جـامعـــة العـربـــي التبســـي – تبســـة

كليـــة الحقـوق والعلـوم السيـاسيـة –تبسـة–

قســـم الحقـــوق

مـذكـــرة مقـدمـــة ضمـن متطلبـات نيـل شهـادة ماستـر

تخصص: قانون جنائي وعلوم جنائية

بعـــنـــوان:

جـــــريمـــة الإرهـــــاب الالكترونـــي

إعـداد الطـالـــب:

❖ علي بوعمـــــرة

إشـــــراف الدكتور:

* خذيري عفـــــــاف

لجنـة المناقشـة

الاســـم واللـقـــب	الـرتبـــة العلميـــة	الصـفـــة
دلـــول الطاهـــر	أستـــاذ	رئيسـا
خذيـري عفـــاف	أستـــاذة محـاضـــر -ب-	مشرفا ومقررا
مقـــران ريمـــة	أستـــاذ محـاضـــرة -أ-	ممتحنا

السنـــة الجـامعيـــة: 2020-2021 م

جـامعـــة العـربـــي التبســـي – تبســـة

كليـــة الحقـوق والعلـوم السيـاسيـة –تبسـة–

قســـم الحقـــوق

مـذكـــرة مقـدمـــة ضمـن متطلبـات نيـل شهـادة ماستـر

تخصص: قانون جنائي وعلوم جنائية

بعـــنـــوان:

جـــــريمـــة الإرهـــــاب الالكترونـــي

إعـداد الطـالـــب:

❖ علي بوعمـــــرة

إشـــــراف الدكتور:

* خذيري عفـــــــاف

لجنـة المناقشـة

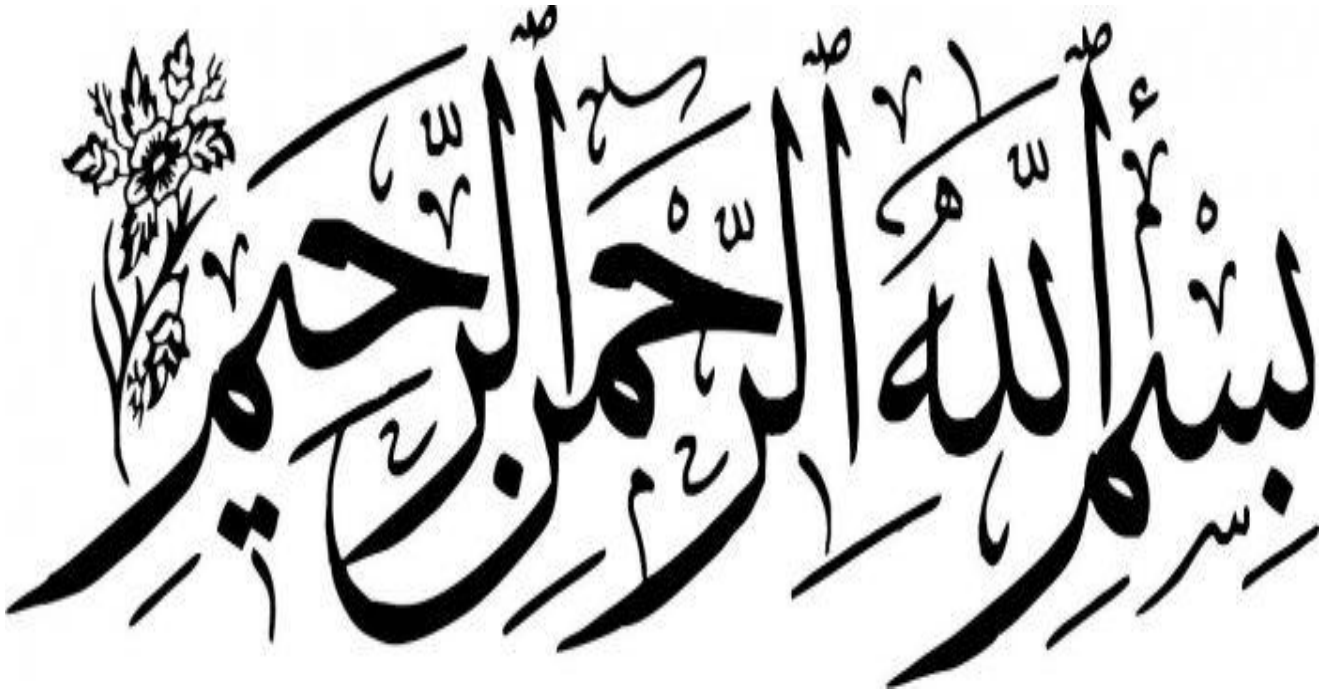
الاســـم واللـقـــب	الـرتبـــة العلميـــة	الصـفـــة
دلـــول الطاهـــر	أستـــاذ	رئيسـا
خذيـري عفـــاف	أستـــاذة محـاضـــر -ب-	مشرفا ومقررا
مقـــران ريمـــة	أستـــاذ محـاضـــرة -أ-	ممتحنا

السنـــة الجـامعيـــة: 2020-2021 م

الكلية لا تتحمل أي مسؤولية

على ما يرد في هذه المذكرة

من آراء


بسم الله الرحمن الرحيم

الإهـــداء

أهدي ثمرة هذا العمل المتواضع.

إلى والدي الكريمين رعاهما الله وأدامهما لنا .

إلى إخوتي الذين كانوا نعم السند .

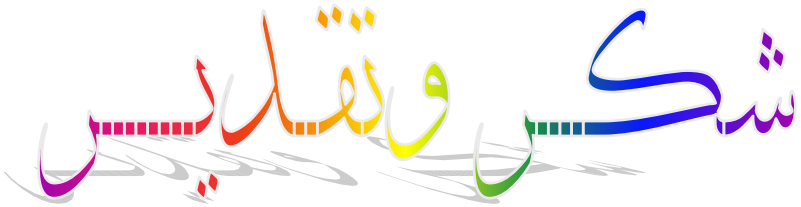
إلى ابن عمي توفيق الذي كان عونا لي.

إلى كل أساتذتي و عائلتي و أصدقائي و زملائي.

إلى صديقتي التي أسهمت ورافقتني طوال رحلة البحث.

إلى كل من ساندني و لو بالكلمة الطيبة إلى الذين حملوا شعلة العلم إلى الذين يلتمسون الطريق المستقيم.

علي بوعمرة



أولا و قبل كل شيء أشكر الله عز و جل على توفيقه لي في إتمام هذا العمل المتواضع

كما أتقدم بالشكر إلى الأستاذة المشرفة خذيري عفاف على ما قدمته لي من نصائح وتوجيهات قيمة

إلى كل من قدم لي يد المساعدة من قريب أو من بعيد

مقدمـــــــة

تعد ظاهرة الإرهاب من الظواهر القديمة نسبيا يرتبط وجودها بوجود الأنظمة السياسية والشعوب، حيث أنها ظاهرة لا تقتصر على شعب دون آخر أو دولة دون أخرى أو ثقافة دون أخرى، فهي آفة خطيرة تجد نماءها وسرعة انتشارها خاصة في الظروف الاجتماعية والسياسية.

ومع تطور الإنسان في شتى الميادين خاصة في مجال التقنية وظهور الإنترنت حيث غزت جميع المجالات نظرا لما تتسم به من الدقة و السرعة، وأصبحت في متناول الجميع، كل ذلك أدى إلى ظهور طائفة جديدة من أخطر الجرائم نتيجة الانعكاس السلبي لهذه الثورة العلمية، وأهمها ظاهرة الإرهاب الإلكتروني حيث تعتبر من أخطر الجرائم التي تهدد المجتمع والعالم ككل.

ونظرا للتفشي السريع لجرائم الإرهاب الإلكتروني فقد أولى لها العديد من الباحثين في مختلف المجالات قدرا كبيرا من الاهتمام، كما سارعت الكثير من الدول إلى إصدار قوانين وتشريعات للوقاية من هذه الجرائم ومكافحتها، وإحداث هيئات حكومية لهذا الغرض مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذلك السماح بالمراقبة الإلكترونية فيما يخص هذه الجرائم، خاصة مع تطور الاعتداءات من شكلها البسيط إلى عهد الإلكترونيات شديدة الحساسية والفعالية.

وتتمثل مظاهره في التصرفات والأفعال الخارقة للقوانين والأنظمة والتعليمات، والتي تهدف إلى نشر الخوف وبث الرعب بطرق تقنية حديثة تسمح باستغلال شبكة الإنترنت من طرف أخصائيين مستعملين في ذلك أسلحة حديثة وتكنولوجية، ويعد الفضاء الإلكتروني فضاء واسعا للتواصل فيما بينهم والتخطيط لأعمالهم الإجرامية.

أهمية الموضوع

تظهر الأهمية العلمية للدراسة من خلال حرص المجتمع الدولي عموما والمشرع الجزائري خصوصا على مكافحة هذه الظاهرة، و تعد كذلك هذه الدراسة بالغة الأهمية

لارتباطها الوثيق بأمن الدول والشعوب على حد سواء، إضافة إلى كون الإرهاب الإلكتروني يعد من أبرز المواضيع المثارة في العصر الحالي.

بينما تتمثل الأهمية العملية لهذه الدراسة في معرفة الحماية الجنائية المكفولة للدول والشعوب حيال هذه الظاهرة، إضافة إلى الاهتمام الخاص بالبحث في موضوع الإرهاب الإلكتروني بغية شرح وتحليل المفاهيم القانونية المتعلقة به.

أسباب اختيار الموضوع

تعود أسباب اختيار هذا الموضوع إلى أسباب ذاتية وأخرى موضوعية

تتمثل الأسباب الذاتية في الرغبة والميول للبحث في هذا الموضوع ودراسته، وذلك نظرا للانتشار الواسع للوسائل التقنية الحديثة والتي تسهل على الإرهابيين ارتكاب جرائمهم والاعتداء على الدول ونشر الخوف بين الشعوب.

أما الأسباب الموضوعية فأغلبها تتلخص في محاولة فهم ما إذا كانت الأحكام والنصوص القانونية كافية من الناحية الإجرائية والعقابية لمكافحة هذه الظاهرة ومواجهتها سواء على الصعيد الدولي أو على الصعيد الوطني، أم أنها تحتاج إلى تعديل وتدعيم، إلى جانب الخوض في مختلف الإشكالات القانونية التي يثيرها هذا الموضوع

الإشكالية

على ضوء ما سبق يمكن طرح الإشكالية التالية:

فيما تتمثل ظاهرة الإرهاب الإلكتروني و ما هي الإجراءات المتبعة لمكافحته؟

منهج الدراسة

تـم الاعتمـاد فـي هـذه الدراسـة علـى المـنهج التحليلـي القـائم علـى تحليـل مضـمون النصـوص القانونيـة ذات الصـلة بالموضـوع، للوقـوف علـى فعاليـة تلـك النصـوص فـي تحقيـق التوازن بين المصلحة الخاصة للفرد والمصلحة العامة للدولة والمجتمع.

كمـا تـم الاعتمـاد علـى المـنهج الوصـفي لعـرض جميـع الجوانـب الخاصـة بمفهـوم الإرهـاب الإلكتروني و نطاقه القانوني، والأحكام المتعلقة بمكافحته.

أهداف الدراسة

تنقسم أهداف هذه الدراسة إلى أهداف علمية وأهداف عملية، حيث تتمثل الأهداف العلمية في تبيان مفهوم الإرهاب الإلكتروني وإبراز خصائصه وصوره ودراستهم باعتبار أن هذا الموضوع يعد من أخطر المواضيع في العصر الحديث.

فـي حين تتجلى الأهداف العلميـة فـي جمـع القوانين ذات الصـلة بالموضـوع وتسـليط الضـوء علـى مختلـف المـواد القانونيـة فـي المنظمـات العالميـة والقاريـة وكـذا فـي التشـريع الجزائري والتـي تعنـي بهـذا الموضـوع والوقـوف علـى مـدى ملائمتهـا لطبيعتـه وقـدرتها علـى مكافحته، ومنه الوصول إلى لفت النظر إلى مدى خطورة الإرهاب الإلكتروني.

الدراسات السابقة

فيما يخص موضوع الإرهاب الإلكتروني فقد تناولت بعض الدراسات التي وجدتها، إلا أنها لم تتطرق إلى جميع جوانب الموضوع و حاولت تجميعها في هذه الدراسة، و أهم هذه الدراسات

1- حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 03، 2014

2- نـور الله تلـة، الإرهـاب بالوسـائل الإلكترونيـة، مـذكرة ماجسـتير، كليـة الحقـوق، جامعـة دمشق،2016.

3- نـورة طرشـي، مكافحـة الجريمـة المعلوماتيـة، مـذكرة ماجسـتير، كليـة الحقـوق، جامعـة الجزائر، 2012.

صعوبات الدراسة

تجسـدت صـعوبات البحـث فـي هـذا الموضـوع إلـى صـعوبة الوصـول إلـى المراجـع والمكتبات نظرا للحجر الصحي المفروض في بلادنا نتيجة تفشي جائحة كورونا، كما أن هذا الموضوع يتسم بالاتساع مما يجعل من الصعب الإحاطة بكافة جوانبه فهو مترامي الأطراف بين قانون العقوبات و قوانين أخرى خاصة.

ولتحقيق الهدف من الدراسة حسب المنهجية المعتمدة تم تقسيم الموضوع وفق خطة ثنائية مقسمة إلى فصلين:

الفصل الأول بعنوان مفهوم الإرهاب الإلكتروني مقسم بدوره إلى مبحثين جاء في المبحث الأول تعريف الإرهاب الإلكتروني، وصور الإرهاب الإلكتروني في مبحث ثان.

أما الفصل الثاني فجاء بعنوان الآليات القانونية والأمنية لمكافحة الإرهاب الإلكتروني وتم تقسيمه كذلك إلى مبحثين حيث تم التطرق في المبحث الأول إلى الآليات القانونية و الأمنية لمكافحة الإرهاب الإلكتروني على الصعيد الدولي، وفي المبحث الثاني تناولت الآليات القانونية و الأمنية لمكافحة الإرهاب الإلكتروني على الصعيد الوطني.

الفصل الأول:

مفهوم الإرهاب الالكتروني

المبحث الأول: تعريف الإرهاب الالكتروني

المبحث الثاني: صور الإرهاب الالكتروني

نظرا للتطور الكبير الحاصل في مجال وسائل الاتصال والانترنت، ما جعل ذلك يساهم بشكل كبير في تطور أنواع الجرائم وانتشارها بسرعة رهيبة، ومن أهم وأخطر هذه الجرائم نجد الإرهاب الإلكتروني، كونه يعتمد في الأساس على الانترنت والشبكة المعلوماتية لتهديد الدول والمجتمعات بهدف بث الرعب ونشر الخوف، وتبرز من الناحية الفقهية والتشريعية اختلافات كثيرة في موضوع تعريف الإرهاب الإلكتروني حيث لم يتم الاتفاق على تعريف موحد، وفي ظل التطور الحاصل تعددت صور الإرهاب الإلكتروني وأنواعه، إضافة إلى أن الإرهاب الإلكتروني يختلف عن الإرهاب التقليدي في العديد من الجوانب.

وتعتبر أسباب الإرهاب الالكتروني متعددة وذلك لأن الإرهاب الالكتروني يعتبر نوعا من أنواع الإرهاب وشكلا من أشكاله، دوافعه متعددة ومتنوعة، وهي عينها أسباب ظاهرة الإرهاب عموما.

وبما أن هذه الظاهرة تعد من الجرائم الحديثة نسبيا حيث تستغل الجماعات الإرهابية الانترنت من أجل نشر أفكارها المتطرفة والاتصال فيما بينها وكذلك إنشاء حسابات ومواقع تخدم مصالحها لذلك كان لزاما التعرض في هذا الفصل إلى تحديد مفهوم الإرهاب الإلكتروني من خلال إبراز تعريفه وخصائصه وصوره.

