الإلكتروني

تعاني الدول والمجتمعات من ظاهرة الإرهاب الإلكتروني حتى أصبح من أكبر المشاكل في العصر الحديث ذلك لما يشكله من خطر كبير على الشعوب والدول مما فرض عليها وعلى المنظمات الدولية الاتفاق على مواجهته والقضاء عليه نظرا للخطورة الكبيرة التي يتسبب بها.

1- الطاهر بن يحيى ناعوس، مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية دون طبعة، دون سنة نشر، ص 52.

2- الأمر رقم 09-04، المرجع السابق.

الفرع الأول: مكافحة الإرهاب الإلكتروني في المنظمات الدولية

- **أولا: منظمة الأمم المتحدة**

بذلت هيئة الأمم المتحدة جهودا كبيرة في سبيل العمل على مكافحة جرائم الإرهاب الإلكتروني وذلك لما تسببه هذه الجرائم من خسائر اقتصادية، ومشاكل سياسية واجتماعية بالغة الخطورة وأن التصدي لهذا التهديد ومكافحته يتطلب استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به[1].

و لقد أصدرت الأمم المتحدة عدة قرارات عبر جمعيتها العامة في توضيح منها لتصاعد الاهتمام العالمي لاستخدام وسائل تكنولوجيا الإعلام و الاتصال بشكل غير سلمي ففي 22 نوفمبر 2002 تبنت قرارا بشان التطورات في ميدان المعلومات و الاتصالات السلكية و اللاسلكية في سياق الأمن الدولي و في ديسمبر من نفس السنة اتخذت قرار أخر بهدف إرساء ثقافة عالمية لأمن الفضاء الإلكتروني و اعتبر هذا القرار من بين أهم القرارات التي استهدفت العمل على حماية البنية التحتية للمعلومات ،وحث الدول و المنظمات الدولية على تكثيف جهود التعاون لمواجهة الإرهاب الإلكتروني[2] .

وفي سنة 2004، أشرف الأمين العام لمنظمة الأمم المتحدة آنذاك السيد "كوفي عنان" على تشكيل فريق دولي لدراسة قضية إدارة الأنترنيت والمخاطر الناجمة عنها وفي نفس الوقت قام بإنشاء مجموعة الخبراء الحكومية والتي ترمي إلى مناقشة الأخطار القائمة والمحتملة في المجال الأمني المعلوماتي الدولي والإجراءات اللازمة والممكنة لوضع أسس دولية تهدف إلى تقوية امن نظام الاتصالات والمعلومات العالمية [3].

1- عواطف عثمان، محمد عبد الحليم، جرائم معلوماتية، مجلة العدل، العدد 24، ص، 69.

2- شفيق نوران أثر، التهديدات الإلكترونية على العلاقات الدولية، ط1, المكتب العربي للمعارف، القاهرة، مصر, 2015 ص 108.

3- بوحادة سارة، أثر الإرهاب الإلكتروني على امن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية، الجزائر ص 15.

ولقد توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب وأشار القرار إلى أن الإجراء الدولي لمواجهة الجرائم الإلكترونية بين الدول الأعضاء ويتمثل في:

1- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من اجل ضمان تطبيق القوانين الجنائية الراهنة، على نحو ملائم وإدخال التعديلات إذا دعت الضرورة.

2- مصادرة العائد والأصول من الأنشطة غير المشروعة.

3-اتخاذ تدابير الأمن والرقابة مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

4-رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذه الجرائم ومحاكمة مرتكبيها.

5-التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمن مناهج مدرسية[1].

ودعت لجنة منع الجريمة والعدالة الجنائية التي عقدت اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية من اجل دراسة شاملة للجريمة السيبرانية بالتطرق إلى المواضيع التالية:

1- جمع المعلومات والإحصائيات المتعلقة بالإرهاب الإلكتروني وتحدياته.

2- مدى فعالية التشريعات للظاهرة الإرهابية الإلكترونية.

3- إجراء التحقيق.

4- التعاون الدولي.

5- الأدلة الإلكترونية.

6- مسؤولية متعهدي خدمات الأنترنيت.

7- التصدي للجريمة خارج دائرة التدابير القانونية.

8- المساعدة التقنية الدولية.

9- دور القطاع الخاص في الحد من الجريمة.

1- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، رسالة دكتوراه في القانون في القانون، الجامعة الإسلامية، كلية الحقوق، ص 186.

وعملت منظمة الأمم المتحدة في إطار استمرار الجهود المبذولة لمكافحة الإرهاب الإلكتروني، من خلال محاربة جرائم الكمبيوتر والأنترنيت، وهذا من خلال ثلاث اتجاهات رئيسية وهي كالتالي:

- **حماية البيانات الشخصية:** وهو حماية الخصوصية المعلوماتية وكل البيانات الشخصية من مخاطر التلف، التزوير، القرصنة، الاستعمال، الحذف، التشويه، وهذا يعتبر أيضا حماية لحقوق الإنسان.
- **حماية الملكية الفكرية للمصنفات الرقمية:** وهو حماية البرمجيات وقواعد البيانات والدوائر المتكاملة وعناصر مواقع الأنترنيت في الوقت الحاضر.
- **حماية استخدام الكمبيوتر والأنترنيت:** وهو من الأنشطة التي تستهدف المعلومات ونظامها وأداء الكمبيوترات ووظائفها وأداء الشبكات وهي نفسها جرائم الكمبيوتر والأنترنيت، لهذا عملت الأمم المتحدة في ميدان تطوير التشريعات الجنائية وبحث الظواهر الجديدة في ميدان الأنترنيت.

ثانيا: المنظمة العالمية للملكية الفكرية

تم التوقيع على الاتفاقية المنشئة في ستوكهولم سنة 1967 وأصبحت تابعة للأمم المتحدة من سنة 1974، تشجع هذه المنظمة على توقيع معاهدات دولية جديدة و التنسيق بين التشريعات القومية و تقديم المساعدات القانونية للدول النامية بهدف حماية الملكية الفكرية و تنميتها و مع تزايد حاجة المنظمة على غرار باقي المنظمات لحماية البرامج شكلت مجموعة عمل تضم عددا من الخبراء بهدف برامج الحواسيب من التهديد أو الهجوم الإلكتروني ، حيث أفضى بعد ذلك سلسلة من الاجتماعات إلى انتهاج اغلب الدول و الميل إلى برامج الحاسوب لقوانين حماية المؤلف[1].

1- طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، مصر ،2006، ص 214.

ثالثا: الاتحاد الدولي للاتصالات

تم إنشاءه بمقتضى اتفاقية باريس سنة 1865 باسم "اتحاد التلغراف الدولي" ثم تم تعديله وأصبح اسمه الاتحاد الدولي للسلكية واللاسلكية عام 1947 يعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى على وضع المعايير المتعلقة بالأمن ألمعلوماتي ومكافحة الإجرام والإرهاب الإلكتروني، وإذ يقوم بالاشتراك مع الوكالة الأوروبية لأمن الشبكات و المعلومات بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات[1] .

رابعا: الولايات المتحدة الأمريكية

تعد الولايات المتحدة من الدول السباقة في محاربة ظاهرة الإرهاب بالوسائل الإلكترونية من خلال قوانينها الوطنية أو من خلال سعيها لعقد اتفاقيات دولية بهذا الخصوص أو من خلال إنشاء الأجهزة المختصة بمكافحة الإرهاب بالوسائل الإلكترونية حيث تميزت الإستراتيجية الأمريكية لمكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة وانصبت هذه الاستراتيجيات في بادئ الأمر على المجال العسكري حيث عمد البنتاغون سنة 2005: إلى إنشاء وحدة عسكرية متخصصة عهد إليها بمهمة تحصين الفضاء المعلوماتي الأمريكي وتأمين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة وتعد الولايات المتحدة الأمريكية من أولى الدول التي أصدرت قوانين لمكافحة الإرهاب الإلكتروني وتعمل الحكومة الفيديرالية الأمريكية جاهدة على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث تحاول تقنين استخدام محرك البحث YAHOO-GOOGLE-MSN في مجموعة من الشركات.