المبحث الأول: تعريف الإرهاب الإلكتروني

مما لا شك فيه أن العالم يشهد اليوم تطورا هائلا في وسائل الاتصالات وتقنية المعلومات، حتى سمي هذا العصر بالعصر الرقمي، ومنه بروز مصطلح الإرهاب الإلكتروني، الذي زاد من تعقيد الجرائم الإرهابية وخطورتها، ومنه يمكن أن نعتبرالإرهاب الإلكتروني جريمة عصرية تعتمد على طرق ووسائل متطورة أدت إلى انتشارها وتزايد الأخطار الناجمة عنها وتعبر هذه الأمور من السلبيات التي تتميز بها شبكة الانترنت بم لها من طابع عابر للحدود الوطنية وما تمتاز به من سرعة وفعالية، لهذا وجب تعريف الإرهاب الإلكتروني وتبيان خصائصه وصوره.

المطلب الأول: التعريف اللغوي والإصلاحي للإرهاب الإلكتروني

لم يتم اعتماد تعريف موحد للإرهاب الإلكتروني خاصة في جانبه اللغوي حيث تم الاعتماد على تعريف الإرهاب لغة دون التطرق إلى الإلكتروني منه ما يجعل نفس التعريف المعتمد للإرهاب العادي ينطبق على الإرهاب الإلكتروني.

الفرع الأول: التعريف اللغوي

هو أسلوب من أساليب الصراع الذي تقع فيه الضحايا جزافا كهدف عنف فعال، وتشترك هذه الضحايا الفعالة في خصائصها مع جماعة أو طبقة في خصائصها مما يشكل أساسا لانتقائها من أجل التضحية بها[1].

[1]– سلوى أحمد ميدان، الإرهاب والجهود الدولية لمكافحته، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، العدد الخامس، 2016، ص 54.

و في موسوعة المعلومات الأمريكية نجد أن الإرهاب الإلكتروني يعني "استخدام القوة أو التهديد باستخدامها باللجوء و بشكل خاص إلى التفجيرات والخطف والاغتيال من أجل الوصول إلى هدف سياسي"[1].

كما عرفه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي بأنه "العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دينه أو دمه وعقله و ماله وعرضه، ويشمل صنوف التخويف الأذى والتهديد والقتل بغير حق، وما يتصل بصورة الحرابة وإخافة السبيل وقطع الطريق، وكل فعل من أفعال العنف أو التهديد يقع تنفيذا لمشروع إجرامي فردي أو جماعي، و يهدف إلى إيقاع الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أموالهم إلى الخطر.[2]

الإرهاب من المصطلحات التي كثر الاختلاف في بيان معناها وتحديد مدلولها علما بأنها من أكثر الكلمات استخداما في مختلف وسائل الإعلام العالمية في السنوات الأخيرة، ورغم ذلك فإنه لم تتفق كلمة لباحثين على التعريف الدقيق والمحدد لهذا المصطلح بالنظر لطبيعة الأعمال الإرهابية واختلاف وجهات النظر لمثل هذه الأعمال ولغاية توضيح تعريف الإرهاب الالكتروني سنقوم ببيان تعريف الإرهاب ومن ثم نستخلص تعريفا للإرهاب الالكتروني[3].

إذا فمن الناحية اللغوية لم تذكر المعاجم العربية القديمة كلمة إرهاب ولكنها عرفت الفعل رهب يرهب رهبة ورهبا، وهذا يعني الانزعاج والإخافة، وقد تداركت المعاجم الحديثة ذلك إذ جاء في المعجم الوجيز أن الإرهابيين هو وصف يطلق على الذين يسلكون سبل العنف والإرهاب لتحقيق أهدافهم السياسية.[4]

---

[1]– حسن طاهر داوود، جرائم نظم المعلومات، ط 3،دار الكتاب العلمي، الرياض، المملكة العربية السعودية، 2008، ص 144.

[2]– عفيفي كامل عفيفي، جرائم الكمبيوتر، ط 2، دار الثقافة للطباعة والنشر والتوزيع، القاهرة، مصر، 2012، ص 138.

[3]– سلوى أحمد ميدان، المرجع السابق، ص 55.

[4]– سلوى أحمد ميدان، المرجع نفسه، ص 55

الفرع الثاني: التعريف الاصطلاحي

هو علم إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية ينتج عنه تدمير وتعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو أيديولوجية[1].

ويعرف أيضا بأنه: كل هجوم الغرض منه الحصول على المعلومات المرتبطة بالغير وإمكانياته واستراتيجياته التي يتخذها للدفاع عن نفسه أو تدمير نظم المعلوماتية أو نشر المعلومات الزائفة من أجل تضليله بتوظيف تكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنت[2].

كما يعرف أيضا بـ: كل جماعة إرهابية تستعمل وسائل التكنولوجيا كالإنترنت من أجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق أو لتبادل المهارات والخبرات والأساليب، أو جمع تبرعات من أجل تمويل عملياتهم الإرهابية[3]

وهناك من عرفه بأنه: "هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا توجه من أجل الانتقام والابتزاز أو الإجبار أو التأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره، لتحقيق أهداف دينية أو سياسي أو اجتماعية معينة، وبالتالي لكي يلقب شخص ما بأنه إرهابي على الانترنت وليس مخترقا فقط فلا بد أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب"[4].

مما سبق يتبين أن جرائم الإرهاب الإلكتروني ضمن الجرائم الإلكترونية التي تستهدف السيطرة على نظم المعلومات، بغية التخويف ونزع الثقة بنظم التقنية، وذلك

---

[1]– عادل عبد الصادق، الإرهاب الإلكتروني وتأثيره على الدول، ط1، دار الأهرام للنشر والتوزيع، القاهرة: مصر، 2014، ص 86.

[2]– عفيفي كامل عفيفي، المرجع السابق، ص138.

[3]– عادل عبد الصادق، المرجع السابق، ص87.

[4]– علي عدنان الفيل، الإجرام الإلكتروني، ط 1، مكتبة زين الأدبية والحقوقية، لبنان، 2011، ص 60 .

باستخدام نظم الكومبيوتر والشبكات الإلكترونية بوصفها وسيلة لارتكاب جرائمها، إضافة إلى استخدامها التكنولوجيا بهدف سرقة المعلومات أو نشرها، أو من أجل تمويل العمليات الإرهابية، أو تجنيد الإرهابيين.[1]

ويكمن الاختلاف بين الإرهاب العادي والإرهاب الإلكتروني كون هذا الأخير يعتمد على العنف الإلكتروني باستخدام تطبيقات الانترنت والخدمات المتصلة بها وبالتالي طريقته عصرية في استخدام الموارد المعلوماتية التي جلبتها تقنية عصر المعلومات.[2]

ويعرف الإرهاب على أنه "الاستخدام العمدي والمنظم لوسائل من طبعها إثارة الرغبة والفزع بقصد تحقيق بعض الأهداف"، كما يعرف أيضا بأنه: "أحد مظاهر العنف الاجتماعي وعليه فهو ظاهرة مركبة ومتعددة الأبعاد يختلط فيها العنصر النفسي بالعناصر الاجتماعية والمالية والمادية والثقافية والسياسية والتاريخية"[3]. أما الاتفاقية العربية لمكافحة الإرهاب فقد عرفته على أنه: "كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه يقع تنفيذا لحكم إجرامي فردي أو جماعي.

ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة والخاصة. أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر. ويتضح من التعريفات السابقة أن جوهر الإرهاب هو حالة الرعب التي يتمكن فاعلها من فرض سيطرته لتحقيق هدف ما[4].

ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة، واستهداف غايات معينة، ويتميز الإرهاب الالكتروني من غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة

---

[1]– محمد عبد المحسن سعدون، مفهوم الإرهاب وتجريمه في التشريعات الوطنية والدولية، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، العدد السادس، 2016، ص55.

[2]– نور الله تلة، الإرهاب بالوسائل الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة دمشق،2016،ص.27

[3]– سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مقال منشور في مجلة كربلاء العلمية، جامعة اليرموك، العراق، العدد 14، 2014، ص 226.

[4]– أحمد فتحي سرور، مواجهة الإرهاب الإلكتروني، ط 3، دار النهضة العربية، القاهرة، مصر، 2011، ص 31.

في استخدام الموارد المعلوماتية والوسائل الالكترونية التي جلبتها حضارة تقنية في عصر المعلومات، لذا فان الأنظمة الالكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين[1].

وغني عن البيان أن الإرهاب الالكتروني يشير إلى عنصرين أساسيين هما: – الفضاء الافتراضي والإرهاب، إضافة إلى ذلك هنالك كلمة أخرى تشير إلى الفضاء الالكتروني وهي العالم الافتراضي والذي يشير إلى التنفيذ الرمزي والزائف والمجازي للمعلومات، وهو المكان الذي تعمل فيه الأجهزة وبرامج الحاسوب وشبكات المعلوماتية، كما تنتقل فيه البيانات الالكترونية، ونظرا لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية، فقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة.[2]

كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية للأنظمة والشبكات المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وهناك ما يشير إلى إمكانية انهيار البنية التحتية للأنظمة والشبكات المعلوماتية في العالم كله، وليس في بعض المؤسسات والشركات الكبرى أو في بعض الدول المستهدفة، فالإرهاب الالكتروني أصبح خطرا يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في منزله أو في مكتبه أو في غرفته الفندقية وبعيدا عن أنظار السلطة والمجتمع.[3]

[1]– إسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربته في العالم المعاصر، ط3، منشأة المعارف، مصر، 2010، ص51.

[2]– أحمد فتحي سرور، المرجع السابق، ص33.

[3]– إسماعيل عبد الفتاح عبد الكافي، المرجع السابق، ص 52.

المطلب الثاني: خصائص الإرهاب الإلكتروني

يتميز الإرهاب الإلكتروني بعدة خصائص تبين درجة خطورته، لهذا من الأنسب معرفتها حتى يمكن مواجهته ومحاولة تجنب الخطورة الناجمة عنه،

ومن أهم هذه الخصائص ما يلي:

الفرع الأول: الخصائص العامة

ويكمن إبرازها على النحو التالي:

أولا- عصري يعتمد على التقنيات الحديثة

من خلال الاعتماد على استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، حيث يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي في أنه يعتمد على التقنيات الحديثة في مجال المعلوماتية والاتصالات، وكل ما هو جديد في هذا المجال، واستغلال الإمكانات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، في ارتكاب وتنفيذ جرائمه.[1]

فالتكنولوجيا الرقمية الحديثة، وبخاصة في مجالي المعلومات والاتصالات، في تقدم مذهل ومتسارع يوميا، و قد يساء استخدامها في اعتداءات إجرامية أو إرهابية، تتطلب من المجتمع الدولي كله اقتراح واتخاذ كافة أساليب وإجراءات العلاج العاجلة والفعالة لمكافحة الإرهاب في العصر الرقمي[2]، ما يجعله يعد من الجرائم غير التقليدية، حيث يتسم بالخطورة البالغة نظرا لأغراضه المتعددة وحجم الخسائر الناجمة عنه قياسا بالجرائم التقليدية[3] ، خاصة وأن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي

[1]- جمال علي الدهشان، الإرهاب الإلكتروني في العصر الحديث، ط2، دار الفكر العربي، القاهرة، مصر، 2018، ص164.

[2]- فتحي شمس الدين، الإرهاب الإلكتروني وخطره على المستقبل، د ط، منشأة المعارف، الإسكندرية، مصر،2017، ص 89.

[3]- سامر مؤيد عبد اللطيف، المرجع السابق، ص 228.

الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي و الشبكة المعلوماتية.[1]

ثانيا- تعدد أشكاله وتنوع أساليبه

فالإرهاب الإلكتروني لا يتخذ شكلا واحدا أو أسلوب واحد وإنما تتعدد أشكاله وتتنوع صوره وأساليبه، تتمثل أشكاله في التجسس الإلكتروني، والاختراقات، أو القرصنة على المواقع الحيوية للمنشآت و المؤسسات الرسمية في المجتمعات المختلفة، والتجنيد الإلكتروني من خلا ما يطلق عليه التلقين الإلكتروني.

وأخيرا التهديد والترويع الإلكتروني، كما أن أدواته متعددة متمثلة في فيروسات اختراق البيانات وتدميرها والتجسس وتجنيد الإرهابيين وجمع الأموال وتمويل العمليات الإرهابية وحروب الدعاية للأفكار المتطرفة والهدامة وغيرها.[2]

كما يتميز بأنه يتم ارتكابه عادة من قبل فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرا صعبا وانطواءه على سلوكيات غير مألوفة كنشر الأفكار الهدامة التي تنسب إلى الدين وبث الفتاوى البعيدة عن أصول الدين والعقيدة على مواقع الشبكة.[3]

ثالثا- سهولة استخدامه مع شدة أثره وضرره

حيث يمكن لمن لديه بعض المعارف والمعلومات البسيطة عن التعامل مع شبكة المعلومات الدولية الانترنت وأدواتها وعلوم الحاسب أن يقوم بالعديد من جرائم الإرهاب الإلكتروني بسهولة، ويؤدي إلى إحداث خسائر عديدة تتجاوز حدود الدول وقد تمت إلى العالم اجمع، ومما زاد من سهوله استخدامه توفر خدمات الانترنت من خلال الأجهزة النقالة وحاسبات الجيب التي أصبحت في متناول الجميع في أي مكان وفي أي وقت، حيث يعتمد الإرهاب الإلكتروني على استغلال الإمكانات العلمية والتقنية، واستخدام

---

[1]- عقيلة هادي عيسى وإسراء جواد حاتم، الإرهاب المعلوماتي وطرق مكافحته، مقال منشور في المجلة السياسية والدولية، الجامعة المستنصرية، العراق، العدد 16، 2010، ص183.

[2]- صادق عادل، الأمن السيبيراني، د ط، المركز العربي لأبحاث الفضاء الإلكتروني، الأردن، 2017، ص166.

[3]- عقيلة هادي عيسى وإسراء جواد حاتم، المرجع السابق، ص 191.

وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار والدماء لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور. كما لا يشترط توافر التنظيم في الإرهاب الرقمي فقد يرتكب فرد لوحده بعيدا عن أي تنظيم سلوك إرهابي. [1]

رابعا- تخطيه للحدود وقدرته على التأثير على الجميع

فالهجوم الإلكتروني نشاط عابر للحدود ومن ثم فهو نشاط عالمي، حيث يستخدم الإرهابيون الفضاء الإلكتروني في التأثير على الرأي العام وتجنيد أعضاء جدد من مختلف أنحاء العالم والتمويل، ونشر رسالتهم والوصول إلى أكبر عدد ممكن من الجمهور وشن حرب نفسية ضد الأعداء والدعاية للتنظيم.

حيث يعتبر الإرهاب الالكتروني جريمة عابرة للقارات ويصعب اثباتها لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة ولغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم. [2]

خامسا- الصبغة الدينية للإرهاب الإلكتروني

فالإرهاب الإلكتروني غالبا ما يكون مغطي بطبقة دينية كثيفة من الصعب إزالتها عنه إلا بقاشط حاد، ومن قبل جراحين متخصصين، فنقرأ أن اسم الموقع الإلكتروني اسم ديني، ونرى أن معظم المواد المنشورة عليه تتضمن بين ثناياها -إذ لم يكن في كل سطر من سطورها- حديثا نبويا شريفا، أو آية قرآنية كريمة، قد تم حشرها قسرا، وتفسيرها تفسيرا قسريا، وتم لي عنقها ليا شديدا، لكي تناسب واقع الحال، و تعبر عن المآل. [3]

---

[1]- عطية محمد، الإرهاب الإلكتروني وطرق مواجهته، ط 2، دار الحسن للنشر والتوزيع، عمان،الأردن،2017، ص248.

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

[3]- جمال علي الدهشان، المرجع السابق، ص 166.