وهناك خطوات عديدة اتخذتها الولايات المتحدة لمكافحة الجريمة والإرهاب الإلكتروني منها:

- إصدار قانون تعزيز أمن المعلومات.
- وضع الإستراتيجية الوطنية لتأمين الفضاء الإلكتروني.

1- الشافعي نوري رشيد، وسامر مؤيد عبد اللطيف، ومنى محمد عبد الرزاق، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مجلة رسالة الحقوق، المجلد 10، العدد 02، جامعة كربلاء، كلية القانون، العراق، 2018، ص 20.

- أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الإلكتروني.
- كما تم إنشاء لجنة حماية البنية التحتية الحساسة في الولايات المتحدة والتي أسست مجموعة خاصة تتناول جوانب الإرهاب الإلكتروني وأطلقت عليها اسم: مركز حرب المعلومات.
- كما تم إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات وبرنامج وغيرها من المبادرات[1].

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات القارية

في شهر أكتوبر من سنة 1999اجتمع في موسكو وزراء العدل و الداخلية للدول الثمانية الكبار(الو م أ ،اليابان ،ألمانيا ،روسيا ،إيطاليا ،المملكة المتحدة ،فرنسا و كندا)[2] و طلبوا من ممثليهم وضع خيارات و حلول عملية تسمح بكشف و متابعة الاتصالات الإلكترونية الدولية في إطار التحقيقات الجنائية .وقد صدر عنهم التصريح التالي : بغية التأكد من أننا جميعا نستطيع أن نحدد مكان و هوية المجرمين الذين يستخدمون الاتصالات الإلكترونية لأهداف مشروعة، لذلك يجب أن يتعاون الجميع مباشرة من اجل مكافحتها و إيجاد حلول سريعة و حديثة[3] .

وفي شهر أفريل من سنة 2000 تم توقيع اتفاقية منظمة مكافحة الفساد إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية بإشراف منظمة الأمم المتحدة والتي نصت في مادتها

---

1 – صباح كزيز، أمال كزيز، الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث رقم 01 ،العدد 08 2008 ص 03.

2– مجموعة الثمانية G08 تضم الدول الصناعية الكبرى في العالم وهم (الو م أ، اليابان ألمانيا، روسيا، إيطاليا، المملكة المتحدة، فرنسا وكندا).

3– وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة المنار، تونس 2014 ،ص 204.

الأولى على أنه: ينبغي أن تكفل عدم توفر قوانينها وممارستها ملاذا آمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية[1].

كما توجت الجهود التي بذلها الاتحاد الأوروبي والمجلس الأوروبي بصدور اتفاقية بودابست لمكافحة جرائم المعلوماتية (الجرائم الإلكترونية) وتعرف بالاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية. ووضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في 2001/11/23 وأصبحت حيز التنفيذ سنة 2004، وتعتبر الاتفاقية متاحة أمام أي دولة من دول العالم للانضمام إليها.

واشتملت الاتفاقية على 48 مادة وفي إطار التعاون نصت الاتفاقية على أن تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم "[2].

وعقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل ما بين 12-19 أفريل 2010 حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات الجنائية في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك جرائم الحاسوب حيث احتل هذا النوع من الجرائم موقعا بارزا على جدول أعمال المؤتمر وذلك لخطورتها والتحديات التي تشكلها[3].

وفي إعلان قمة شيكاغو في اجتماع مجلس شمال الأطلس في 20 ماي 2012 تم التأكيد على ضرورة دمج إجراءات الدفاع الإلكتروني في هياكل وإجراءات الحلف مع الالتزام بتحديد وتوفير قدرات الدفاع الإلكتروني الوطنية التي تعزز التعاون والعمليات المشتركة بين دول

1- مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا من 10 إلى 18 أفريل 2000.

2 - اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

3- صغير يوسف، الجريمة المرتكبة عبر الأنترنيت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر 2013 ص 94.

الحلف، بالإضافة إلى تطوير قدرات الدول الأعضاء بصورة أكثر لمنع الهجمات الإلكترونية واكتشافها والتصدي لها ومعالجة التهديدات الأمنية الإلكترونية[1].

المطلب الثاني: الجهود الإقليمية لمكافحة جريمة الإرهاب الإلكتروني

بالرغم من كل المواجهات التي آلت إليها الجهود الدولية لمكافحة هذه الظاهرة إلا أنها غير كافية إذ تم الاعتماد عليها فقط وعليه فانه لابد من توسيع دائرة المكافحة من الدولية إلى الإقليمية وذلك لحصر الظاهرة الإجرامية ذلك ما يزيد من فرصة القضاء عليها والحد منها.

الفرع الأول: دور الاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني

أصر الاتحاد الأوروبي على إطلاق مجموعة من التوصيات في ميدان استخدام تكنولوجيا و حماية الشبكة العنكبوتية و في هذا الصدد وقع الاتحاد الأوروبي على اتفاقية تهدف إلى حماية الأشخاص في إطار مواجهة الجرائم المتعلقة بسرقة الأسرار و الغش الرقمي كما اصدر في نفس السياق مجموعة من القواعد التوجيهية على غرار باقي الجهود التي تمثلت في معاهدة أوروبا والتي تختص بحماية الأشخاص من مخاطر التكنولوجيا سنة 1980 هذا وقد عمل الاتحاد الأوروبي إلى إصدار اتفاقية شاملة في سترازبورغ المتعلقة بجرائم الحاسوب والتي دعت بدورها إلى ضرورة حماية المجتمع من الهجمات السيبرانية و وضع الاستراتيجيات اللازمة لمجابهتها و كذا التشريعات الضرورية في سبيل تحقيق ذلك[2].

و سعيا إلى ضمان حماية امثل لاستخدامات التكنولوجيا و توفير الأمن قد تم إنشاء الشبكة الأوروبية للأمن و امن المعلومات ENISA (THE EUROPEAN AGENCY FOR CYBERSECURITY) سنة 2004 و يشمل هيكلها مجموعة من ضباط الاتصال التابعيين للدول الأعضاء، و كذا مجموعة من الممثلين الدائمين لهذه الدول و التي أقرت بدورها عددا من الوثائق الأساسية لمكافحة الإرهاب الإلكتروني و كذا وضع مشروع الإستراتيجية الوطنية

1- وليد الكشباطي، المرجع السابق ص 206.

2- عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، مصر، 2008، ص 168.

للأمن الرقمي داخل الاتحاد الأوروبي بالإضافة إلى تصميم مجموعة عالمية تحتوي على أهم التدريبات في سبيل تحقيق الأمن السيبراني[1].

الفرع الثاني: الجهود العربية في مكافحة الإرهاب الإلكتروني

قطعت العديد من الدول العربية شوطا كبيرا في مجال حفظ الأمن السيبراني ومواجهة المخاطر المحققة للإرهاب الإلكتروني والتي باتت تهدد فعليا أمنها وفي هذا الصدد يمكن الإشارة إلى الجهود المبذولة من قبل بعض الدول العربية حيث تختلف سياسات وتشريعات المواجهة من دولة لأخرى:

مصر: تعد مصر واحدة من أكثر الدول العربية عرضة لخطر الإرهاب الإلكتروني وهذا وفقا للإحصائيات والأرقام، فبحسب مؤشر الجاهزية للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات عام 2018 احتلت مصر المرتبة 23 ما بين 155 دولة شملها المؤشر كما جاء في تقرير نشرته شركة " ترند مايكرو" فان مصر جاءت في المرتبة الأولى في قارة إفريقيا عام 2018 من حث تعرضها للهجمات الإلكترونية على مستوى قطاعاتها الصناعية بالدرجة الأولى، كذلك محاولة اختراق الأنظمة المصرفية والأسواق المالية.

وقد شرعت الدولة المصرية بمختلف مؤسساتها في اتخاذ الإجراءات والتدابير اللازمة لخلق بيئة سيبرانية آمنة داخل الدولة، ومن أبرز هذه الجهود، تشكيل هيئات وطنية للأمن السيبراني ومكافحة الإرهاب الإلكتروني مثل: "المركز الوطني للاستجابة لطوارئ الحاسب الآلي" (سيرت) في عام 2009، ويستهدف حماية البنية التحتية لتكنولوجيا المعلومات وقد نجح هذا المركز بالفعل منذ عام 2012 في تقديم الدعم الفني لمختلف المؤسسات بالدولة والقطاعات

1- ناصر العلجة، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، العدد الأول، 2018، ص 39.

لمواجهة الأخطار السيبرانية بما فيها المساعدة على مواجهة خطر الهجمات الإرهابية السيبرانية [1].

كما أصدر رئيس مجلس الوزراء السابق" إبراهيم محلب" قرارًا بتأسيس "المجلس الأعلى للأمن السيبراني" في 16 ديسمبر 2014، ويرأسه وزير الاتصالات، ويهدف المجلس إلى وضع خطط إستراتيجية للتصدي للهجمات الإلكترونية، فضلًا عن الإشراف على كيفية تنفيذ تلك الإستراتيجية وتحديثها المستمر [2].

العراق : اتخذت الحكومة العراقية خطوات عدة لتفكيك البنية الاتصالية والإعلامية لأهم وأخطر التنظيمات الإرهابية وهو تنظيم "داعش"؛ إدراكًا منها بأن البدء بتفكيك البنية الاتصالية والإعلامية للتنظيم يشل حركته، ويفقده الاتصال بين قواته من جهة، وبين مراكز القيادة من جهة أخرى؛ حيث قامت الحكومة في يونيو 2014 بقطع الإنترنت وحجب مواقع التواصل مثل: (فيسبوك، وتويتر، ويوتيوب،وسكايب، وفيبر)؛ وذلك بسبب تأثير "داعش" على الساحة الإلكترونية، وعلى الرغم من أن أعضاء التنظيم وجدوا لهم مخرجًا بتحميل تطبيق آخر مخصص للتليفونات الذكية، إذ أعلن "داعش" عن كونه أول تنظيم جهادي يصمم تطبيقًا مجانيًّا يسمح بنشر التغريدات الخاصة به، لكن سرعان ما قام موقع جوجل بحذفه، بالإضافة إلى قيام إدارة تويتر بإغلاق عديد من الحسابات التي تدعم "داعش" وتروج له، حتى لو لم يتبنَّها التنظيم رسميا [3].

1- الجهود العربية لمواجهة مخاطر الإرهاب السيبراني الواقع والمأمول على الرابط التالي:

https://arabaffairsonline.com

تم الاطلاع عليه يوم 2023/04/05 على الساعة10:30.

2- المجلس الأعلى للأمن السيبراني"، رئاسة مجلس الوزراء المصري، ديسمبر 2014 على الرابط التالي :https://www.escc.gov.e

تم الاطلاع عليه يوم 2023/04/05 على الساعة12:00.

3- نورا بينداري عبد الحميد، دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية، دراسة حالة "داعش" المركز الديمقراطي العربي، 19 يوليو 2016، على الرابط التالي: https://www.democraticac.de

كما أكد وزير الخارجية العراقي "فؤاد حسين" في 20 نوفمبر 2021 أن العراق بصدد تبنّي إستراتيجية وطنية شاملة لمكافحة الإرهاب بما فيها "الإرهاب السيبراني" وعلى رأسها عصابات تنظيم "داعش" الإرهابي، ومنعه من التغلغل في أوساط المجتمع أو السيطرة على المدن [1].

دول مجلس التعاون الخليجي :قطعت دول مجلس التعاون الخليجي خلال السنوات الماضية شوطًا كبيرًا في مجال مكافحة الإرهاب السيبراني، فالإمارات قامت بإصدار قوانين وتشريعات لتجريم أي عناصر ترتبط بالتنظيمات الإرهابية ومن هذه القوانين مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، كما أسست الإمارات مركز "صواب" في مارس 2015، وهي مبادرة تفاعلية للتراسل الإلكتروني تهدف إلى دعم جهود التحالف الدولي في حربه ضد التطرف والإرهاب، ويتطلع المركز إلى إيصال أصوات الملايين من المسلمين وغير المسلمين في جميع أنحاء العالم ممن يرفضون ويقفون ضد الممارسات الإرهابية والأفكار الكاذبة والمضللة التي يروجها أفراد التنظيم، كما يعمل مركز "صواب" على تسخير وسائل الاتصال والإعلام الاجتماعي على شبكة الإنترنت من أجل تصويب الأفكار الخاطئة ووضعها في منظورها الصحيح[2] .

الفرع الثالث: الإتحاد الإفريقي للشرطة الجنائية "الأفريبول"

ترجع فكرة إنشاء آلية الاتحاد الإفريقي للتعاون الشرطي" أفر يبول " لسنة 2013 بمناسبة انعقاد المؤتمر الإقليمي الإفريقي الـ 22 للإنتربول وفي هذا الإطار قامت أفر يبول بعدة مساعي تصب جلها في إرساء أطر للتعاون مع المنظمات الأخرى لا سيما من خلال

1- العراق: تتبنى إستراتيجية وطنية شاملة لمكافحة الإرهاب"، أخبار اليوم، 20 نوفمبر 2021، على الرابط التالي:
https://www.m.akhbareyoum.com
تم الاطلاع عليه يوم 2023/04/06 على الساعة23:00.

2- مكافحة الإرهاب والتطرف"، وزارة الخارجية والتعاون الدولي بدولة الإمارات العربية المتحدة، 27 أغسطس 2021 على الرابط التالي:
https://www.mofaic.gov.ae/ar-ae/the-ministry/the-foreign-policy/combating-terrorism-and-extremism.
تم الاطلاع عليه يوم 2023/04/07 على الساعة10:00 .

الشروع في إبرام اتفاقات للتعاون مع أجهزة الشرطة الإقليمية والدولية مثل أنتربول وأمريبول هذه الاتفاقيات هي حاليا قيد الدراسة على مستوى المكتب القانوني الاتحاد الإفريقي تلتزم كل دولة عضو في آلية الافريبول بأن تنشئ وفقا لتشريعاتها الوطنية مكتبا للاتصال الوطني لضمان سلاسة وسير وتنفيذ أنشطة هذه الآلية وقد بلغ عدد هذه المكاتب المنشأة تقريبا أكثر من 30 مكتبا.

وتجدر الإشارة أن نظام الأساسي المنشئ لآلية الأفريبول قد أناطت باللجنة الفنية المتخصصة للدفاع والسلامة والأمن ومسؤولية توفير القيادة السياسية والتوجيه فيما يتعلق بشؤون الشرطة في إفريقيا[1].