الفرع الثاني: الخصائص الخاصة

أولا- تزايد خطورته في الدول التي تدار بنيتها التحتية بالحواسب الآلية والشبكات

ففي ظل اعتماد أنشطة الحياة في المجتمعات المعاصرة على المعلوماتية وشبكة الانترنت، لنا أن نتصور النتائج المترتبة على وقوع هجوم إلكتروني على أحد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل، من خلال شن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية، بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه المتفجرات من كوارث، وربما يقوم أحد التنظيمات الإرهابية بهجوم إرهابي عن طريق الإنترنت على أحد البنوك والمصارف المالية بقصد السرقة والاستيلاء على الأموال، من أجل تمويل ذلك التنظيم الإرهابي.[1]

ثانيا- عدم توافر درجة عالية من اليقين في نتائج هجمات الإرهاب الإلكتروني

ففي الهجمات التقليدية يكون الموقع المستهدف محدد والأضرار من الممكن توقعها كما أنه يمكن إصلاح تلك الأضرار بشكل سريع لأنه يسهل اكتشاف مصادر الخلل على عكس الهجمات الإلكترونية، حيث يتميز بسرعة التنفيذ، فلا يتطلب تنفيذ الجريمة عبر الشبكة الوقت الكثير و بضغطة واحدة على لوحة المفاتيح بمكن أن تنتقل ملايين الدولارات المسروقة من مكان إلى آخر، وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة[2].

ثالثا- القدرة على التخفي وتجهيل مصادر المعلومات

تتميز جرائم الإرهاب الإلكتروني بأنها صعبة الإثبات لا توجد أدلة مادية واضحة كما هو الحال في الهجمات التقليدية ويرجع صعوبة إثباتها إلى العديد من الأسباب: من يقوم بارتكابها شخص ذو درجة كفاءة عالية، وارتفاع درجة الخداع والتضليل، واختلاف الزمان والمكان والقانون المطبق في الدولة التي ارتكبت فيها. فإذا قامت جهة ما بنسب

[1]- صادق عادل، المرجع السابق، ص167.

[2]- عطية محمد، المرجع السابق، ص249

هجمة أو إرهاب إلكتروني إلى جهة معينة، ستصطدم بتحدي "الإنكار المقبول"، إذ يمكن رفض هذه التهم بكل بساطة. وبسبب إمكانية إخفاء الهوية التي يتيحها الفضاء السيبراني، ولذلك تستغله الحكومات للتجسس وجمع المعلومات الاستخبارية، ولا توجد حتى الآن أية آليات فعالة لردع الجهات الحكومية عن القيام بهجمات سيبرانية.[1]

رابعا- رخص التكلفة

وهو ما يجعله عنصر جاذب للجماعات الإرهابية، ففي حين يحتاج الإرهاب الفعلي إلى أسلحة و مدرعات و قنابل و تحركات سرية جدا قد تصيب أو تخفق ناهيك عن التكاليف المادية لإنجاح هذه العمليات، يحتاج الإرهاب الإلكتروني إلى بعض المعلومات ليستطيع اقتحام الحواجز الإلكترونية، كما أن تكاليف القيام بهذه الهجمات لا تتجاوز جهاز حاسوب والدخول إلى الشبكة العنكبوتية.[2]

من هذه الخصائص يفهم أن الإرهاب الإلكتروني يهدف إلى تحقيق جملة من الأهداف أهمها:

- نشر الخوف والرعب بين الأشخاص والشعوب والدول المختلفة.
- الإخلال بالنظام العام والأمن المعلوماتي وزعزعة الطمأنينة.
- تعريض سلامة المجتمع وأمنه للخطر.
- إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال و المنشآت العامة والخاصة.
- تهديد السلطات العامة والمنظمات الدولية وابتزازها.
- الانتقام من الخصوم.
- الدعاية والإعلان وجذب الانتباه وإثارة الرأي العام.
- جمع الأموال والاستيلاء عليها.
- اغتيال الشخصيات السياسية والأمنية.

[1]- صادق عادل، المرجع السابق، 167.

[2]- جمال علي الدهشان، المرجع السابق، ص 166.

- العمل على تقويض النظام السياسي للبلاد.
- اغتيال رعايا الدول الأخرى انتقاما من سياسة دولهم.
- اختطاف وسائل النقل العامة أو تفجيرها.[1]

[1]– محمد بن عبد العزيز بن محمد العقيل، التحريض الإلكتروني على الإرهاب، مقال منشور في مجلة الفقه والقضاء السعودي، كلية الأمير نايف للعلوم الأمنية، جامعة الرياض، المملكة العربية السعودية،2011، ص 361.

المبحث الثاني: صور الإرهاب الإلكتروني

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

المطلب الأول: الصور التقليدية للإرهاب الالكتروني

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

الفرع الأول: التهديد والتجسس الإلكتروني

أولا- التهديد الإلكتروني

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

وأصبحت الجماعات الإرهابية تستغل شبكة الإنترنت العالمية من أجل بث الخوف و الرعب في نفوس الأفراد والدول ولقد تعددت الأساليب التي تستعملها في التهديد

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

عبر الإنترنت سواء بتهديد الضحية بنشر صور خاصة أو مقاطع فيديو أو فضح معلومات سرية مقابل دفع مبالغ نقدية طائلة، ويمكن أيضا استخدامه للإفصاح عن المعلومات السرية الخاصة بشركة أو مكان عمل ويحدث ذلك عن طريق استدراج الضحايا عن طريق البريد الإلكتروني أو مواقع التواصل الاجتماعي التي تستخدم من كل الفئات العمرية، كما يهدد بقتل الشخصيات السياسية في الدولة أو بتفجير مراكز سياسية أو تدمير البنية التحتية المعلوماتية عن طريق نشر الفيروسات لإتلاف الأنظمة المعلوماتية، في حين أن التهديد في السابق كان يتم عن طريق المراسلات الهاتفية أو التهديد المباشر[1].

وهذا من خلال بث عدد من النشرات والفيديوهات التي تظهر قوة وقسوة الجماعات الإرهابية، وصور تعذيب وقتل من يخالف أوامرها وتعليماتها، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار والدماء لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور[2].

والوحشية هي أبرز سمات هذه الجماعات التي فاقت كل تصور بوحشيتها الدموية، وقد لخصت إحدى الدراسات صور وأشكال الإرهاب الإلكتروني والتي يتم استخدام الفضاء الإلكتروني فيها بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال عدة أدوات، هذه الأدوات يصعب الفصل بينها بمعني أنه قد يتم استخدام كل هذه الأدوات في عملية واحده ويصعب الفصل بين الأدوات المستخدمة فيها.[3]

تعتمد جل التنظيمات الإرهابية في نشر رسائلها عبر مختلف صفحاتها الالكترونية على نظرية الرعب كمنهج يرمي الى تسويق مختلف المضامين الدعائية لها، ففي الوقت الحالي باتت الشبكات الاجتماعية تلعب دورا كبيرا في تغذية ودعم ظهور العنف والإرهاب والتطرف من خلال استغلال الإرهابيين لها في تسويق أغراضهم، فأصبح أسلوب الصدمة

[1]– غادة نصار، الإرهاب والجريمة الإلكترونية، ط2، دار العربي للنشر والتوزيع، القاهرة، مصر،2019، ص 49.

[2]– علي جابر، جرائم الانترنت، د ط، مكتبة زين الحقوقية، لبنان، 2018، ص 316.

[3]– هشام محمد، المرجع السابق، ص 129.

النفسية أو الخروج عن المألوف أو تحطيم كل القيم عوامل رمزية دعائية ووسائل اتصالية توظف من أجل كسب النصرة في مرحلة أولية ومن ثم التجنيد في صفوف المجامع المتطرفة التي تجعل من صور الدم والرعب جزء من نبل الحياة البشرية ومركزها لدى التنظيمات الإرهابية.[1]

ثانيا- التجسس الإلكتروني

لقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات وكذلك الأفراد ومراقبة المعلومات التي يتم تداولها حول العالم.

يعد التجسس من أقدم وأخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب، ولقد تطور عقب الطفرة التي حققتها التكنولوجيا والإعلام واستخدام الحواسب الآلية وشبكات الإنترنت، وأصبح الهاجس الأكبر للدول من أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات، ولا تكمن خطورته في استخدام الإنترنت بل في ضعف الرسائل الأمنية المختصة في حماية الشبكات الخاصة بالمؤسسات والهيئات.[2]

وفي هذا العصر أصبحت الحدود الجغرافية مستباحة بأقمار التجسس والبث الفضائي، الأمر الذي أصبح يهدد سيادة الدول، خاصة إذا كان من يستخدمها هم الإرهابيين، لأن الخطر الحقيقي في التجسس لا يكمن في العابثين أو المخترقين فمخاطر هؤلاء تعد محدودة وتقتصر عادة على العبث أو اتلاف المحتويات التي يمكن استعادة النسخة المخزنة منها في الغالب، ولكن الخطر الأكبر يظهر من خلال استخدام الإرهاب لهذه الجريمة على الأشخاص أو الدول أو المنظمات أو الهيئات الدولية أو الوطنية.[3]

---

[1]- عادل عبد الصادق، مكافحة الإرهاب الإلكتروني، ط 1، دار الكتاب الحديث، القاهرة، مصر، 2017، ص 187

[2]- حسين شفيق، الإرهاب الإلكتروني في العصر الحديث، ط 1، منشورات الحلبي الحقوقية، لبنان، 2017، ص 110.

[3]- غادة نصار، المرجع السابق، ص51.

وتستهدف عمليات التجسس الإرهابي ثلاثة أهداف رئيسية وهي التجسس العسكري والسياسي والاقتصادي، حيث تقوم التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة بالحصول على أسرار و معلومات الدولة من ثم إفشائها لدول أخرى معادية أو استغلالها بما يضر المصلحة العامة للوحدة الوطنية.[1]

حيث يقوم الإرهابيون المبرمجون الذين يسمون (الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء بما في ذلك البريد الإلكتروني، واشتراكات المستخدمين وما إلى ذلك.[2]

وبالتالي فإن ارتكاب جرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي في إطار جرائم الإرهاب الإلكتروني، يتم باستخدام الفيروسات الإلكترونية، بقصد الحصول على معلومات متعلقة بالأماكن و المنشآت الحيوية لاستهدافها بالعمليات الإرهابية، أو من أجل تدمير أو تعطيل في برامج الحواسيب، و من الأساليب المستخدمة لتدمير المواقع أيضا ضخ كميات هائلة من الرسائل الإلكترونية إلى الموقع المستهدف بالتدمير، مما يؤثر على سعته التخزينية، ويؤدي في نهاية المطاف إلى تفجير الموقع وتشتيت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه.[3]

[1]– عبد الرحمان بن عبد الله، الإرهاب الإلكتروني وطرق مكافحته، ط 3، أكاديمية نايف للعلوم الأمنية، المملكة العربية السعودية،2017، ص 128.

[2]– عادل عبد الصادق، المرجع السابق، ص 188.

[3]– علي جابر، المرجع السابق، ص 318.

الفرع الثاني: الحروب الإعلامية وغسيل الأموال

أولا:- الحروب الإعلامية

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

وقد لخصت إحدى الدراسات صور وأشكال الإرهاب الإلكتروني والتي يتم استخدام الفضاء الإلكتروني فيها بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال عدة أدوات، هذه الأدوات يصعب الفصل بينها بمعني أنه قد يتم استخدام كل هذه الأدوات في عملية واحده ويصعب الفصل بين الأدوات المستخدمة فيها.[1]

تسعى العديد من المواقع الالكترونية التابعة للجماعات الإرهابية الى نشر البيانات والتصريحات والكتب والنشرات، من أجل بث الأفكار المتطرفة التي تتبناها الجماعات الإرهابية التي قامت بالإنشاء، كما أنها تقوم على نشر الأخبار الكاذبة والمضللة لأجهزة الأمن والرأي العام، أو الآراء التي تسبب التفرقة، أو الإساءة إلى الأديان أو الأعراق أو الأصول، أو تشويه سمعة أشخاص أو جبهات معينة والتحريض ضدهم.[2]

وفي ذلك السياق يمكن أن يكون الهدف من استخدام الإرهابيين للتكنولوجيا نشر ثقافة العنف، والتشجيع على الاستخدام المفرط له، والانخراط في أعمال الإرهاب، من خلال نشر الجبهات الإرهابية لنصوص وصور وتسجيلات ومقاطع فيديو وألعاب إلكترونية، تتضمن مشاهد مروعة تحرض على العنف، وتروج لمثل هذه الأنشطة، وتنشر حالة من الرعب والخوف في الوقت ذاته.

---

[1]- نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2012، ص 38.

[2]- حسين شفيق، المرجع السابق، ص112.

ومع تزايد استخدام المعلوماتية مؤخرا، أصبح الانترنت وسيلة مهمة من الوسائل التي تلجأ إليها المنظمات الإرهابية لتوثيق عملياتها وتمجيد مرتكبيها، من خلال نشرهم أفلام مصورة توضح كيفية ارتكابها، وبيانات منظميها.[1]

ولعل الأمثلة الأبرز في هذا النطاق الأفلام التي نشرتها مواقع الكترونية تابعة لتنظيم الدولة الإسلامية في العراق وبلاد الشام، والتي أظهرت إحراق الطيار الأردني معاذ الكساسية حيا، ومن بعدها فيديو ذبح الرهائن المصريين الأقباط، مع الإشارة أن معظم الأشرطة التي نشرتها مثل هذه التنظيمات المتطرفة تتصف بالاستعانة بمهارات التصوير الفائقة، واستخدام التأثيرات السمعية والبصرية المتطورة، بغية التأثير في الجمهور، سواء بالترغيب من خلال استدرار عواطفهم ومحاولة كسب ودهم وتأييدهم للانضمام إليهم، أم الترهيب من أجل إضعاف معنوياتهم وتثبيط هممهم بتوجيه التهديدات إليهم وإرعابهم.[2]

كما تستخدم هذه المواقع الالكترونية وغيرها من التقنيات الحديثة بوصفها بنية نموذجية لتسهيل الحصول على مصادر الدعم المثالي واللوجيستي اللازم لتمويل الإرهابيين وأنشطتهم الإجرامية، ومن الممكن أن يتم ذلك من خلال الاستيلاء على الأموال عبر إجراء تحويلات غير مشروعة،أو من خلال القيام بعمليات تزوير وتزييف باستخدام الوسائل الالكترونية

المتنوعة أو عن طريق الاستيلاء على حسابات عملاء البنوك، مما تتدرج في هذا السياق الأنشطة الالكترونية التي ترتكب من خلال المنظمات الإرهابية جرائم غسيل الأموال، والتجارة بالمخدرات أو البشر أو الأسلحة وما إلى ذلك أو ما تقوم بيه الجمعيات الإرهابية العامة تحت الغطاء الإنساني أو التطوعي، باستغلال الوسائل التكنولوجية المختلفة في جميع التبرعات، التي يتم تحويلها دون علم المتبرعين بها لتمويل الجماعات الإرهابية.[3]

[1]– سماح عبد الصبور، الإرهاب الرقمي، د ط، معهد اليرموك للنشر، العراق، 2019، ص75.

[2]– أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، ط2، دار الحامد للنشر والتوزيع، الأردن، 2018، ص251.

[3]– عبد الرحمان بن عبد الله، المرجع السابق، ص129.

ثانيا- غسيل الأموال

تعد ظاهرة غسيل الأموال من الجرائم المستحدثة المحظورة قانونيا فهناك إجماع دولي على تحريمها مما دفع مرتكبيها إلى استخدام تقنيات حديثة ووسائل متطورة للتمويه والتعتيم والتضليل عبر شبكة معقدة من ترتيبات وإجراءات وعلى درجة عالية من السرية ومما لاشك فيه أن استخدامها لتلك التقنيات و الوسائل المتطورة جعلها من أخطر الجرائم وأكثرها شرا على الاقتصاد العالمي، وذلك بارتباطها بكافة أشكال الجريمة المنظمة وأخصها تجارة السلاح و المخدرات،[1] ودعم المنظمات الإرهابية بصورة مباشرة، فهي ترتبط بأنشطة غير مشروعة وعمليات مشبوهة، وتعتبر من الجرائم ذات الطابع الدولي فتزداد انتشارا يوما بعد يوم رغم كل الجهود الدولية الإقليمية المبذولة لمواجهتها.[2]

لقد أثبتت مختلف الدراسات وجود علاقة بين غسيل الأموال بصورتها التقليدية أو المعاصرة بحركات الإرهاب والتطرف والعنف الداخلي.

لقد أدى استعمال الوسائل التقنية الحديثة في جريمة غسيل الأموال إلى تسهيل إجراء العديد من العمليات المصرفية وتحويل الأموال في دقائق معدودة مما يصعب رصد حركة هذه الأموال كما ساهمت مواقع الانترنت في تبييض وتسهيل حركة الأموال الغير مشروعة.[3]

ويعد التبييض إحدى الركائز الضرورية التي يعتمد عليها الإرهاب لتمويل أعمالهم وأنشطتهم الإجرامية، وهناك علاقة وطيدة بينها خاصة باحتكاك كل منهما بالتكنولوجيا الحديثة وتظهر هذه العلاقة بصفة مباشرة بانتهاج الإرهابيين للإجرام المنظم في أعمالهم الإرهابية إلى جانب الاتجار بمعادن نفسية، والأسلحة والمخدرات وغيرها من المصادر

[1]- محمد حسن براوري، غسيل الأموال وعلاقته بالجرائم المعلوماتية، ط 2، دار القنديل للنشر والتوزيع، الأردن، 2017، ص188.

[2]- محمد إبراهيم زيد، الإرهاب والجرائم المعاصرة، د ط، دار الهدى للطباعة والنشر، القاهرة، مصر، 2009، ص 69.

[3]- محمد أمين بشرى، التحقيق في الجرائم المستحدثة، ط4،مركز الدراسات والبحوث، المملكة العربية السعودية، 2012، ص 214.

الأخرى الغير مشروعة بهدف الحصول على الأموال المشروعة التي يوظفونها لإتمام أعمالهم الإرهابية.[1]

كما أن العلاقة الوثيقة بينهما تدفع الإرهابيين للجوء لبعض أجهزة المخابرات والتجسس واستخدام الأموال الهاربة التي يتحصل عليها مختلف المجرمين كتجار المخدرات وتبييضها واستخدامها في تمويل الجماعات الإرهابية أو تأسيسها من أجل مزاولة أعمالها لغير المشروعة وعملياتها التخريبية والتدميرية المواجهة إلى أنظمة أو الحكومات معينة في مختلف الدول، عن طريق استخدام شبكة المعلوماتية وذلك بتأسيس مواقع الكترونية وقنوات قضائية لدعم تلك التنظيمات الإرهابية وتضليل الرأي العام، ومع اتساق نطاق العلاقة بينهما نصت الاتفاقيات الدولية في الآونة الأخيرة إلى إدراج جرائم الفساد والإرهاب ضمن جرائم غسيل الأموال بهدف تجفيف منابع الفساد والإرهاب.[2]

المطلب الثاني: الصور الحديثة للإرهاب الالكتروني:

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

الفرع الأول: تدمير واختراق المواقع الإلكترونية

أولا: تدمير المواقع الإلكترونية

ويتمثل فيما تتعرض له المجتمعات المعلوماتية الحديثة والدمار الذي قد يلحقه الهجوم الإرهابي بمنظومة المعلومات التي تتحكم في حياة هذه المجتمعات التي تعتمد على الكمبيوتر و الانترنت اعتمادا مطلقا والخسائر التي قد تنجم عن مثل المعلوماتية

[1]– حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 03، 2014، ص 82.

[2]– محمد حسن براوري، المرجع السابق، ص 71.

الحديثة والدمار الذي قد يلحقه الهجوم الإرهابي، فإرهاب الفضاء المعلوماتي أو إرهاب الانترنت يعتمد على القدرة على اختراق شبكات الانترنت لتحقيق أهداف عدوانية ذات طابع سياسي في الأغلب وإن كان يحلق وراءه وآثار سلمية تنال كثيرا من جوانب الحياة، كمهاجمة نظم التحكم الوطني في الطيران لإحداث تصادم بين الطائرات، و مهاجمة نظم التحكم الوطني في قطارات السكك الحديدية لإحداث تصادم بين القطارات، و تعطيل البنوك و عمليات التحويل المالي مما يلحق الأذى بالاستثمار الأجنبي و بالثقة في الاستثمار عامة، وإلحاق الأذى بالاقتصاد الوطني.[1]

تشير إلى محاولة اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وتخليق أنواع جديدة من الفيروسات التي تسبب الدمار لأجهزة الكمبيوتر وللمعلومات.[2]

أو عن طريق فيروسات الحاسب الآلي والتي تنتشر بسرعة كبيره عن طريق شبكة الانترنت، وذلك يرجع إلى عدد الملفات الهائل التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات هي عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط هذه الفيروسات تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها، ولها أضرار مختلفة تتمثل في فقد الملفات المخزنة وقد تصل تلك الأضرار إلى تحطم نظام التشغيل في الجهاز[3].

فما يتاح للإرهاب الإلكتروني سقفا لا يمكن تصور ارتفاعه في تنفيذ عمليات إرهابية، كميا ونوعيا، فقد تشن التنظيمات الإرهابية هجمات إلكترونية، بقصد تدمير المواقع والبيانات والنظم الإلكترونية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف ثلاثة أهداف أساسية وهي الأهداف: العسكرية، والسياسية، والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف، غالبا الثلاثة نفسها، وعلى رأسها مراكز القيادة

[1]– عبد الرحمان بن عبد الله، المرجع السابق، ص 130.

[2]– حكيم غريب، المرجع السابق، ص 83.

[3]– نورة طرشي، المرجع السابق، ص 40.

والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.[1]

وبالتالي فان ارتكاب جرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي في إطار جرائم الإرهاب الالكتروني. يتم استخدام الفيروسات الالكترونية، يقصد الحصول على معلومات متعلقة بالأماكن والمنشآت الحيوية لاستهدافها بالعمليات الإرهابية أو من أجل تدمير أو تعطيل في برامج الحواسيب، ومن الأساليب المستخدمة لتدمير المواقع أيضا ضخ كميات هائلة من الرسائل الالكترونية إلى الموقع المستهدف بالتدمير مما يؤثر على سعته التخزينية، ويؤذي في نهاية المطاف إلى تفجير الموقع وتشتت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه.[2]

ثانيا- اختراق المواقع الإلكترونية

يتم اختراق المواقع الإلكترونية لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل في الموقع تعلن اختراقه وكأنه بمثابة رفع راية النصر.[3]

يشير إلى الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، وبالتالي تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على استقبال الرسائل من العملاء، ويؤدي ذلك إلى التوقف عن العمل تماما.[4]

وتتمثل هذه الأضرار على سبيل المثال في: شل أنظمة القيادة والاتصالات، قطع شبكة الاتصال بيت الوحدات والقيادات المركزية، تعطيل أنظمة الدفاع الجوي، التحكم في خطوط الملاحة الجوية والبحرية والخطوط البرية، اختراق النظام المصرفي وإلحاق أضرار

[1]- عبد الرحمان بن عبد الله، المرجع السابق، ص131.

[2]- محمد معمري، الإرهاب في صوره الحديثة، ط1، منشأة المعارف، الإسكندرية، مصر، 2017، ص 71.

[3]- محمد حافظ الرهوان، مواجهة الإرهاب الحديث، ط3، دار هلا للنشر والتوزيع، القاهرة، مصر،2012، ص 228.

[4]- محمد حافظ الرهوان، المرجع نفسه، ص228

بأعمال البنوك وأسواق المال العالمية، ويتم استخدام تقنية المعلومات لإصابة المرافق الحيوية ومن ثم فإن الأهداف التي تتعرض للتهديد: تخزين المعلومات، عمليات إدخال المعلومات، إرسال واستقبال الرسائل، استهداف البنية التحتية للمعلومات وخاصة في قطاعات الكهرباء والاتصالات والكمبيوتر التي تعد وبحق ركائز الأمن القومي الجديد.[1]

وقد أدى الفضاء الالكتروني إلى تحول الإرهاب إلى تهديد عالمي، وأصبح الإرهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتصاعد نشاط الجماعات الإرهابية عبر الفضاء الالكتروني وتعزيز بعدها العالمي وثم استخدام المنجزات التكنولوجية في ممارسة الإرهاب، والتي استطاع الإرهابيون من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض.[2]

استغلت الجماعات الإرهابية بكافة أشكالها وأنماطها الفكرية المزايا الالكترونية كعنصر حيوي لدعم وتحقيق أهدافها، وتحولت بعد أن كانت مجموعات قلائل من الأفراد موزعة جغرافيا إلى مجتمع افتراضي غير محدد الأبعاد وكان ذلك له دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات، والإرهاب هو سلاح ضعيف غير قادر على شن حرب ضد الدولة، ومن ثم يلجأ إلى الإرهاب في محاولة منه إلى إلحاق الأذى بالقوى العظمى وهزيمتها، ويمثل الإرهاب وسيلة لتأكيد الهوية وجذب الانتباه.[3]

[1]– رامي متولي القاضي، مكافحة الجرائم المعلوماتية، ط 3، دار النهضة العربية، القاهرة، مصر، 2016، ص 113.

[2]– مصطفى محمد موسى، جرائم الكمبيوتر، ط 1، المركز العربي للدراسات القانونية، مصر، 2009، ص68.

[3]– مصطفى محمد موسى، المرجع نفسه، ص68.

الفرع الثاني: تبادل المعلومات وإدارة العمليات عبر الانترنت

أولا- تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها، و ذلك نظرا لقلة تكاليف الاتصال باستخدام الانترنت، مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفا بذلك عن النمط الهرمي القديم للجماعات الإرهابية، وكل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية.[1]

تستخدم الجماعات الإرهابية البريد الالكتروني وشبكات التواصل الاجتماعي والمنتديات وغيرها من وسائل الاتصال الحديثة، بوصفها و سهلة للتواصل وتبادل المعلومات والمقترحات فيما بين أعضائها، والتخطيط لعملهما، وذلك لهدف تقليل المخاطر الناجمة عن القيام باللقاءات المباشرة بين أعضاء الجماعات الإرهابية على ارض الواقع، أو التخفيف من استخدام الاتصالات التقليدية التي يسهل من خلالها تتبع الإرهابيين وإلقاء القبض عليهم.[2]

كما يمكنهم استخدامه لنشر أفكارهم والترويج لها، وكسب تعاطف الآخرين معها، وفي هاذ الإطار يقوم الإرهابيون كذلك باختراق البريد الالكتروني للأشخاص، من أجل تتبع مراسلاتهم والاطلاع على بياناتهم الشخصية والسرية، بغية الاستفادة منها في التخطيط لعملياتهم الإرهابية.

[1]- شعباني سيد أحمد، استخدام الإرهاب للتكنولوجيات، ط1، دار نايف للعوم، المملكة العربية السعودية، 2009، ص 17.

[2]- سويدان أحمد حسين، استراتيجيات الإرهاب الإلكتروني، د ط، دار النهضة العربية، القاهرة، 2006، ص189

وعلى سبيل المثال فقد كان من أوائل من وظف الوسائل الالكترونية في التواصل وبث الأفكار حيث أسس عام 1985 مجموعة بريد الكتروني للتواصل مع أتباعه وبعد "توم" أحد أشهر المتطرفين الأمريكيين، ومؤسس مجموعة المقاومة اليمنية العنصرية.[1]

ولا يقتصر الهدف من إنشاء الإرهابيين لمثل هذه المواقع على تقديم التعليم النظري أو الفكري وحسب، بل يتعداه إلى إعطاء التعليمات والإرشادات، وتقديم طرق لتعليم الأعضاء وسائل التخفي ومسح الأثر عن عيون الأمن، وتدريسهم على كيفية صناعة المتفجرات أو طريقة صناعة الأحزمة الناسفة وتركيبها، أو آلية اختراق المواقع الالكترونية وتدميرها وتعطيلها، أو الوسائل المستخدمة في نشر الفيروسات، أو طريقة التخطيط والتنسيق للأعمال الإرهابية، وما إلى ذلك من الأساليب المستخدمة لنشر الوعي الإرهابي بين الإرهابيين.[2]

ثانيا- إدارة العمليات الإرهابية عبر شبكة الانترنت

فالجماعات الإرهابية أصبح لها انتشار كبير على الانترنت، لها آلاف الصفحات والمواقع والتي تستخدمها في استقطاب الشباب من مختلف دول العالم، كما تستخدمها في الترويج لأهدافها وللدعاية الخاصة بها، ومن خلال ما أطلق عليه الحضانات الإلكترونية أو الجماعات الإرهابية الإلكترونية، فتنظيم القاعدة على سبيل المثال له العديد من المواقع الإلكترونية والصحف الإلكترونية والتي تصدر بلغات مختلفة، ومؤخرا ظهور تنظيم الدولة الإسلامية (داعش) والذي يستخدم الفضاء الإلكتروني بشكل واسع، له العديد من المواقع الإلكترونية والصحف والتي تصدر بلغات مختلفة ويستخدمها للترويج له[3]، حيث يقوم بنشر الأعمال الإرهابية التي يرتكبها والمصورة بتقنية عالية الجودة، كذلك الترويج لنمط حياة الأفراد في المناطق لتي يسيطر عليها التنظيم، وترويج وتضخيم لقوتهم لتشكيل صورة ذهنية عنهم بأنهم الأقوى والأخطر عالميا، وتتمثل خطورة الإرهاب الإلكتروني

[1]- إسماعيل عبد الفتاح، الإرهاب ومحاربته في العالم المعاصر، ط2، دار الكتاب العربي، القاهرة، مصر، 2009، ص 86.

[2]- جعفر حسن جاسم، جرائم تكنولوجيا المعلومات، د ط، دار البداية للنشر والتوزيع، الكويت، 2013، ص241.

[3]- مصطفى محمد موسى، المرجع السابق، ص 74.

بشكل كبير في سهولته بمعني القدرة على القيام بالهجمات الإرهابية من المنزل[1] وتعدد أشكاله وتنوع أساليبه وأدواته وقدرته الهائلة على التخريب والتدمير وتوفير قدر كبير من الأمان والسلامة للإرهابيين.

وقد رصدت إحدى الدراسات أشهر المواقع والنوافذ التي تطل من خلالها التنظيمات الإرهابية على العالم وأشهرها ثمانية عشر(18) شبكة إعلامية بعدة لغات، من بينها مؤسسة السحاب ومؤسسة الملاحم، ومؤسسة المنارة البيضاء، و وكالة أعماق الإخبارية، ومؤسسة الفرقان، ومؤسسة الحياة، ومؤسسة أجنا.[2]

أصبحت مواقع التواصل الاجتماعي أداة رئيسة للمجمعات الإرهابية تنشر أفكارها المتطرفة واستقطاب مجندين لها، خاصة بعد أن وصل عد مستخدميها إلى ما يقارب المليارى مستخدم، هذا ويعتبر موقع "فيسبوك"، أكثر وسائل التواصل الاجتماعي استخداما في تجنيد المتطرفين، حيث تقوم الجماعات الإرهابية بإنشاء "مجموعات" على "فيسبوك" من أجل اجتذاب الذين يتوافقون معها فكريا، وذلك من خلال إيهامهم بتبني قضايا ذات بعد إنساني، كدعم القضية الفلسطينية مثلا أو الحديث عن الإسلام بصفة عامة، ومع زيادة عدد الأعضاء المنتمين إلى هذه المجموعات، يتم تحميل المواد الجهادية تدريجيا بطريقة لا تتحالف مع سياسات الفيسبوك، من ثم يتم توجيه أعضاء المجموعة مباشرة إلى الموقع أو المنتديات المرتبطة بالجمعة الإرهابية.[3]

وتتيح الانترنت العديد من الإمكانيات لجميع مستخدميه، من حيث سهولة الاستخدام ورخص التكلفة والقدرة على التخفي والتمويه والتشتيت بين الأفراد، فضلا عن تسهيل الحصول على المعلومات والدخول على قواعد البيانات ومعظم الخدمات الحكومية، خاصة مع اتحاد كثير من الدول إلى تحديث أنظمتها وخدمتها الالكترونية.[4]

[1]– محمد حافظ الرهوان، المرجع السابق، ص 235.