المطلب الثالث: الجهود الوطنية لمكافحة جريمة الإرهاب الإلكتروني

تعتبر الجزائر من الدول التي عانت من ويلات الإرهاب سواء التقليدي أو الإلكتروني بجميع صوره ، و لقد عمدت الجزائر على غرار باقي الدول إلى السعي في بذل كافة الجهود لمكافحته حيث كثفت كل جهودها لتحقيق مساعيها حيث بدأت بالجانب التشريعي لما يلعبه من دور فعال في إثبات الجريمة الإلكترونية وسن القوانين الردعية التي تجرم الأفعال الماسة بالأنظمة المعلوماتية و كذا الإجراءات الجزائية لمكافحة الإرهاب الإلكتروني الذي أصبح خطرا يهدد الأمن السيبراني العالمي و الوطني، ولقد حاول المشرع الجزائري إصدار قوانين عامة و خاصة للتصدي للإرهاب الإلكتروني وهي من بين أهم الأمور التي أعطى لها المشرع الجزائري أهمية قصوى و ذلك للحفاظ على امن الدولة و الحفاظ على النظام العام .

الفرع الأول: آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات العامة

لقد أخص المشرع الجزائري تنظيم الجرائم الإلكترونية بقوانين عامة وخاصة وتتمثل فيما يلي:

أولا: الدستور الجزائري

1- شنتير خضرة، الآليات القانونية لمكافحة الإرهاب الإلكتروني، دراسة مقارنة، أطروحة دكتوراه، القانون الجنائي، كلية الحقوق، جامعة أحمد دراية، أدرار ،2020، ص 246.

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

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

ثانيا: قانون العقوبات

استدرك المشرع الجزائري الفراغ القانوني في مجال الجريمة الإلكترونية لذلك خصص القسم السابع مكرر من القانون 04-15 المتضمن تعديل قانون العقوبات، للمساس بأنظمة المعالجة الآلية للمعطيات و تضمن 08 مواد إذ أقرت المادة 394 مكرر بمعاقبة كل من يدخل أو يبقى عن طريق في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، أما المادة 394 مكرر 1 فنصت على معاقبة كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها، و نصت 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 الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم الأول.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

1- القانون رقم 16-01 المؤرخ في 06 مارس 2016، المتضمن التعديل الدستوري، الجريدة الرسمية عدد 14، المؤرخة في 07 مارس 2016.

أما المادة 394 مكرر 3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم إذ استهدفت جريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات اشد وفي المادة 394 مكرر 4 شدد المشرع على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة مالية تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

وفي سنة2009صدر القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وطرق مكافحتها.

ثالثا: قانون الإجراءات الجزائية

تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والشهادة والخبرة.

إن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية ، و نص على التفتيش في المادة: 45 الفقرة 7 من نفس القانون المعدلة حيث اعتبر التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية و الموضوعية ، فالتفتيش و إن كان إجراء من إجراءات التحقيق، قد أحاطه المشرع بقواعد صارمة و بالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية و نص كذلك على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 و كذا على" اعتراض المراسلات وتسجيل الأصوات و التقاط الصور من المادة 65 مكرر 5[1].

1- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية، طرابلس 24-25 مارس، 2017، ص 130.

لقد أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للجريمة الإلكترونية لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شانها أن تتفادى وقوع الجريمة أو على الأقل الكشف المبكر لها يسمح بتدارك مخاطرها وهو ما استدركه المشرع بتضمين القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية تدابير إجراءات مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها وتسريبها.

ويقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين الاستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء إلى هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو التالي:" إذ اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .... يجوز لوكيل الجمهورية المختص أن يأذن:

- باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص ".[1]

فموجب هذه المادة إن المشرع الجزائري هنا يسمح لسلطات التحقيق و الاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها ،أو التحقيق في الجريمة الإلكترونية ، أو اللجوء إلى إجراء اعتراض المراسلات السلكية و اللاسلكية و تسجيل المحادثات و الأصوات و التقاط الصور و كذلك الاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف

1- المادة، 65 مكرر 5 ،المرجع السابق.

عن ملابسات الجريمة و إثباتها دون التقيد بقواعد التفتيش و الضبط المألوفة مع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال و التحري و تصون الحقوق و الحريات العامة و الحياة الخاصة للأفراد[1].

رابعا: القانون المدني الجزائري

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع الجزائري ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري:" كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض."

وقد جاء هذا النص عاما وشاملا لأي اعتدا ء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة وقد أورد هذا النص مبدأ مهما هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض " فالفعل الضار هو أساس المسؤولية " وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الأنترنت وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات وفي تحديد هوية المعتدى، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث

1- براهيمي جمال، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية العدد 02 كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص 138-140.

الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة[1].

الفرع الثاني: آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات الخاصة

أولا :القانون الخاص بحماية حق المؤلف والحقوق المجاورة :يعتبر بعض الفقهاء أن الموقع الإلكتروني مصنف له عدة أغراض يتم استخدامه من الشركات كعلامة تجارية لها لتمييز منتجاتها عن غيرها من المنتجات الأخرى على شبكة الأنترنيت كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو أعمالهم الفنية و يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو اسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة، وبمجرد تسجيل اسم الموقع يحظى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه أي بتحديد القانون الواجب التطبيق حسب الطبيعة القانونية للمواقع فعند تسجيل الموقع كمصنف أدبي أو فني " لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد. " كاستعمال اسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها أو استغلال صورة أي شخص في الموقع دون الموافقة منه والمصنف من حيث المفهوم لا ينصرف فقط إلى المادة الملموسة وإنما هي الفكرة المدرجة في المحل الملموس وهي جوهر الإبداع الأدبي أو الفني لأنها الأساس الذي يقوم عليه المصنف.

وبهذه الصورة فإن حماية مواقع الأنترنت التي تستغل مصنفا أدبيا أو فنيا على شبكة الأنترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الأدبي والمالي للموقع المسجل كمصنف ، وحماية قانونية لأي حق آخر يتم الاعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الاسم والصورة والمعلومات الخاصة وفي كل الأحوال لا يمكن الفصل

1- حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، مداخلة مقدمة في الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، كلية الحقوق والعلوم السياسية، جامعة الجزائر، 29 مارس 2017 ص 121-122.

بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف والحقوق المجاورة في الوقت نفسه، لأن حماية الموقع تؤدي بالضرورة إلى عدم محتوياته بما في ذلك المصنف[1].

ثانيا :قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

نص القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 04 على

أنه "**:يمكن القيام بعمليات المراقبة المنصوص عليها في المادة الثالثة منه :**

"...للوقاية من الأفعال الموصوفة بجرائم الإرهاب

والتخريب أو الجرائم الماسة بأمن الدولة في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية.."[2]

وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات، بالنسبة للمساس بالحياة الخاصة للغير و المقصود من النص من النص أن القانون يخول لبعض السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الإلكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة إذا تلقوا معلومات عن احتمال اعتداء على منظومة معلوماتية لكن في حدود ما يسمح به القانون لاسيما احترام و عدم المساس بالحياة الخاصة للأفراد ، تحت طائلة تعرضهم للعقوبات المقررة في قانون العقوبات الجزائري عن جنحة المساس بالحق في الحياة الخاصة[3].

1- حسين نوارة، المرجع السابق ص 120-121.

2- المواد من 04.03.02 من القانون رقم 04/09 مرجع سابق.

3- حسين نوارة، المرجع السابق ص 120-121.

ثالثا :قانون البريد والاتصالات السلكية واللاسلكية

ولقد أصدر المشرع الجزائري القانون رقم 18-04 المؤرخ في 10 ماي 2018 المحدد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية،[1] والذي أكد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد وفي حالة مخالفة ذلك يتعرض المخالف للأحكام الجزائية التي تضمنها هذا القانون والمتمثلة فيما يلي:

1- انتهاك سرية المراسلات الإلكترونية

وفقا لنص المادة 164 من القانون رقم 18-04 يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية من 500.000 دج إلى 1.000.000 دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو يفشي مضمونها أو ينشره أو يستعمله بدون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها.