[2]– سويدان أحمد حسين، المرجع السابق، ص204.

[3]– جعفر حسن جاسم، المرجع السابق، ص 251.

[4]– حكيم غريب، المرجع السابق، ص97.

يقوم الإرهابيين بإنشاء وتصميم مواقع على شبكة الانترنت لبث أفكارهم الضالة، الدعوة إلى مبادئهم المنحرفة، ولإبراز قوة التنظيم الإرهابي، والتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الالكتروني، والتدريب الالكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، وقد أنشئت مواقع إرهابية الكترونية لبيان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية الفتاكة ولشرح طرق اختراق البريد الالكتروني، وكيفية اختراق وتدمير المواقع الالكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات، ونحو ذلك.[1]

وقد سمحت ثورة الانترنت للمجموعات الإرهابية بإخفاء عملياتها بطرق جديدة، أكثر تعقيدا عن سابقتها التقليدية، فالجماعات الإرهابية أصبحت تدرك أهمية الانترنت من خلال ما يوفره من خدمات موثوق بها وشروط ميسرة، وهويات افتراضيه.[2]

[1]– عادل عبد الصادق، المرجع السابق، ص 195.

[2]– سماح عبد الصبور، المرجع السابق، ص 89.

خلاصة الفصل الأول

الإرهاب الإلكتروني هو إرهاب العصر الحاضر والمستقبل خاصة مع ما يشهده العالم من تطورات كبيرة في مجال التكنولوجيا والانترنت على وجه الخصوص، ما يجعله يقوم بعملياته على وجه السرعة وببساطة كبيرة.

لذلك كان لزاما التطرق إلى مفهوم الإرهاب الإلكتروني من خلال تعريفه لغة واصطلاحا، حيث تم توضيح إشكالات تعريف الإرهاب الإلكتروني ووضع العديد من التعريفات، ثم إبراز خصائصه المتمثلة في العصرية وتعدد أشكاله وتنوع أساليبه مع سهولة الاستخدام وصوره التقليدية منها والحديثة، والتي تعمل عل مهاجمة الأنظمة الإلكترونية للدول والأفراد وبث الرعب بين الشعوب

الفصل الثاني:

الفصل الثـــــاني: الآليات القانونية والأمنية لمكافحة الإرهاب الالكتروني

المبحث الأول: الآليات القانونية والأمنية لمكافحة الإرهاب الالكتروني على الصعيد الدولي

المبحث الثاني: الآليات القانونية والأمنية لمكافحة الإرهاب الالكتروني على الصعيد الوطني

مع التقدم الهائل في المجال التكنولوجي وما يشهده هذا العالم من قفزات نوعية في شتى المجالات ما جعل الانترنت تساهم وبشكل كبير في انتشار الجريمة وانتقالها بين الحدود بسرعة كبيرة الأمر الذي يصعب مواجهته نظرا لتداخل القوانين واحتكام كل دولة إلى اختصاصها القانوني، كان لزاما على الدول التكاتف من أجل مكافحة ظاهرة الإرهاب الإلكتروني وذلك بإبرام اتفاقيات ومعاهدات فيما بينها تساعد على مكافحة هذه الظاهرة تتمثل قوة الإرهاب الإلكتروني في قدرة الإرهابيين الكبيرة على استخدام الانترنت بدرجة عالية من الكفاءة، الأمر الذي أدى بالتشريعات الحديثة إلى مواكبة التطورات والسعي إلى سن قوانين من شأنها مكافحة هذه الظاهرة واسعة الانتشار، كما تهدف إلى حماية الفضاء الإلكتروني من التهديدات الإرهابية في هذا المجال.

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

المبحث الأول: الآليات القانونية والأمنية لمكافحة الإرهاب الإلكتروني على الصعيد الدولي

تعاني الدول والمجتمعات من ظاهرة الإرهاب الإلكتروني حتى أصبح من أهم وأكبر المشاكل في العصر الحديث وهذا لما يشكله من خطر كبير على الشعوب والدول وهذه الأخطار فرضت على الدول والمنظمات الدولية والإقليمية الاتفاق على مكافحة الإرهاب الإلكتروني يقينا منها بوجوب مواجهته والقضاء عليه نظرا لما يتسم به من خطورة بالغة، وهذا هو محور دراستنا في هذا المبحث:

المطلب الأول: الاتفاقيات الإقليمية لمكافحة الإرهاب الإلكتروني

ندرس في هذا المطلب جهود الاتحاد الأوروبي والمنظمات القارية في مكافحة الإرهاب الإلكتروني.

الفرع الأول: مكافحة الإرهاب الإلكتروني في المنظمات العالمية

أولا- منظمة الأمم المتحدة

أصدرت الأمم المتحدة عدة قرارات عبر جمعيتها العامة، في توضيح منها لتصاعد الاهتمام العالمي لاستخدام تكنولوجيا الاتصال و المعلومات استخدام غير سلمي، ففي 22 نوفمبر 2002 تبنت قرارا بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس السنة اتخذت قرارا آخرا بهدف إلى إرساء ثقافة عالمية لأمن الفضاء الالكتروني، واعتبر هذا القرار من بين أهم القرارات

التي استهدفت العمل على حماية البنية التحتية للمعلومات، وحث الدول والمنظمات الدولية على تكثيف جهود التعاون لمواجهة الإرهاب الالكتروني.[1]

وفي العام 2004، أشرف الأمين العام لمنظمة الأمم المتحدة آنذاك "كوفي عنان" على تشكيل فريق دولي لدراسة قضية إدارة الانترنت والمخاطر المترتبة عنها، إلى جانب إنشاء مجموعة الخبراء الحكومية بهدف مناقشة الأخطار القائمة والمحتملة في المجال الأمني المعلوماتي الدولي والإجراءات اللازمة والممكنة لوضع أسس دولية تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية.[2]

تحركت الأمم المتحدة لمواجهة ومكافحة خطر الإرهاب الالكتروني وفق مؤشر تصاعدي يبين بوضوح تطور الوعي الدولي بخاطر الإرهاب عبر الفضاء الالكتروني وتداعياته على الأمن الإنساني، ومثال ذلك ما أشار بيه الأمين العام "كوفي عنان" في تقرير الألفية الثانية، أن العولمة من أهم الأسباب التي ساعدت على انتشار الإرهاب الدولي والرقمي (الالكتروني)[3].

وإذا ما أخذنا في الاعتبار أن السياق الأممي جاء لمواجهة شتى صنوف العدوان، وإذا ما تم اعتبار الإرهاب الالكتروني واستخدام الحرب الالكترونية والرقمية يقعان ضمن دائرة هذا العدوان، فان قوة القانون تطبق هنا، لا سيما وأن ميثاق الأمم المتحدة في مادته

[1]– شفيق نوران، أثر التهديدات الإلكترونية على العلاقات الدولية، ط 1، المكتب العربي للمعارف، القاهرة، مصر، 2015، ص 108.

[2]– بوحادة سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، د ط، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، د س ن، ص 15.

[3]– محمد أمين الشوابكة، جرائم الحاسوب والانترنت، ط3، دار الثقافة للنشر والتوزيع، الأردن، 2012، ص 281.

الثانية (2) الفقرة الثالثة(3) قد أورد ما يلي: "يفض جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه يجعل السلم والأمن والعدل الولي عرضه للخطر".[1]

وتتقدم الأمم المتحدة قائمة المنظمات الدولية المعنية بمواجهة الإرهاب على اختلاف أصوله و أصنافه وأهدافه، بما في ذلك الإرهاب الالكتروني، بالنظر إلى قدراتها وخبراتها الواسعة في هذا المجال أضف إلى التأييد الدولي الذي تتمتع به، وعلى الرغم من كون ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية في إطار ما يعرف بالإرهاب الالكتروني إلا أن روح الميثاق تتفق وتنسجم مع تحريم استخدامه بوصفه انتهاكا وورد في الميثاق بخصوص التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة[2].

ومن ثمة لجوء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الالكتروني، يعرض السلم و الأمن الدوليين للخطر، لما فرضته من قيود خارجية على الإدارة الوطنية، ونتيجة تركيز الثروة في يد فئة محدودة (الدول الغنية)، وبالتالي وجوب تحويل هذه العولمة السلبية إلى عولمة ايجابية ينتفع بها الجميع بدلا من أن تكون وبالا على الكثير، يقول بهذا الشأن: "ولذلك فان التحدي الأساسي الذي نواجهه اليوم يتمثل في تحويل العولمة إلى قوة ايجابية يستفيد منها جميع سكان العالم، على أساس القوة التمكينية الكبيرة التي يقيمها السوق"[3].

بيد أن قوى السوق وحدها لن تحققها، والمطلوب هو بذل حدود أوسع لتهيئة مستقبل مشترك يقوم على إنسانيتنا بكل تنوعاتها...."، ولقد كانت الدعوة الأممية لدول

---

[1]– أحمد مصطفى منصور، مكافحة الدول للإرهاب الرقمي، ط2، منشأة المعارف الإسكندرية، مصر، 2016، ص158.

[2]– محمد مسعود قيراط، استراتيجيات مكافحة الإرهاب، ط 1، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية،2010، ص 08

[3]– شفيق نوران، المرجع السابق، ص 109.

العالم إلى اتخاذ الإجراءات ،والتدابير العلمية الفاعلة لمكافحة الأعمال الإرهابية (بما فيها الالكترونية) وملاحقة ومحاسبة مقترفيها عبر إلزامها بالآتي:

- الامتناع عن تقديم أي شكل من أشكال الدعم الصريح والضمني للكيانات الإرهابية.
- عدم توفير الملاذ لمن يمولون الأعمال الإرهابية أو يديرونها أو يرتكبونها.
- تعزيز التدابير الرامية إلى الكشف وفق المال و التمويل للأغراض الإرهابية.
- تشجيع الدول على تبادل المعلومات مع الدول الأعضاء
- دعوة المنظمات الدولية والإقليمية لتعزيز التعاون مع الأمم المتحدة في نطاق تواجدها.....
- ويقينا منا (الأمم المتحدة) أن جهاز الحاسب الآلي (الكمبيوتر) أصبح أكبر تهديد يواجه حق الإنسان بالخصوصية والحرية الشخصية والأمن، كونه يعد من أدوات المراقبة والتطفل خاصة إذا ما تم تخزين البيانات الشخصية إلى ذاكرته.[1]
- وبعد أحداث 11 سبتمبر 2001 أصبح الإرهاب الالكتروني أكثر شمولية وتطورا باستخدام المعطيات الثورة المعلوماتية وأشد فتكا على أمن الدول جميعا، فكانت استجابة الأمم المتحدة أكثر حزما وشمولا ، واتخذت في دوريتها 56 /258 بتاريخ:31جانفي 2002 قرار يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية، و أصبحت قضية أمن المعلومات المرتبطة بخطر استخدام تكنولوجيا الاتصال والمعلومات للتأثير أو الهجوم على وسائل تكنولوجيا الاتصال والمعلومات الخاصة بدول أخرى، مواقف تشكل للسلم والأمن الدوليين.[2]

وإجمالا، فان الأمم المتحدة أخذت في طريق مواجهة الإرهاب الالكتروني والجرائم المتصلة بالكمبيوتر والفضاء الرقمي ثلاثة محاور أساسية:

[1]– شفيق نوران، المرجع السابق، ص 110.

[2]– بوحادة سارة، المرجع السابق، ص 18

- الإدانة والتحذير من مخاطر الإرهاب بطوره الجديد وتطوير الوعي الدولي بتداعياته على السلم والأمن الدوليين عبر سلسلة من التطورات والجهود الأممية.
- ضرورة حرية التعبير والتنقل الحر للمعلومات والأفكار والمعرفة لمجتمع المعلومات(الشبكة المعلوماتية) مع الدعوة الى مراقبة الانترنت للحفاظ عللا السلم والأمن.
- المواجهة الأممية لمخاطر الإرهاب الالكتروني، بوضع استراتيجيات علمية وشاملة لمكافحة الإرهابية على أرض الواقع.[1]

ثانيا- المنظمة العالمية للملكية الفكرية

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

ثالثا- الإتحاد الدولي للاتصالات

نشأ بمقتضى اتفاقية باريس عام 1865 باسم "اتحاد التلغراف الدولي"، ثم عدل ليصبح الاتحاد الدولي السلكية واللاسلكية، انضم عام 1947.

يعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى على وضع المعايير المتعلقة بالأمن المعلوماتي ومكافحة الإجرام والإرهاب الالكتروني، وإذ يقوم بالاشتراك مع الوكالة

[1]- أحمد مصطفى منصور، المرجع السابق، ص 159.

[2]- طارق عزت رخا، المنظمات الدولية المعاصرة، ط، دار النهضة العربية ' مصر، 2006، ص 214.

الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات.[1]

ولقد طالبت بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، ولقد طالبت القمة العالمية لمجتمع المعلومات بتونس في نوفمبر 2005، بأن الاتحاد الدولي للاتصالات الآلية لبناء الثقة و الأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات، عبر إطلاق برنامج الأمن الالكتروني ،وعين لذلك فريق خبراء خلص إلى تقديم الاقتراحات الخمسة التالية: [2]

- يتم إسداء المشورة بشأن كيفية التعامل مع الأنشطة المعلوماتية من خلال وضع التشريعات متوافقة دوليا.
- بناء القدرات من خلال استراتيجية: زيادة الوعي، نقل الخبرة، تعزيز الأمن السيبرانية ....
- التركيز على التدابير الرئيسية الرامية إلى معالجة مواطن الضعف في منتجات البرمجيات.
- التعاون الدولي لوضع استراتيجية للحوار والتنسيق على الصعيد الدولي في مجال التصدي للأخطار الالكترونية.
- وضع هياكل تنظيمية بإطار عمل استراتيجيات الاستجابة، فيما يتعلق بمنع الهجمات السيبرانية وتتبعها والرد عليها وإدارة الأزمات المتعلقة بها، بما في ذلك أنظمة البنية التحتية الحرجة للمعلومات.[3]

[1]– سامر مؤيد عبد اللطيف ونوري الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مقال منشور في مجلة كربلاء العلمية، جامعة اليرموك، العراق، العدد 18، 2018، ص 20.

[2]– سامر مؤيد عبد اللطيف ونوري الشافعي، المرجع السابق، ص 21.

[3]– محمد أمين الشوابكة، المرجع السابق، ص 287.

الفرع الثاني: مكافحة الإرهاب الإلكتروني في المنظمات القارية

وفي شهر أكتوبر 1999 اجتمع في موسك وزراء العدل والداخلية للدول الثماني الكبار وطلبوا من ممثليهم وضع خيارات وحلول عملية تسمح بكشف ومتابعة الاتصالات الالكترونية الدولية في إطار التحقيقات الجنائية. وقد صدر عنهم التصريح التالي: "بغية التأكيد من أننا جميعا نستطيع أن نحدد مكان وهوية المجرمين الذين يستخدمون الاتصالات الالكترونية لأهداف مشروعة. يجب علينا أن نزيد قدراتنا على اقتفاء أثر وكشف هذه الاتصالات أثناء وبعد إجرائها حتى وان كانت تلك الاتصالات تمر عبر الدول. ولما كانت الإجراءات الخالية تتسم بالبطء وتتم في إطار تعاون ثنائي فقط بدلا من أن تهدف الى مواجهة الجرائم بصفة مطلقة. لذلك يجب أن يتعاون الجميع مباشرة من أجل مكافحتها وإيجاد حلول سريعة وحديثة.[1]

وفي 12 أفريل 2000 تم توقيع اتفاقية منظمة مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية بإشراف منظمة الأمم المتحدة التي أكدت في مادتها الأولى على أنه "ينبغي أن تكفل عدم توفير قوانينها وممارساتها ملاذا أمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية". كما توجت الجهود التي بذلها الاتحاد الأوروبي والمجلس الأوروبي بصدور اتفاقية بودابست لمكافحة جرائم المعلوماتية (الجرائم الالكترونية)، وتعرف بالاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية.[2]

[1]– وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة المنار، تونس، 2014، ص204.

[2]– علي يوسف شكري، المنظمات الدولية، د ط، دار الصفاء للنشر والتوزيع . الأردن، 2016، ص 59.

ووضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في 23 /2001/11 ودخلت حيز التنفيذ في 2004، وتعتبر الاتفاقية متاحة أمام أي دولة من دول العالم للانضمام إليها.

واشتملت الاتفاقية على 48 مادة موزعة على أربعة فصول الأول تعريف المصطلحات المستخدمة وتناول الفصل الثاني الإجراءات الواجب اتخاذها على المستوى المحلي في مجال قانون العقوبات والإجراءات الجنائية وقواعد الاختصاص القضائي، ويهدف الفصل الثالث إلى تنظيم التعاون الدولي، ويضم الفصل الرابع والأخير الشروط الختامية.[1]

وفي إطار هذا 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 الالكتروني لهذه الجرائم"، كما أنه يمكن لكل طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريع مثل الفاكس أو البريد الالكتروني على أن تستوفي تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها للمساعدة في ذلك.[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 الجرائم الحاسوبية، حيث احتل هذا النوع من

[1]- ناصر بن محمد، مكافحة جرائم الإرهاب المعلوماتي، ط 1، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، 2010، ص11.

[2]- ناصر بن محمد، المرجع نفسه، ص 11.

الجرائم موقعا بارزا على جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها.[1]

وفي إعلان قمة شيكاغو في اجتماع مجلس شمال الأطلس في 20 ماي 2012 تم التأكيد على ضرورة دمج إجراءات الدفاع الالكتروني في هياكل وإجراءات الحلف، مع الالتزام بتحديد وتوفير قدرات الدفاع الالكتروني الوطنية التي تعزز التعاون والعمليات المشتركة بين دول الحلف، بالإضافة إلى تطوير قدرات الدول الأعضاء بصورة أكثر لمنع الهجمات الالكترونية واكتشافها والتصدي لها ومعالجة التهديدات الأمنية الالكترونية بالاشتراك مع الدول الشريكة المعنية في إطار كل حالة بمفردها، وكذلك مع المنظمات الدولية. ومن بينها الاتحاد الأوروبي على النحو المتفق عليه ومجلس أوروبا و الأمم المتحدة ومنظمة الأمن والتعاون في أوروبا من أجل زيادة التعاون الملموس.[2]

المطلب الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الإقليمية

سوف نتطرق في هذا المطلب إلى جهود كل من الاتحاد الأوروبي وجامعة الدول العربية في مكافحة الإرهاب الإلكتروني.

[1]– صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص 94

[2]– وليد الكشباطي، المرجع السابق، ص 206.

الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتحاد الأوروبي

لعب المجلس الأوروبي دورا مهما في محاولة الحد من الجرائم الالكترونية والإرهاب الالكتروني ، من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصيغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات ، وفي 28/ 1981/01 تم توقيع الاتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصيغة الشخصية وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحساب وهي التوصية التي حققتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية. وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد اتفاقية في هذا الإطار[1].

وقد أثمرت جهود الاتحاد عن ميلاد أول المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية والإرهاب الالكتروني بالعاصمة المجرية بودابست عام 2001، وقد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وانسجام التشريعات الوطنية ببعضها البعض، وتعزيز قدرات القضاء وكذا تحسين التعاون الدولي في هذا الإطار[2].

إضافة إلى تحديد عقوبات جرائم المعلوماتية في إطار القوانين المحلية، ما قام به المجلس في هذا المجال هو إشرافه على اتفاقية بودابست الموقعة ورغم ان هذه الاتفاقية في الأصل أوروبية الميلاد إلا أنها دولية الطابع تظهره من بعد حقيقي عن الاهتمام

[1]– سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2013، ص 85.

[2]– عبد الصبور عبد القوي، الجريمة المعلوماتية، ط 1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2013، ص 319.

الدولي بهذه النوعية من الجرائم ، حيث أعد مجلس أوروبا هذه الاتفاقية بالتعاون مع كندا واليابان وجمهورية جنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في 01 /2001/11 ودخلت حيز التنفيذ في 2004/07/01، تهدف الاتفاقية إلى إرساء نظام سريع وفعال للتعاون الدولي ، وبالتالي فهي تتضمن الاتفاقية أحكاما تهدف الى استحداث هكذا إطار في سبيل تعاون دولي سريع وموثوق وتطلب من الدول الأطراف مد بعضها البعض بمختلف أشكال التعاون.[1]

وقد بينت المذكرة التفسيرية لهذه الاتفاقية أن تحديد الجرائم الالكترونية فيها هدفه تحسين وإصلاح وسائل منع وقمع الجريمة المعلوماتية من خلال تحديد معيار بالحد الأدنى المشترك، الذي يسمح باعتبار بعض التصرفات من قبيل الجرائم المعلوماتية، وأنه بالإمكان أن يتم استكمال هذه القائمة في القوانين الداخلية ، كما أنه يأخذ في الاعتبار الممارسات غير المشروعة الأكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد، وقد حددت الاتفاقية (اتفاقية بودابست) الجرائم الالكترونية وصنفتها في خمسة عناوين في القسم الأول من الاتفاقية.[2]

أولا– ويضم جوهر جرائم الحاسب أو جرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم وإتاحة البيانات والنظم.

ثانيا– ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي.[3]

[1]– صغير يوسف، المرجع السابق، ص100.

[2]– ناصر بن محمد، المرجع السابق، ص 15.

[3]– نورة طرشي، مكافحة الجريمة المعلوماتية، المرجع السابق، ص 67

ثالثا– ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى، وهي التي تخص الإنتاج والنشر الغير المشروع ، في المادة التاسعة من الاتفاقية.

رابعا– ويشمل الجرائم المنظمة بالاعتداء على الملكية والحقوق المرتبطة بها في نص المادة العاشرة من الاتفاقية.

خامسا– وهو يشتمل على أحكام إضافية بخصوص الشروع والاشتراك و أيضا الإجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوي.

كما أنشأ الاتحاد الأوروبي أجهزة لتساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوروبول والمركز الأوروبي لمكافحة الجريمة والإرهاب الالكتروني، الذي افتتح في جانفي 2013.[1]

الفرع الثاني: مكافحة الإرهاب الإلكتروني في جامعة الدول العربية

في العالم العربي توجد بعض التشريعات التي تغطي جرائم المعلوماتية والحاسب بشكل أو بآخر خاصة في تونس والمغرب والمملكة العربية السعودية والأردن والإمارات العربية المتحدة وعمان وقطر.

ولقد حققت دول المجلس التعاون لدول الخليج العربية تقدما ملحوظا في مجال استخدامات تكنولوجيا المعلومات. وقد حظيت دولة الإمارات العربية المتحدة بموقع ريادي في هذا المجال، وقد استدعى هذا التقدم اتساعا في الثغرات التي تمكن "الإرهابيين الالكترونيين" من شن هجماتهم. وهو الأمر الذي حدا بخبراء دوليين إلى اعتبار أن "حكومات دول الخليج العربي عرضة لمخاطر كبيرة من الإرهاب الالكتروني عبر

[1]– نورة طرشي، مكافحة الجريمة المعلوماتية، المرجع السابق، ص 67.

الانترنت". مشيرين الى "هذه المخاطر تتفاقم مع مرور الأيام لأن التقنية وحدها غير قادرة على حماية بيانات الحكومات بشكل كلي من الهجمات المتوقعة".[1]

وتعتبر دولة الإمارات العربية أول دولة عربية تسن قانونا مستقلا لمكافحة الجرائم المعلوماتية. وفي هذا السياق تنص المادة 21 من القانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على أنه: "كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقيادتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على الخمس سنوات".[2]

وتجدر الإشارة إلى أن المشرع الإماراتي قد نص صلب المادة 7 من قانون (1) لسنة 2004 بشأن مكافحة الإرهابية على معاقبة كل من يقوم بتدريب شخصا أو أكثر على استعمال الأسلحة التقليدية أو غير التقليدية أو وسائل الاتصال السلكية أو اللاسلكية أو الالكترونية أو أية وسيلة اتصال أخرى أو عمله فنونا حربية أو أساليب قتالية أيا كانت بقصد الاستعانة به لتنفيذ عمل إرهابي بالسجن المؤبد أو المؤقت[3].

ولقد صدرت في المملكة العربية السعودية بعض لأنظمة واللوائح و التعليمات والقرارات لمواجهة الاعتداءات الالكترونية والإرهاب الالكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء

[1]– عبد الصبور عبد القوي، المرجع السابق، ص 326.

[2]– محمد أمين الشوابكة، المرجع السابق، ص 293.

[3]– سامر مؤيد عبد اللطيف ونوري الشافعي، المرجع السابق، ص22.

رقم (163) في: 1417/10/24 هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها.[1]

كما نص القرار على تكوين لجنة دائمة برئاسة وزارة الداخلية وعضوية وزارات: الدفاع، المالية، والثقافة والإعلام، والاتصالات وتقنية المعلومات، والتجارة والشؤون الإسلامية، والتخطيط، والتعليم العالي، والتربية والتعليم، ورئاسة الاستخبارات، ومدينة الملك عبد العزيز للعلوم والتقنية، وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام (الانترنت) والتنسيق فيما يخص الجهات التي يراد حجبها ولها على الأخص ما يلي:

- الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للأنترنت والتي تتنافى مع الدين الحنيف والأنظمة.
- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة الشبكة الوطنية.

وهذا القرار يبين مبادرة المملكة العربية السعودية وسعيا لتنظيم التعاملات الالكترونية وضبطها.[2]

كما تم إصدار أنظمة تحد من جرائم الإرهاب الالكتروني وفي هذا السياق تم إقرار نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 وتاريخ:8 /3/ 1428 هجري بناء على قرار مجلس الوزراء رقم (79) وتاريخ1428/3/7 هجري الذي فرض عقوبات بالسجن والغرامة أو كليهما معا على كل شخص ينشأ موقعا لمنظمات إرهابية على شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أو نشر كيفية صنع المتفجرات.

[1]– طارق عزت رخا، المرجع السابق، ص 219.

[2]– أحمد مصطفى منصور، المرجع السابق، ص 164.

وفي هذا السياق تنص المادة السابعة من هذا القانون على أنه "يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال. أو بإحدى هاتين العقوبتين كل شخص يقوم بإنشاء موقع منظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهره الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أداة نستخدم في الأعمال الإرهابية".[1]

وفي المغرب تفطن المشرع المغربي لخطورة انتشار الإجرام المعلوماتي وأثر ذلك على أمن واستقرار المجتمع المغربي ، وقد ظهر ذلك مع عرض المشروع القانون المتعلق بالإرهاب على مجلس الوزراء بتاريخ 16جانفي 2003. حيث وردت لأول مرة الإشارة إلى إمكانية ارتكاب أفعال إجرامية إرهابية عن طريق المعالجة الآلية للمعطيات.[2]

وما يلفت النظر هو أن القانون المغربي رقم 03-03 المتعلق بالإرهاب بعد أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمديه بمشروع فردي أو جماعي يهدف الى المساس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف. فالفصل1-218 حدد بعض الأفعال المجرمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات الفقرة 7، وذلك بعد محاولة تحديد مفهوم الإرهاب في مستهل هذا الفصل.[3]

ومما تجدر الإشارة إلية عند الحديث عن القانون المغربي رقم 03-03 المتعلق بمكافحة الإرهاب أن الفصل 2-218 منه عاقب على استعمال وسائل الإعلام ومنها الالكترونية في الإشادة بالأعمال الإرهابية. وقد حدد الفصل المذكور العقوبة في الحبس

[1]- محمد مسعود قيراط، المرجع السابق، ص24.

[2]- سماح عبد الصبور، المرجع السابق، ص101.

[3]- هشام محمد، المرجع السابق، ص 149.

من سنتين إلى ست سنوات وبغرامة بين 10 ألاف و200 ألف درهم. ومعلوم أن وسائل الإعلام الالكترونية متعددة من أبرزها الشبكة الدولية للمعلومات الانترنت.[1]

وفي السودان صدر قانون جرائم المعلوماتية لسنة 2007 الذي ينص في الفصل الخامس منه على أنه "كل من ينشأ أو يستخدم موقعا على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابية تحت أي مسمى لتسهيل الاتصال بقيادتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد لحارقة أو المتفجرة أو أية أدوات نستخدم في الأعمال الإرهابية يعاقب السجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو العقوبتين معا".[2]

أما المشرع الأردني فقد نص صلب المادة 10 من قانون جرائم أنظمة المعلومات لسنة 2010 على أن "كل من استخدام نظام المعلومات أو الشبكة المعلوماتية أو أنشأ موقعا الكترونيا لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة".[3]

أما في قطر فقد صدر القانون رقم 14 لسنة 2014 المتعلق بمكافحة الجرائم الالكترونية الذي نص صلب المادة 5 منه على أن: "يعاقب القانون بالحبس مدة تتجاوز ثلاث سنوات والغرامة 500 ألف ريال لإدارة موقع يتبع تنظيما إرهابيا، أو نشر أخبار

[1]– عبد المجيد الحلاوي، التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، مداخلة مقدمة في الدورة تدريبية حول مكافحة الجرائم الإرهابية المعلوماتية أيام 09-14 أفريل 2006، جامعة محمد الخامس، الرباط، المغرب.

[2]– الأخضر عمر الذهيمي، دور المنظمات الدولية في التصدي للإرهاب، ط1، جامعة نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية، د س ن، ص 174.

[3]– عطية محمد، المرجع السابق، ص263.

تعرض الدولة للخطر أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية".[1]

[1]– محمد القاسم وآخرون، تجارب الدول في مكافحة الجرائم المعلوماتية، ط 2، المركز الأمني للدراسات الاستراتيجية، الدوحة، قطر، 2019، ص 55.

المبحث الثاني: الآليات القانونية والأمنية لمكافحة الإرهاب الإلكتروني على الصعيد الوطني

تتطلب مكافحة الإرهاب الإلكتروني جهودا كبيرة من الدولة مقارنة مع الجهود الدولية المبذولة لمكافحته، وذلك من خلال سن تشريعات جديدة تواكب التطور الحاصل في المجال الإلكتروني، ويجب أن تكون هذه المواجهة من جميع الجوانب القانونية والعسكرية والفكرية، بعد معرفة الجهود الدولية في مكافحة الإرهاب الإلكتروني يتوجب معرفة كيفية مواجهة القانون الجزائري لهذه الظاهرة، وهو موضوع دراستنا في هذا المبحث

المطلب الأول: الاستراتيجية الجزائرية في مكافحة الإرهاب الإلكتروني

تعتبر الجزائر من أوائل الدول التي عانت من ويلات الإرهاب سواء التقليدي أو الحديث بجميع صوره بما فيه الإلكتروني منه، وقد اتخذت العديد من الإجراءات في سبيل مواجهته والتصدي له من خلال اعتباره من أولويات السلطات العليا في البلاد، وذلك من خلال ما يلي:

الفرع الأول: الإجراءات الوقائية لمكافحة الإرهاب الإلكتروني

أولا- إنشاء مركز التوجيه العسكري في عمليات مكافحة الإرهاب

إن التطورات والأزمات التي مرت بها الكينونة الأمنية الجزائرية في العقد الأخير من القرن العشرين، قد أظهرت بشكل جلي التحديات الأمنية الخطيرة التي مر بها النظام الأمني الجزائري في مواجهة التهديدات التي يثيرها الإرهاب الحديث، وعلى هذا الأساس يأتي مركز التوجيه العسكري في عمليات مكافحة الإرهاب ليقوم على مقاربة إجرائية

للحصول على نتائج استراتيجية أو أثر عملياتي على التنظيمات الإرهابية المنتشرة إلكترونيا وحدوديا على وجه التحديد، وذلك من خلال تبني آلية متعددة الجوانب على أوسع مدى للقدرات العسكرية و الأمنية،[1] فهذه الجزئية تعتبر مقاربة تكيفية تتخذ شكلا متداخلا لتمتد و تشمل الأبعاد الميدانية والعملياتية والاستراتيجية لأي اشتباك، كما أنها تعتمد على استخدام قدرات أمنية استخباراتية تشوه سلوك الجماعات الإرهابية وعمق تفكيرها، لاسيما على مستوى مختلف المضامين الإلكترونية المتطرفة التي تحتويها شبكات التواصل الاجتماعي.[2]

إن الهدف الرئيسي لهذا المركز، يتوقف على المستوى الاستراتيجي بحيث يجري التخطيط للعمليات الأمنية المجدية في السياق الاستخباراتي من أجل تحديد هدف التنظيمات الإرهابية بطريقة فعالة تسهل تحقيق كل الأهداف المحددة، و المتبلورة في استخدام المؤسسة العسكرية الجزائرية نهج الاختراق والحرب في العمق ضد المواقع الإلكترونية الإرهابية.[3]

إن التحديات الأمنية لمؤسسة الجيش في الوقت الراهن تغيرت وتشبعت أيضا على كل الجبهات ففي ظل تغول شبكات إرهابية دولية متناثرة في كل الأوطان، والأكثر خطورة تواجدها الرهيب في الفضاء السيبراني، وانطلاقا من هذا السياق المتشعب، فإن وزارة الدفاع الوطني بمختلف وحداتها تعمل بالإضافة إلى المستوى الميداني والتعبوي بالتركيز على الجانب الاستراتيجي من أجل استهداف القيادة المحورية للتنظيمات والجماعات

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

[2]– ميلود صولي، السياسة الجزائرية في مواجهة المضامين الإلكترونية الإرهابية عبر شبكات التواصل الإجتماعي، مجلة الاتصال والصحافة، الجزائر، العدد التاسع، 2018، ص 188.