تتحقق هذه الجريمة باطلاع الشخص على الرسائل الإلكترونية أو سماع المحادثات الإلكترونية بصورة غير مشروعة، بصرف النظر عن مضمونها أو محتواها فيما إذا كان يتضمن أسرار أم لا إضافة إلى إفشاء مضمونها أو نشره أو استعماله بدون ترخيص.

2- تحويل المراسلات الصادرة عن طريق البريد الإلكتروني

تعاقب المادة 165 من القانون 18-04 بالحبس من سنة إلى ثلاث سنوات وبغرامة مالية من مليون دينار إلى خمس ملايين دينار أو بإحدى هاتين العقوبتين كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية [2].

1- القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق ل 10 ماي سنة 2008 , يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في :2018/05/13 الجريدة الرسمية العدد 27.

2- المواد 165-164 من القانون رقم 18-04 نفس المرجع السابق.

رابعا :قانون التأمينات

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني وكذا الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر 2 و التي تنص : " يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة مالية من 100.000 دج إلى 200.000 دج كل من يستلم بهدف الاستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة "[1].

1- القانون رقم 83-11 المؤرخ في 2 يوليو سنة 1983 المتعلق بالتأمينات الاجتماعية الجريدة الرسمية المؤرخة في 24 رمضان 1403 الموافق ل 2 يوليو 1983.

المبحث الثاني: الهيئات الخاصة لمكافحة جريمة الإرهاب الإلكتروني

نظرا لتفاقم الظاهرة الإجرامية المعلوماتية من يوم لأخر ونظرا إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم كان من الضروري تطوير أساليب ووسائل مكافحتها لتواكب التطور الحاصل في مجال الجريمة الإلكترونية لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الإنتربول واليوروبول.

أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات تابعة لسلك الأمن والدرك الوطني ووحدات أخرى قضائية.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08 غير انه في 2019 صدر مرسوم رئاسي 19-172[2] المعدل بالإلغاء لأحكام المرسوم الرئاسي 15-261 وذلك نتيجة الظروف السياسية والأمنية التي عرفتها البلاد في تلك الفترة مما أدى إلى ظهور مخاطر فعلية لتعرض الأمن العمومي وكذا المؤسسات الدستورية للخطر فجاء هذا المرسوم ليغير من الطبيعة القانونية للهيئة حيث نقل الإشراف عليها.

1- المادة، 13 من القانون 09-04 مرجع سابق.

2- المرسوم الرئاسي 19-172، المؤرخ في 03 شوال عام 1440، الموافق ل 06 يونيو 2019، الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتنظيمها وكيفيات سيرها، الجريدة الرسمية عدد 37 مؤرخة في 09 يونيو 2019.

وبموجب المرسوم الرئاسي رقم: 20-183 تم أعادة تكييفها من جديد على أنها سلطة إدارية مستقلة لكن تحت سلطة رئيس الجمهورية غير انه وبموجب المرسوم الرئاسي رقم 21-439. الذي يهدف إلى إعادة تنظيمها[1].

- **تنظيم الهيئة:** بالرغم من الأهمية المرجوة من هذه الهيئة إلاّ أنّه لم بتم إلى حد الساعة إنشاءها، ولم يصدر تنظيم تشكيلتها ستحوي مجموعة من فإنّ خاص بها يحدد تشكيلتها وتنظيمها وسيرها وباستقراء نصوص القانون 04/09 فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة[2].

- **مهام الهيئة:** من خلال اسمها فإن للهيئة دوران أساسان يمكن أن تلعبهما في حالة تأسسها:

1- الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات ومن أهم هذه الجرائم : التجسس على الاتصالات والرسائل الإلكترونية ،التلاعب بحسابات العملاء أو ببطاقات ائتمانهم اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية.... الخ.

2- مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة14 من القانون 04/09 تتمثل في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

1- المرسوم الرئاسي 21-439، المؤرخ في 02 ربيع الثاني عام 1443، الموافق ل 04 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية عدد 86 مؤرخة في 11 نوفمبر 2021.

2- بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، جامعة محمد بوضياف، المسيلة العدد الحادي عشر، 2018، ص 368.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم [1].

3– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم : في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات)المماثلة لها على مستوى الدولي بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم[2].

1– المادة 14 من القانون رقم 04/09 المرجع السابق.

2–عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، ص 232–233.

المطلب الثاني: الهيئات القضائية المختصة في البحث في الجرائم الإلكترونية

إن السلطة القضائية ستتعامل في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ولاسيما بعد اللّجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي[1].

تم إنشاء هذه الأقطاب بموجب القانون رقم 04-14 المؤرخ في 01 نوفمبر 2004[2]، وتختص هذه الجهات القضائية بموجب المواد 37-40 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار معالجة مثل هذه الجرائم.

ومنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم أولا دمج مادة الجريمة المعلوماتية في برنامج تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء في العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة وإطارات وزارة العدل في إطار التعاون الثنائي.

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 04 - 14المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية على أنه يجوز تمديد دائرة الاختصاص للمحكمة وكذا لوكيل الجمهورية و قاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم

1- بوضياف إسمهان، المرجع السابق، ص 370.

2- القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004.

المتعلقة بالتشريع الخاص بالصرف كما نصت المادة 40 مكرر من قانون الإجراءات الجزائية على أنه :" تُطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 40 ، 37 ، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه[1].

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنَّه جعل المشرع الجزائري لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية[2].

فيتجنب إنشاء هيئات قضائية جديدة لكنّه يوسع من دائرة الاختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها اختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن اختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أن التخصص الذي سيسود التنظيم القضائي الجزائري سيركز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية.

هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006،[3] في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم الخاصة بالصرف ولأن الجريمة المنظمة تشمل جرائم تبييض الأموال والإرهاب، تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وتُرتكب من طرف عدة أفراد يتصرفون بطريقة منظمة تعد الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية

1 – المادة 40 من القانون 04-14، المرجع السابق.

2 –عمار بوضياف، النظام القضائي الجزائري، دار ريحانة، الجزائر ص229 ،230.

3 –المرسوم التنفيذي رقم 06-348، المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية رقم63 المؤرخة في 05 أكتوبر 2006.

والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الاختصاص القضائي في إطار الاهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة[1].

المطلب الثالث: جهازي الأمن الوطني والدرك الوطني

سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[2].

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالآتي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

1- بوضياف أسمهان، المرجع السابق، ص 371.

2- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية مجلة إيليزا للبحوث والدراسات العدد الثاني، ديسمبر 2017، المركز الجامعي إليزي، الجزائر ص 34-35.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط الشرق، الغرب، الجنوب، لنقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن.

- المصلحة المركزية لمكافحة الجريمة المعلوماتية: (SCLCO)

Le Service Centrale de Lutte Contre le Crime Organisé

أسستها المديرية العامة للأمن الوطني بتاريخ 30 أكتوبر 2021، تتولى هذه المصلحة مهمة مباشرة التحريات في قضايا الإجرام المنظم والإرهاب والأعمال الهدامة، بالتنسيق مع الشركاء الأمنيين، كما تضطلع بمهمة مكافحة الإجرام الاقتصادي والمالي، إلى جانب باقي المصالح المتخصصة الوطنية الأخرى، على غرار الديوان المركزي لقمع الفساد والهيئة الوطنية للوقاية من الفساد ومكافحته، وكذا خلية الاستعلام المالي، كما أنها تعتبر في مجال تخصصها، الجهة الرئيسية التي يتم التعامل معها لمركزة التحري مع الأقطاب الجزائية المتخصصة وتعزيز التعاون على المستوى الدولي.

وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة (أنتبول، أفريكوم أو مصالح الشرطة لكبرى الدول) وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الإجرام (الشرطة القضائية) [1].

1- cabinet، Cellule com وزير الداخلية و الجماعات المحلية و التهيئة العمرانية يشرف على تدشين المصلحة المركزية لمكافحة الجريمة المنظمة "الموقع الرسمي لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية مؤرشف من الأصل في 2022-07-09 اطلع عليه بتاريخ:18-07-2022 .

الفرع الثاني: الوحدات التابعة للقيادة العامة للدرك الوطني

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة أو على مستوى القيادات الجهوية والمحلية نذكر منها:

- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.

أولا: المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني (INCC)

Institut National de Criminalistique et de Criminologie

التابع للقيادة العامة للدرك الوطني المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 04-183 بتاريخ: 26 جوان 2004[1] وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة.

ولهذا فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام مكلف خصوصا بـ:

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح.
- مساعدة المحققين للسير الحسن للمعاينات خاصة عن طريق الوضع تحت تصرف الأفراد المؤهلين أثناء الحاجة.
- تنفيذ مناهج الشرطة العلمية والتقنية، لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.
- ضمان المساعدة العلمية في التحريات المعقدة.

1- المرسوم رئاسي رقم 04-183 ،ممضي في 26 يونيو 2004 ،المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني و تحديد قانونه الأساسي، الجريدة الرسمية، رقم 41 ،مؤرخة في 26 يونيو 2004.

- المشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام، مشاركة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المزودة بالتحاليل والخبرات في ميدان علم الإجرام، والمساهمة في إنجاز سياسة مكافحة الإجرام [1] .

يعمل المعهد مع عدة معاهد وجامعات عالمية مختصة في العلم الجنائي والإجرام والمتمثلة في المعهد الأمريكي "إي سي تاب"، مكتب التحقيقات الأمريكي "أف بي أي"، بالإضافة إلى تبادل الخبرات مع الأنتربول، ومعهد الأدلة الجنائية التابع للدرك الفرنسي، والدرك الإيطالي، والحرس المدني الإسباني، ومعهد العلوم الجنائية ببلجيكا، والمعهد التركي "جي كا دي بي"، وجامعة "لوزان" بسويسرا، كما شارك ضباط المعهد، في عدة ملتقيات عالمية، مثل : "الملتقى المنعقد بالنمسا حول حوادث المرور"، وملتقى البيولوجيا الذي عقد بواشنطن، والأدلة الجنائية بالبرتغال وآخر نظمته الأنتربول.

ويحتوي معهد الأدلة الجنائية وعلم الإجرام للدرك الوطني على 916 تجهيز علمي من أحدث طراز، و31 مخبر أدلة جنائية و98 خبيرا قانونيا و18 مخبرا لعلم الإجرام، إضافة إلى قاعدة بيانات تزوّد يوميا بمعطيات جديدة لمختلف العمليات والتحقيقات.

منذ إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني تبن المعهد نظام إدارة الجودة مما مكنه من الحصول على شهادة الاعتماد على المستويين الوطني و الدولي بمهاراته التقنية و التنظيمية و معتمد في مجال الأدلة الجنائية من خلال اعتماد 56 طريقة تحليلية وفق المعيارين الدوليين **ISO 17025 ISO 17020** من قبل هيئة الاعتماد الجزائرية ALGERAC [2] .

---

1 جمال بوازدية، الاستراتيجيات المغاربية لمكافحة الإرهاب، أطروحة دكتوراه، الدراسات الدولية، قسم الحقوق، جامعة الجزائر, 2012, ص 128.

2 https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php
تم الاطلاع عليه يوم 2023/04/09 على الساعة10:00 .

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية (CPLCIC)

Centre de Prévention et de Lutte Contre la Criminalité Informatique et la Cybercriminalité.

التابع للقيادة العامة للدرك الوطني حيث كشف المدير الفرعي للإجرام الخاص بقيادة الدرك الوطني الرائد "رميلي محمد" عن إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر، وهذا من أجل تأمين منظومة المعلومات لخدمة الأمن العمومي، و قام خبراء ومختصين جزائريين وإطارات من الجيش الوطني الشعبي، الشرطة والجمارك أن قيادة الدرك الوطني بصدد إنجاز مركز لمكافحة الجريمة المعلوماتية، يكون بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لا سيما تلك المستعملة في البيوت والبنوك وأضاف المتحدث أن مركز مكافحة الجريمة المعلوماتية، يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى ومهامه لا تختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص[1].

1- سهام مسيعد نشر في صوت الأحرار يوم 18-05-2008.

ملخص الفصل

أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الأنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم وتتفاقم هذه المخاطر بمرور كل يوم لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية ، وفي ظل زيادة خطورة هذا الإرهاب الجديد وانتشاره الرهيب أصبحت محاربته ضرورة حتمية تستوجب على دول تكثيف جهودها بسن تشريعات و إبرام الاتفاقيات وإنشاء منظمات الدولية والإقليمية لمكافحته ، وفرض على الحكومات تطوير وسائلها و قدراتها للتصدي لتهديداته و ذلك بتوفير التقنيات اللازمة للحماية وتقنين قواعد وتشريعات على مستوى الإقليمي والدولي.

الخاتمة

خاتمة

في نهاية هذه الدراسة و من خلال ما تم تقديمه نخلص إلى أن جريمة الإرهاب الإلكتروني من أهم جرائم العصر الحالي ذلك لخطورتها وتنامي انتشارها وبروز العديد من التنظيمات الإرهابية في مختلف أرجاء العالم التي لا تربط بينهم منطقة معينة أو ثقافة محددة بل تربطهم عوامل جديدة أفرزتها الثورة التكنولوجية حيث تعد هذه الأخيرة من الجرائم المستحدثة التي تعتمد عل الموارد المعلوماتية الأمر الذي أوجب على مكافحة الإرهاب الإلكتروني و التصدي له بجميع الإمكانيات و الآليات سواء التشريعية و التنفيذية و القضائية و على جميع المستويات العالمي و الإقليمي، و نجد أن الجزائر لازالت تسعى بشكل صارم إلى التصدي للإرهاب بشكل عام و الإرهاب الإلكتروني بشكل خاص بمختلف مظاهره و أشكاله ذلك لحماية الناس و المجتمع من العمليات الإرهابية الإلكترونية التي سببت ضررا جسيمة مما استدعى إلى تضافر الجهود و الاستراتيجيات الهادفة لمكافحة هذا الخطر وعليه فإننا سجلنا مجموعة من النتائج والاقتراحات تضمنتها الدراسة نذكرها فيما يلي :

أولا: النتائج

- لا يوجد هناك اتفاق على تعريف قانوني جامع للإرهاب الإلكتروني في القانون الدولي وذلك راجع إلى نظرة كل دولة إلى الظاهرة فالبعض يعتبره سلوكا إجراميا ويعاقب عليه بينما البعض الأخر يعتبره مقاومة مشروعة كما أن هناك تداخل لمفهوم الإرهاب الإلكتروني مع غيره من المفاهيم الأخرى.
- يعتبر الإرهاب الإلكتروني امتدادا للجريمة الإرهابية التقليدية ويكمن الفرق في الوسيلة المستعملة والتي تتمثل في استغلال الوسائل الإلكترونية والتقنية وشبكة الأنترنت لارتكاب هذه الجريمة الخطيرة على الدول والشعوب.
- تتميز جريمة الإرهاب الإلكتروني بعدة خصائص وهذا مثل أنها من الجرائم العابرة للحدود كما أنها ترتكب عن بعد ولا يتم اكتشافها إلا بعد فوات الأوان.
- وجود تعاون بين أجهزة الشرطة في مختلف الدول وذلك لمكافحة الجرائم العابرة للحدود ومن بينها جرائم الإرهاب الإلكتروني كذلك تنفيذ عمليات شرطية مشتركة بين الدول لتعقب الجناة الذي يبدأ في دولة وينتهي على إقليم دولة أخرى.