[3]– أحمد فتحي سرور، استراتيجيات الدول في مكافحة جرائم الإرهاب، ط 1، منشأة المعارف، الإسكندرية، مصر، 2014، ص347.

الإرهابية فضلا عن إيقاع الفوضى في صفوفها حتى لا تستطيع إيصال تعليماتها إلى خلاياها وتجنيد عناصر جديدة في صفوفها.[1]

وبالنظر إلى تزايد حجم التهديدات الإرهابية الخطيرة على الجزائر، تم في نهاية 2014 استحداث لجنة أمنية مشتركة متخصصة في مجال مكافحة الإرهاب من طرف وزارتي الداخلية والدفاع، بالإضافة إلى تعقب المنتديات الجهادية في مسعى جديد يأتي في ظل تنامي المخاطر الأمنية وعلى خلفية تزايد نشاط شبكات التجنيد التي تم تفكيكها من طرف وحدات الدرك الوطني و مصالح الأمن و الجيش في العديد من ولايات الجمهورية، وبعدما كشفت أيضا الكثير من التحريات الأمنية الدقيقة عن وجود صفحات بمواقع للتواصل الاجتماعي تروج للأفكار الجهادية المتطرفة، وتعمل أيضا في الجهة المقابلة على استقطاب مقاتلين مفترضين عبر الإنترنت في سبيل الالتحاق بصفوف الجماعات الإرهابية في كل من العراق و سوريا و ليبيا[2].

ثانيا- إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

لقد عرفت الجزائر أزيد من 100 جريمة الكترونية سنة 2014 وتضاعف هذا العدد خلال السداسي الأول لسنة 2015 ، حيث سجلت المصالح الأمنية أزيد من 200 جريمة الكترونية متنوعة ، وفي هذا الإطار عملت الدولة الجزائرية على تأسيس الهيئة الوطنية للوقاية من الجرائم الالكترونية ومكافحتها في 09 أكتوبر 2015، بعدما وقع رئيس الجمهورية على مرسوم رئاسي يقضي بإنشاء هذه الجديدة[3]، والتي تعد بمثابة سلطة إدارية مستقلة لدى وزير العدل، كما تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير

[1]- ميلود صولي، المرجع السابق، ص 188.

[2]- بلهول نسيم، المرجع السابق، ص 17

[3]- المرسوم الرئاسي رقم 261/15،المؤرخ في 2015/10/09، المتضمن تأسيس الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها.

العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقاء.

كما تضم الهيئة قضاة وضباطا تابعين لمصالح الاستعلامات العسكرية والدرك والأمن الوطنيين، وأعوانا من الشرطة القضائية وفقا لأحكام قانون الإجراءات الجزائية. وتكلف هذه الآلية الجديدة، باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الحديثة، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام[1].

وهنا على سبيل المثال كمحاربة كل المضامين الإرهابية المتطرفة التي تدعو إلى الغلو الديني أو تسعى إلى تجنيد الشباب الجزائري في صفوفها، كما تعمل هذه الهيئة على جمع المعلومات والتزويد بها من خلال الخبرات القضائية وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي واستثناء هيئات وطنية أخرى.[2]

الفرع الثاني: حماية الفضاء المعلوماتي من جرائم الإرهاب الإلكتروني

أولا- السماح بالمراقبة الإلكترونية وأنظمة الحجب

من الضروري على الحكومات والدول فرض الرقابة والسيطرة على كل ما يقدم من خلال شبكة الإنترنت، في إطار إيجاد بيئة إلكترونية خالية من الجريمة والإرهاب.

[1]- إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، الجزائر، العدد 630، 2016، ص44

[2]- إلهام غازي، المرجع نفسه، ص 44.

أ- المراقبة الإلكترونية

وهي عبارة عن إجراء مميز يتطلب السرية بطبيعته، يتم اللجوء إليه إما للحيلولة دون وقوع الجريمة كإجراء وقائي فيما يخص الجرائم الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وقد يتم اللجوء إليه بعد ارتكاب الجريمة في إطار التحقيقات القضائية الجارية أو مستلزمات التحقيق بشأن بعض الجرائم المحددة قانونا[1] .

وقد كرس المشرع الجزائري المراقبة الإلكترونية من خلال مضمون القانون رقم 04/09،[2] في مادته الثالثة والتي تنص على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية لتجميع وتسجيل محتواها[3].

يجب على الدول فرض رقابة على كل ما يقدم عبر شبكة الإنترنت، لمنع الدخول للمواقع التي يتضمن محتواها مواد تتعلق بالإرهاب، فضلا عن مراقبة الاتصالات عبر شبكة الإنترنت والبريد الإلكتروني بهدف ضبط المجرمين وتفتيشهم، وجمع الأدلة لإدانتهم وتقديمهما للمحاكمة. ويجب أن تكون هذه المراقبة مشروعة وتحقق التوازن بين حق الأفراد في الخصوصية وحق المجتمع في مكافحة الجريمة.[4]

لا تعني الرقابة المنع من استخدام شبكة الإنترنت، لكنها تدبير وقائي، لمنع وقوع الجرائم، فالرقابة على الإنترنت هي التحكم في النشر والوصول إلى المعلومات على الإنترنت، وتستخدم الرقابة تقنية تعتمد على الجدار الناري أو البروكسي، ويتم ذلك من

---

[1]- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، ط 7، دار النهضة العربية، القاهرة، مصر، 1993، ص 131

[2]- قانون رقم 04/09 مؤرخ في 2009/08/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، ط 1، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2015، ص 186.

[4]- نور الله تلة، المرجع السابق، ص 167.

خلال إجبار المتعاملين مع الشبكة على المرور عبر خوادم البروكسي قبل الوصول إلى الشبكة،[1] فمزودات خدمة الإنترنت تتسلم وتنظم كل الطلبات، وتستخدم برامج تحسس الرقم الخاص IP، مما يعطي بعض البيانات عن المستخدم حتى لو استخدم اسم وهمي لدخول الشبكة، ويوجد برامج عدة للمراقبة الإلكترونية وبرامج متخصصة بجمع الأدلة والقرائن من رسائل البريد الإلكتروني، فعلى سبيل المثال: توظف الصين مليوني شخص لمراقبة الأنشطة على شبكة الإنترنت، حيث تعد شبكة الإنترنت في الصين من أكثر الشبكات التي تشهد سيطرة ورقابة حكومية صارمة في العالم، حيث تعد مواقع الإنترنت تحت الرقابة الجبرية الدائمة، بل وصل الأمر إلى حد التدخل لحذف التعليقات ذات الحساسية بصورة روتينية على مواقع الشبكات الاجتماعية.[2]

ب- أنظمة الحجب

من أهم ما يجب توافره في هذا الصدد حجب المواقع الضارة التي تدعو إلى الشر و الفساد، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، والقيام بالإجراءات كلها بما في ذلك ترشيح المحتوى.

ولقد جاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسب الجرائم.[3]

ثانيا- حماية الأنظمة من الاعتداءات الإلكترونية

تتم الحماية من الاعتداءات الالكترونية سواء كانت إرهابية أو غيرها، بوسائل فنية عدة منها:

[1]- نور الله تلة، المرجع السابق، ص 168.

[2]- عبد الرحمان بن عبد الله سند، المرجع السابق، ص 23.

[3]- عبد الرحمان بن عبد الله سند، المرجع نفسه، ص 24.

- تشفير البيانات المنقولة عبر الانترنت، سواء كانت منقولة عبر وسائل الاتصالات أو عبر الألياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة، لأن عملية التشفير مكلفة.[1]
- إيجاد نظام أمني متكامل يقوم بحماية البيانات والمعلومات.
- توفير برامج الكشف عن الفيروسات لحماية الحاسب والبيانات والمعلومات من الإضرار بها.
- عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية،
- عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة.
- استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد أو الصوت.
- استخدام كلمة مرور، حيث تعد كلمة المرور من ابسط أشكال الحماية وبفضل اختيار كلمة مرور ذات بنية قوية، ويجب مراعاة تغييرها الدوري، وسندرس في هذا الفرع عن بعض هذه الوسائل بشيء من الإيجاز[2]

أ- نظام التحقق من الهوية

يشير مفهوم التعرف بالهوية إلى التعرف الايجابي الدقيق بهوية مستخدمي الشبكة ومضيفاتها، وتطبيقاتها، وخدماتها، ومصادرها.

يوجد تقنيات عدة للتحقق من الهوية وخصوصا بأساليب التحقيق البيولوجي من الهوية، بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص، حيث تعتمد هذه

[1]- بوحادة سارة، المرجع السابق، ص 31.

[2]- نور الله تلة، المرجع السابق، ص 175.

الأنظمة على تسجيل معلومات عن بصمات الأصابع والوجوه والأصوات، وقزحية وشبكية العين، التوقيع اليدوي، وغيرها.[1]

يمكننا النظر إلى هذه التقنية على أنها تعتمد على شيء لا يمكن نسيانه أو فقده أو تركه في مكان فير امن، مثل البطاقات الممغنطة أو كلمات السر.

لكن تبقى كلمة السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعا للتحقيق من الهوية، وهنالك وسائل كثيرة يمكن استخدامها، تعتمد هذه الوسائل أساسا على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم.[2]

ب- خدمات الأدلة

برمجيات خدمات الأدلة هي عبارة عن قواعد بيانات خاصة، ذات مستوى عال من الأمان عادة، ومصممة لجمع وإدارة المعلومات المتعلقة بمستخدمي الشبكة، ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين، ويتم استخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بمكوناتها جميعا كالتطبيقات و الأجهزة الخادمة والمجلدات وحتى شكل الشاشة التي يستعملها المستخدم، وتدار كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة والمستخدمين.[3]

---

[1]- حسن بن احمد الشهري، الإرهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، العدد الثامن، 2015، ص 17.

[2]- درياد مليكة، حماية البيانات في العصر الحديث، ط 1، دار هومة للنشر و التوزيع، الجزائر، 2017، ص 134.

[3]- عبد الله عبد الكريم، جرائم المعلوماتية و الإنترنت، د ط، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 87.

جـ- استخدام التشفير لحماية المعلومات الهامة

يعتبر التشفير عملية تحويل المعلومات إلى شيفرات غير مفهومة تبدو دون معنى، لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة.

يعتبر التشفير سلاح ذو حدين، حيث أنه يوفر الحماية للبيانات، لكن إذا فقد المفتاح السري أو البرنامج الذي شفر المحتوى، فلا فائدة ترتجى من المحتوى المشفر.[1]

د- الجدار الناري

هو فلتر يسمح بالتعاملات والتبادلات المرغوب فيها فقط، حيث تعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالاعتماد على مجموعة من السياسات، حيث تقوم بتصفية حركة حزم البيانات بالسماح بمرور الحزم الواردة من جميع المصادر الأخرى المعروفة والموثوق بها، ومنع الحزم الواردة من جميع المصادر الأخرى وكذلك السماح بتشغيل الخدمات اللازمة لأعمال المؤسسية ومنع تشغيل الخدمات الأخرى.[2]

ويوجد ضمن الجدران النارية صنفان، الأول: هو الجدران النارية المؤسسية التي تقوم بحماية تطبيقات المؤسسات، والثاني: هو الجدران النارية الشخصية، والجدران النارية في تطور مستمر وذلك ردا على تطور القراصنة ومحاولات اختراقها أو تعطيلها.

[1]- محمد فتحي، تفتيش شبكة الإنترنت بضبط جرائم الاعتداء على الآداب العامة، ط 1، المركز القومي للإصدارات القانونية، الجزائر، د س ن، ص 37.

[2]- مسعود قيراط، المرجع السابق، ص 28.

هـ- الشبكات الافتراضية الخاصة

لا توجد طريقة أكثر أمنا من الشبكات الافتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى الشبكة، وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديد مدير الشبكة، وفي هذه الحالة يمكن للمستخدمين المعنيين النفاذ إلى الشبكة عبر الانترنت، وإسقاط الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين[1]

المطلب الثاني: إقرار نصوص قانونية خاصة لمكافحة الإرهاب الإلكتروني

مع التطور الملحوظ في الجرائم الإلكترونية والزيادات المعتبرة من سنة إلى أخرى سارع المشرع الجزائري إلى سن العديد من النصوص القانونية الخاصة لمواجهة هذه الظاهرة وهذا ما سوف نتطرق إليه في هذا المطلب.

الفرع الأول: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني

تندرج مكافحة الإرهاب الالكتروني في الجزائر ضمن مكافحة الجريمة السيبرانية بكافة أشكالها، مع أنه يوجد غموض وعدم دقة في النصوص القانونية الوطنية في تعريف هذا النمط من الجرائم المستحدثة. لقد تنبه المشرع الجزائري إلى ضرورة جعل المنظومة القانونية مواكبة للتطور الحاصل في تكنولوجيا المعلومات والاتصال. في هذا الصدد

[1]- أحمد مصطفى منصور، المرجع السابق، ص 186.

صدر القانون المتعلق بالمعالجة الآلية للمعطيات ثم القانون رقم المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

ومن التدابير المتخذة من قبل الحكومة الجزائرية ما يتعلق بالوقاية الالكترونية التي تشمل، كما حدد القانون 09-04، الوقاية من جرائم الإرهاب والمساس بأمن الدولة، الوقاية من التعدي على أنظمة معلومات يكون هدفه المساس بالدفاع الوطني، ما تقتضيه التحريات والتحقيقات القضائية والمساعدات القضائية الدولية. كما نص القانون على قواعد تفتيش منظومات المعلومات وحجز المعطيات في إطار التحريات[2].

وقد صدر القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ليشكل تكملة لجملة القوانين والنصوص المتعلقة بمكافحة الإجرام و الإجرام الالكتروني ويهدف إلى أخلقة الحياة العامة، مع توصية بإنشاء مرصد وطني للوقاية من التمييز وخطاب الكراهية، ينص القانون على تأثير وعقوبات متنوعة تمس كذلك من يستخدم تكنولوجيا الإعلام والاتصال (وهنا إشارة إلى شبكات التواصل الاجتماعي) ، لغرض الدعاية والكراهية ونشر العنف، مع التشديد في جريمة استخدام هذه التكنولوجيا لنشر العنف في المجتمع.[3]

واهتمت وزارة الدفاع الوطني بحفظ الأمن السيبيراني، عبر وضع سياسات وبرامج واستحداث آليات لمكافحة الجريمة السيبرانية وحماية البنية التحتية للمعلومات وتم تعبئة عدد من الأجهزة المتخصصة لحماية أمن الفضاء السيبيراني والوقاية من الجريمة مثل

[1]- عبد القادر جعيجع وزهرة تيغزة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة، مجلة دفاتر السياسة والقانون، المجلد 13 العدد الأول، الجزائر، 2021، ص 552.