- سعى المجتمع الدولي إلى إبرام اتفاقيات دولية لمكافحة الإرهاب الإلكتروني وذلك من خلال إبرام معاهدات لمكافحة جرائم الإنترنت.
- وجود نظام مثل نظام تسليم المتهمين كان له الأثر البالغ على إظهار دور المجتمع الدولي في مواجهة جرائم الإرهاب الإلكتروني وما لها من خصوصية عابرة للحدود.

ثانيا :التوصيات والاقتراحات

وفي هذا الإطار يمكننا رصد مجموعة من التوصيات والاقتراحات لمواجهة الإرهاب الإلكتروني وتحقيق امن واستقرار الدول نذكر منها:

- تطوير تقنيات مراقبة شبكة الأنترنت وتعزيز إجراءات الأمن والحراسة للمواقع الرسمية.
- تجريم الإرهاب الإلكتروني في التشريعات الوطنية والقوانين الدولية والإقليمية.
- تعزيز التعاون الدولي في مكافحة ظاهرة الإرهاب الإلكتروني لتسليم المجرمين وتحقيق امن واستقرار الدول.
- إقامة شراكات دولية جديدة لمكافحة الإرهاب الإلكتروني.
- إنشاء غرفة عمليات دولية متخصصة في مراقبة الهجمات الإرهابية الإلكترونية التي تتعرض لها أنظمة معلومات المؤسسات الحساسة كتلك الخاصة بالدفاع والجيش والمؤسسات الأمنية، والحد من آثارها.
- تعزيز الجهود الدولية في مكافحة الإرهاب الإلكتروني والاستفادة من الخبرة الدولية في مجال مكافحته وإنشاء مراكز دولية متخصصة لوضع سياسات واستراتيجيات لرصد ومجابهة مخاطر الإرهاب الإلكتروني.
- إبرام اتفاقيات دولية تتضمن تحديد مفهوم الإرهاب الإلكتروني وخطوا ت عملية لمنعه ومكافحته وضرورة وضع إطار تشريعي شامل لتجريم الإرهاب الإلكتروني وتحديد أركانه واعتباره جريمة دولية.
- ضرورة تقرير قوانين جنائية مستقلة عن التقليدية تحتوي هذا النوع من الجرائم المستحدثة بشكل مفصل ودقيق.

وضع إستراتيجية واضحة وطنيا ودوليا من أجل مكافحة ومواجهة جريمة الإرهاب الإلكتروني والتنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحته من خلال الاتفاقيات والمعاهدات الدولية وحث الدول على ضرورة التعاون فيما بينها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

- دستور 1996.

2. النصوص التشريعية

- القانون رقم 09-04، المؤرخ في 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- القانون رقم 16-01، المؤرخ في 06 مارس 2016، المتضمن التعديل الدستوري المؤرخة في 7 مارس 2016 الجريدة الرسمية عدد 14.
- القانون رقم 83-11، المؤرخ في 2 يوليو سنة 1983، المتعلق بالتأمينات الاجتماعية.
- القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق ل 10 ماي سنة 2008 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية الصادر في 2018/05/13 الجريدة الرسمية العدد 27.
- القانون رقم 21-11، المؤرخ في 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.
- الأمر رقم 66 – 156 المؤرخ في 18 صفر 1386 هـ الموافق 8 يونيو 1966 م والمتضمن قانون العقوبات، ج.ر.ع.4 مؤرخة في 17 رمضان 1437 هـ الموافق 22 يونيو 2016م.
- الأمر رقم 12-02، مؤرخ في 13 فبراير 2012، يعدل ويتمم القانون رقم 05-01، المؤرخ في 27 ذي الحجة عام 1425 الموافق 6 فبراير سنة 2005، والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية عدد 8 صادر في 15 فبراير، 2012.

3. النصوص التنظيمية:

- المرسوم الرئاسي 19-172 المؤرخ في 03 شوال عام 1440 الموافق ل 06 يونيو 2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

والاتصال وتنظيمها وكيفيات سيرها، الجريدة الرسمية عدد 37 الصادرة في 09 يونيو 2019.

- المرسوم التنفيذي رقم 06-348، المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقق الجريدة الرسمية رقم 63.
- المرسوم رئاسي رقم 04-183، ممضي في 26 يونيو 2004 المتضمن، إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية، رقم 41.

قائمة المراجع:

كتب:

- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة7، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2008.
- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والأنترنيت، مكتبة الوفاء القانونية، الطبعة 1 ،2011.
- بلعليات إبراهيم، أركان الجريمة وطرق إثباتها، دار الخلدونية، لطبعة 1، الجزائر 2007.
- حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، دار فكر وفن للطباعة والنشر والتوزيع، 2015.
- خلفيه عبد الرحمن، محاضرات في القانون الجنائي العام، دار الهدى، عين مليلة، الجزائر،2012.
- سامي علي حامد عياد، استخدام تكنولوجيا المعلومات في مكافحه الإرهاب، دار الفكر الجامعي، الإسكندرية، 2007،
- شفيق نوران، أثر التهديدات الإلكترونية على العلاقات الدولية، الطبعة1، المكتب العربي للمعارف، القاهرة مصر 2015.
- طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، مصر 2006.
- الطاهر بن يحيى ناعوس، مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية

- عادل عبد الصادق، الإرهاب الإلكتروني قوة في العلاقات الدولية، نمط جديد وتحديات جديدة، الطبعة1، مركز الأهرام للدراسات السياسية والاستراتيجية، 2009.
- عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، مصر 2008.
- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر.
- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة1، مكتبة زين الحقوقية والأدبية، لبنان 2011.
- عمار بوضياف النظام القضائي الجزائري دار ريحانة، الجزائر.
- محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، 2004.
- منصور رحماني، الوجيز في قانون الجنائي العام، دار العلوم للنشر والتوزيع، عنابة، 2006.
- مولود ديدان، قانون الإجراءات الجزائية الأمر 11-02، دار بلقيس، الجزائر.
- علي عسيري، الإرهاب والأنترنت، جامعة نايف للعلوم الأمنية، الطبعة الأولى، الرياض 2006.
- رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة، 1985

الرسائل العلمية:

- إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني الدراسة مقارنة رسالة ماجستير في القانون العام، كلية الحقوق جامعة، البحرين 2012.
- شاشوه ياسمينة، الإرهاب الإلكتروني بين مخاطره وآليات مكافحته مذكرة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة، اكلي محمد أو الحاج بجاية، 2019 2020.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنيت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.
- عبد الرحمن بن سالم بن فهاد الطريف، اتجاهات الطلاب الجامعيين نحو ظاهرة الإرهاب دراسة ميدانية على طلاب الجامعات في الرياض، مذكرة لنيل شهادة الماجستير في العلوم

الاجتماعية، تخصص تأهيل ورعاية اجتماعية، قسم العلوم الاجتماعية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2006.

- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، رسالة دكتوراه في القانون، الجامعة الإسلامية، كلية الحقوق.
- نجاري بن حاج علي فايزة، الآليات القانونية للإرهاب الإلكتروني، مذكرة ماستر في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر.
- وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة المنار –تونس 2014.

المقالات:

أولا: باللغة الفرنسية

- **Peter belly، Hached attacked، abuses digital crime exposés London،Regan 2002.**

ثانيا: باللغة العربية

- براهيمي جمال، مكافحة الجريمة الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، العدد 02 كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو 2016/11/15.
- بوحاده سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية الجزائر.
- بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، جامعة محمد بوضياف، المسيلة، العدد الحادي عشر، 2018.
- حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، كلية العلوم القانونية والسياسية، جامعة ديالي، عدد خاص.

- حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إإلكترونيا، الملتقى الوطني،" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري" الجزائر، 29 مارس 2017.
- راجع بيان مكة المكرمة الصادر عن المجمع الفقهي الإسلامي التابع لرابطة العالم الإسلامي في دورته 16 مكة المكرمة يوم 01-11-2002 م.
- سهام مسيعد، نشر في نشر صوت الأحرار، يوم 18-05-2008.
- الشافعي نوري رشيد، وسامر مؤيد عبد اللطيف ومنى محمد عبد الرزاق، "دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مجلة رسالة الحقوق، المجلد 10 العدد 02 جامعة كربلاء، كلية القانون، العراق 2018.
- صباح كزيز، أمال كزيز الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم 01 العدد 08، 2008.
- عواطف عثمان محمد عبد الحليم، جرائم معلوماتية، مجلة العدل العدد 24.
- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017.
- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية مجلة إيليزا للبحوث والدراسات العدد الثاني، ديسمبر 2017 المركز الجامعي إليزي، الجزائر.
- محمد الطيب عبد الله خالد، الإرهاب الإلكتروني، مجلة كلية الشريعة والقانون، جامعة أم درمان الإسلامية، المجلد الثالث عشر 2020.
- محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها، الإرهاب الإلكتروني وطرق مواجهته، ملتقى الجرائم المستحدثة في ضل التغيرات والتحولات الإقليمية، كلية العلوم والدراسات الاستراتيجية، المملكة الأردنية الهاشمية 2013.

- ناصر العلجة، الجهود الدولية في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية العدد الأول 2018.
- فايز بن عبد الله الشهري، بحث بعنوان استخدام شبكة الأنترنت في مجال الإعلام الأمني العربي، مجلة البحوث الأمنية مركز الدراسات كلية الملك فهد الأمنية، الرياض المجلد 10، العدد 19، نوفمبر 2001.
- الشافعي نوري رشيد، وسامر مؤيد عبد اللطيف ومنى محمد عبد الرزاق، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مجلة رسالة الحقوق، المجلد 10 العدد 02، جامعة كربلاء، كلية القانون العراق 2018.

الاتفاقيات:

- اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) الصادرة عن هيئة الأمم المتحدة الكلية العامة.
- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

المؤتمرات:

- مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا من 10 إلى 18 أفريل 2000.

المواقع:

- المجلس الأعلى للأمن السيبراني"، رئاسة مجلس الوزراء المصري، ديسمبر 2014. على الرابط التالي: https://www.escc.gov.e
- الجهود العربية لمواجهة مخاطر الإرهاب السيبراني الواقع والمأمول على الرابط التالي: https://arabaffairsonline.com
- نورا بينداري عبد الحميد، "دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية دراسة حالة "داعش"، المركز الديمقراطي العربي، 19 يوليو 2016، على الرابط التالي: https://www.democraticac.de

- العراق: تتبنى إستراتيجية وطنية شاملة لمكافحة الإرهاب"، أخبار اليوم، 20 نوفمبر 2021 على الرابط التالي : https://www.m.akhbareyoum.com
- مكافحة الإرهاب والتطرف"، وزارة الخارجية والتعاون الدولي بدولة الإمارات العربية المتحدة، 27 أغسطس 2021، على الرابط التالي:
https://www.mofaic.gov.ae/ar-ae/the-ministry/the-foreign-policy/combating-terrorism-and-extremism.
- https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php
- بالواضح الطيب قسمة محمد، مكافحة جريمة تمويل الإرهاب على المستويين الدولي والوطني، 2017 متاح على الرابط التالي:
https://www.asjp.cerist.dz/en/article/65104
- أماني مهدي، توظيف التنظيمات الإرهابية لشبكات التواصل الاجتماعي في استقطاب الشباب "الاستراتيجيات وآليات المواجهة 2018 متاح على الرابط التالي:
cs.google.com/document/d/1y2xU5kTJaruolcwhk3o40nOYEkAQG_Qc9QIOTkiVKI/edit

الفهـــرس

الملخص:

أدى التطور التكنولوجي لوسائل الاتصال الحديثة إلى تغيير جذري في الإرهاب وأسهم في إعادة شكله الحالي على وجه لم يعد يحتفظ بشكله التقليدي الذي قد يكون من السهل استهدافه ومحاربته.

تمكنت الجماعات الإرهابية من استغلال الفضاء الإلكتروني للقتال ولقد رأوا في ذلك وسيلة لإعادة توازن القوى لصالحهم، شن الإرهاب هجمات واسعة النطاق عن طريق الأنترنت وبواسطة بوسائل محدودة فتمكنوا من جمع الأموال وتجنيد المقاتلين واختراق مواقع الويب لأغراض الدعاية عن طريق الأداة الرقمية.

يشكل الإرهاب الإلكتروني اليوم خطر على جميع القطاعات، المصرفية والمالية والعسكرية والملاحة الجوية والنقل، والعديد من القطاعات الأخرى التي قد تكون عرضة للخطر بشكل خاص.

سنت الجهات الحكومية في جميع أنحاء العالم تنظيمات وبرامج وسياسات وقوانين وتدابير صارمة أخرى لمواجهة التهديدات، لكن هذه الحرب صعبة تتطلب تحديثًا ورصدًا مستمرا، بسبب التزايد المستمر للتهديدات.

هدف البحث وسعى الى محاولة استكشاف وتحديد معالم الإرهاب الإلكتروني، ولذا اقتصر على بيان ماهية الإرهاب الإلكتروني، وخصائصه وأهدافه وإبراز أهم مظاهره وأشكاله، مع توضيح آليات وطرق التصدي له.

Abstract

L'évolution technologique des moyens de communication modernes fondamentalement transformé le terrorisme et contribué à remodeler ses formes actuelles de sorte qu'il ne garde plus sa forme traditionnelle susceptible d'être ciblée et atteinte.

Des groupes terroristes ont pu investir le cyberespace pour mener leur combat, ils y ont vu un moyen de rééquilibrer le rapport de force à leur avantage, l'internet permettant de mener des offensives d'envergure avec des moyens limités. Ainsi, ils ont pu récolter des fonds, recruter des combattants ou encore pirater des sites internet à des fins de propagande grâce à l'outil numérique.

La menace de cyber terroriste touche aujourd'hui toutes les organisations, le secteur des banques, de la finance, militaire, aéronautique, du transport, et bien d'autres sont particulièrement à risque.

Les secteurs gouvernementaux du monde entier ont édicté des réglementations, des programmes, des politiques, des lois et diverses autres mesures strictes, afin de lutter contre ces menaces, mais cette bataille ardue nécessite une mise à jour et un suivi constant, en particulier à cause de la croissance des menaces.

Le but de la recherche est d'essayer d'explorer et de définir les caractéristiques du cyberterrorisme, et par conséquent, elle s'est limitée à expliquer la nature du cyberterrorisme, clarifier ses caractéristiques et ses objectifs, et mettre en évidence ses manifestations et ses formes les plus importantes, outre une explication du mécanisme et des méthodes pour y faire face.