[2]- عبد القادر جعيجع وزهرة تيغزة، المرجع نفسه، ص 552.

[3]- عبد القادر جعيجع وزهرة تيغزة، المرجع نفسه، ص 552.

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

وكتقييم لبعض الجهود الدولية في مجال مكافحة الإرهاب الالكتروني يمكن القول أن استمرار التطور التكنولوجي والاستخدام المتزايد لشبكة الانترنت من ببن أهم التحديات التي تقف في وجه سياسات واستراتيجيات الدول، إلى جانب عدم وجود تعريف جامع للإرهاب الالكتروني، والثغرات القانونية بالنسبة لهذا النوع من الجرائم، مثل غياب العنصر المادي أحيانا وصعوبة كشف الجريمة في حينها يضاف إلى ذلك غياب سياسة تشريعية موحدة في مجال الإرهاب الالكتروني كما هو الحال لدى الدول العربية.[2]

لقد عملت السلطات العليا في الدولة على سن جملة من النصوص القانونية وتعديل أخرى حتى تتكيف مع تطورات الممارسات الإرهابية متعددة الأبعاد، وفي هذا الإطار جاء قانون العقوبات الجزائري حسب منطوق المادة 87 مكرر12:يعاقب بالسجن المؤقت من خمس سنوات إلى عشر سنوات وبغرامة 100.000 دج إلى 500.000 دج، كل من يستخدم تكنولوجيا الإعلام والاتصال "كشبكات التواصل الاجتماعي" لتحديد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة 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.[3]

---

[1]– بارة سمير، الأمن السيبيراني في الجزائر، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جامعة باتنة، الجزائر، 2017، ص 225.

[2]– بلهول نسيم، المرجع السابق، 28.

[3]– الأمر رقم 156/66 المؤرخ في 1966/06/08، المتضمن قانون العقوبات الجزائري، المعدل والمتمم لاسيما بالأمر رقم 01/20 المؤرخ في 2020/07/30.

وانطلاقا من هذا فإن سن المشروع الجزائري لمثل هذه النصوص القانونية، يأتي كخطوة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي تتبلور إحدى صور هذه الرقابة في سجن أصحاب مقاهي الانترنت المتواطئين مع شبكات التجنيد في صفوف الجماعات الإرهابية المتطرفة، وهو الإجراء الذي يعكس تحرك السلطات القضائية في تحصين الشباب من خطر الإرهاب الذي أصبحت أرضيته الخصبة عبر مختلف منصات التواصل الاجتماعي.[1]

وعلى صعيد آخر قامت الجزائر بسن مرسوم تنفيذي رقم 15-113 في 12 ماي 2015 يتعلق بإجراءات "حجز أو تجميد الأموال في إطار الوقاية من تمويل الإرهاب ومكافحته، وهذا تماشيا مع تطبيق قرارات مجلس الأمن الدولي ذات الصلة بمثل هذه الظواهر، حيث نجد في المادة الثالثة من هذا القانون على أنها تنص على: "معاقبة مرتكب جريمة تمويل الإرهاب. وكل من يقدم أو يجمع أو يسير بإرادته، بطريقة مشروعة أو غير مشروعة، بأي وسيلة كانت، بصفة مباشرة أو غير مباشرة، أموالا بغرض استعمالها شخصيا".[2]

الفرع الثاني: التدابير الإضافية المتخذة لمكافحة الإرهاب الإلكتروني

بالإضافة إلى سن قوانين خاصة بمكافحة الإرهاب الإلكتروني اتخذ المشرع الجزائري العديد من التدابير والتي تعتبر كتحديات مصاحبة لعملية التشريع والتي تهدف إلى القضاء على هذه الظاهرة، ومن أهم هذه التدابير أو التحديات ما يلي:

[1]- صغير يوسف، المرجع السابق، ص 107.

[2]- بارة سمير، المرجع السابق، ص 36.

- **التحديات الأمنية:**

وتتبلور في ضرورة تجاوز مشكلة نقص الخبرات الفنية في مجالات تحديد أركان الجريمة الرقمية المرتكبة عبر الفضاءات المتطرفة وتقديمها كمسألة متكاملة أمام أجهزة القضاء، إلى جانب حتمية تخطي صعوبة الرصد و التحقيق حول الأدلة التقنية، ويضاف إلى ذلك طبيعة الحدود الفنية، يحكم أن الجرائم المرتكبة تتجاوز الحدود الوطنية، مما يصعب من عملية الضبط والملاحقة ضد كل العناصر المتورطة في قضاياي الإرهاب السيبيراني، ناهيك عن أحجام الجمهور المستخدم عن التعاون مع المؤسسات الأمنية في ظل انعدام الثقافة التبليغ فيما يخص المضامين الالكترونية المتطرفة، وهو المتغير الذي يزيد من صعوبة المأمورية لدى مختلف المصالح الأمنية المختصة في مكافحة الجريمة الالكترونية.[1]

- **التحديات الفكرية والثقافية:**

إن الالتباس المسجل في كثير المفاهيم والخلط بين ضرورات وتنازلات المصالح السياسية والضغوط، وموازنة مسألة الثقافة الدينية والواجبات الشرعية، كلها مؤشرات زادت من صعوبة تحديد المسؤول المباشر عن كل المحتويات التحريضية والمتطرفة التي تحملها الفضاءات الالكترونية عبر شبكة الويب. من جهة أخرى فإن "عدم وجود العلماء المعتبرين في بيئة الانترنت بشكل تفاعلي، يزيد من جذب الشباب نحو خطابات التطرف في سبيل الالتحاق بالجماعات الجهادية التكفيرية" [2].

وفي مقابل هذا الطرح، يذهب المجلس الشيوعي الفرنسي في أحد تقاريره الأمنية في أعقاب حادثة شارلي إيبدو إلى التأكيد على ضرورة مواجهة المضامين الالكترونية المتطرفة على الشبكة العنكبوتية عبر خلق دعاية مضادة لمجابهة جسامة الأسلحة

[1]– ميلود صولي، المرجع السابق، ص 193.

[2]– ميلود صولي، المرجع نفسه، ص 194.

الالكترونية للجماعات الإرهابية، وعلى صعيد آخر دعا الاتحاد الإفريقي إلى الامتناع من نشر وبث كل المعلومات ومختلف الأخبار التي تقوم الجماعات المتطرفة بنشرها على الشبكة العالمية"، وذلك كاستراتيجية أفريقية تهدف إلى الحد من أي تأثير متوقع لهذه المنظمات على مختلف الشرائح الاجتماعية وعلى أمن البلدان أيضا.[1]

- **التحديات القانونية والتشريعية:**

تتمثل هذه التحديات في عدم استيعاب التشريعات والأنظمة القانونية للجرائم التي تحملها الفضاءات الالكترونية المتطرفة، والمستحدثة عبر شبكات المعلومات و الوسائط الرقمية، بالإضافة إلى "تنازع القوانين وعدم وضوح الاختصاص القضائي في التعاطي مع مثل هذه الجرائم، إلى جانب ضعف الثقافة القضائية في هذه المسائل الالكترونية، مما يعقد النظر في بعض القضايا" وعليه فان الإطار القانوني للإرهاب الالكتروني، و أنشطة استخدام الانترنت لأغراض إرهابية، يبقى يشكل إحدى المسائل الواسعة متشبعة الفروع، وعلى هذا الأساس بات لزاما العمل على ضرورة تفعيل آليات التعاون الدولي في مجال التدريب الأمني على مكافحة الجرائم المعلوماتية. وبخاصة المرتبطة بالإرهاب عبر الفضاءات الالكترونية المتطرفة، نظرا لما تتضمنه من خطورة على الأمن الدولي، مما تتطلب التكاليف من أجل مكافحته بوضع استراتيجيات تعاون دولية ناجحة.[2]

[1]– أحمد مصطفى منصور، المرجع السابق، ص 191.

[2]– بلهول نسيم، المرجع السابق، ص 31.

خلاصة الفصل الثاني

تم التطرق في هذا الفصل غلى الآليات القانونية والأمنية لمكافحة الإرهاب الإلكتروني وذل من خلال التعرض للإجراءات المتخذة من طرف كل من المنظمات العالمية والقارية والإقليمية مثل الاتحاد الأوروبي وجامعة الدول العربية، كما تم توضيح السياسة الجزائر المنتهجة في مكافحة الإرهاب الإلكتروني من خلال معرفة الإجراءات الوقائية لمكافحته وسبل حماية الفضاء الإلكتروني من الهجمات الإرهابية، وأيضا النصوص القانونية التي سنها المشرع الجزائري ما أجل مكافحة هذه الظاهرة، وكذلك التدابير الإضافية الهادفة إلى وضع حد لهذه الظاهرة.

الخاتمـــــــــة

في نهاية هذه الدراسة ومن خلال ما تم تقديمه نخلص إلى أن الإرهاب الإلكتروني يعتبر ظاهرة حديثة نسبيا ومتطورة نظرا لم يتسم به العالم الافتراضي من تقدم ملحوظ، وبالتالي أولت لها التشريعات الحديثة اهتماما كبيرا من حيث الوقاية والعقاب على حد سواء، وذلك من أجل المحافظة على سلامة الشعوب من ناحية وعلى أمن واستقرار الدول من ناحية أخرى.

فقد لاحظنا أن التشريع لم يقم بتعريف الإرهاب الإلكتروني تاركا ذلك للفقه الذي لم يوفق في إيجاد تعريف موحد له، وعليه تم عرض العديد من التعريفات الفقهية للإحاطة بمفهومه من جميع الجوانب، كما تم إبراز خصائص وصور الإرهاب الإلكتروني التقليدية منها والحديثة

أما الآليات القانونية والأمنية لمكافحته فقد تم التطرق لها من خلال استقراء إجراءات المنظمات العلمية والقارية وكذا الاتفاقيات الإقليمية بين الدول، بالإضافة إلى جهود الدولة الجزائرية في مواجهة ومكافحة هذه الظاهرة، حيث تم استعراض الإستراتيجية الوطنية لمكافحته والمتمثلة في إقرار نصوص قانونية خاصة لمواجهة هذه الظاهرة والتدابير الإضافية المتخذة إلى جانب النصوص القانونية، مثل السماح بالمراقبة الإلكترونية في هذه الجرائم، حيث نجد أن المشرع الجزائري قد سمح بها رغم ما تمثله من انتهاك لخصوصية الفرد المكفولة دستوريا وقانونيا، إلا أن خطورة هذه الجريمة دفعت بالمشرع إلى السماح بهذا الإجراء مع ضرورة احترام الضوابط القانونية المصاحبة لهذا الإجراء.

وقد حاولت قدر المستطاع الإلمام بجميع جوانب هذا الموضوع حسب الخطة المتبعة، وعلى ضوء هذه الدراسة تم التوصل إلى النتائج والتوصيات التالية:

أولا- النتائج

1- حرص الدولة الجزائرية على الحفاظ على أمن وسلامة الشعب واستقرار المجتمع من خلال محاصرته لهذه الظاهرة من كافة الجوانب.

2- أن الإرهاب الإلكتروني يقوم باستغلال الإمكانيات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، في ارتكاب وتنفيذ جرائمه بشكل سهل يصعب تعقبه وإثباته.

3- المشرع الجزائري يتعامل بجدية وحزم مع التهديدات والتحديات المفروضة على الدولة من طرف الإرهاب الإلكتروني.

4- الدول والمنظمات العالمية اتفقت فيما بينها على مكافحة هذه الظاهرة وتوحيد الجهود للقضاء عليها

ثانيا- التوصيات

1- القانون وحده لا يكفي لمواجهة الإرهاب الإلكتروني، وتبقى الوقاية أفضل طريقة، حيث لا بد من التوعية المستمرة للرأي العام من خطورة الإرهاب الإلكتروني على الدول والشعوب.

2- ضرورة تفعيل التعاون التشريعي بين الدول العربية المتضررة من هذه الظاهرة وخاصة تلك المجاورة لبعضها حتى تمنع التسلل وتبادل المعلومات.

3- تشديد العقوبات على الأفراد المنتمين لهذه الفئة من الإرهابيين وكذلك على كل من له صلة بهذا المجال.

4- ضرورة التأكيد على تجنيد خبراء وأخصائيين في مجال الكمبيوتر والانترنت من أجل وضع وتنصيب برامج إلكترونية تمنع الإرهابيين من الوصول إلى أهدافهم.

قائمـــــة

المصادر والمراجع

❖ **المصادر والمراجع:**

أولا- المصادر

1- الأمر رقم 156/66 المؤرخ في 1966/06/08، المتضمن قانون العقوبات الجزائري، المعدل والمتمم لاسيما بالأمر رقم 01/20 المؤرخ في 2020/07/30.

2- قانون رقم 04/09 مؤرخ في 2009/08/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

3- المرسوم الرئاسي رقم 261/15،المؤرخ في 2015/10/09، المتضمن تأسيس الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها.

ثانيا- المراجع

1- أحمد فتحي سرور، استراتيجيات الدول في مكافحة جرائم الإرهاب، ط1، منشأة المعارف، الإسكندرية، مصر، 2014.

2- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، ط 7، دار النهضة العربية، القاهرة، مصر، 1993.

3- أحمد فتحي سرور، مواجهة الإرهاب الإلكتروني، ط 3، دار النهضة العربية، القاهرة، مصر، 2011.

4- أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، ط 2، دار الحامد للنشر والتوزيع، الأردن، 2018.

5- أحمد مصطفى منصور، مكافحة الدول للإرهاب الرقمي، ط 2، منشأة المعارف الإسكندرية، مصر، 2016.

6- الأخضر عمر الذهيمي، دور المنظمات الدولية في التصدي للإرهاب، ط 1، جامعة نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية، د س ن.

7- إسماعيل عبد الفتاح، الإرهاب ومحاربته في العالم المعاصر، ط2، دار الكتاب العربي، القاهرة، مصر، 2009.

8- إسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربته في العالم المعاصر، ط3، منشأة المعارف ' مصر، 2010.

9- بوحادة سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، د ط، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، د س ن.

10- جعفر حسن جاسم، جرائم تكنولوجيا المعلومات، د ط، دار البداية للنشر والتوزيع، الكويت، 2013.

11- جمال علي الدهشان، الإرهاب الإلكتروني في العصر الحديث، ط2، دار الفكر العربي، القاهرة، مصر، 2018.

12- حسين شفيق، الإرهاب الإلكتروني في العصر الحديث، ط1، منشورات الحلبي الحقوقية، لبنان، 2017.

13- درياد مليكة، حماية البيانات في العصر الحديث، ط1، دار هومة للنشر و التوزيع، الجزائر، 2017.

14- رامي متولي القاضي، مكافحة الجرائم المعلوماتية، ط3، دار النهضة العربية، القاهرة، مصر، 2016.

15- عبد الرحمان بن عبد الله، الإرهاب الإلكتروني وطرق مكافحته،ط3،أكاديمية نايف للعلوم الأمنية، المملكة العربية السعودية،2017.

16- سماح عبد الصبور، الإرهاب الرقمي، د ط، معهد اليرموك للنشر، العراق، 2019.

17- سويدان أحمد حسين، استراتيجيات الإرهاب الإلكتروني، د ط، دار النهضة العربية، القاهرة، 2006

18- شعباني سيد أحمد، استخدام الإرهاب للتكنولوجيات، ط1، دار نايف للعوم، المملكة العربية السعودية، 2009، ص 17.

19- شفيق نوران، أثر التهديدات الإلكترونية على العلاقات الدولية، ط1، المكتب العربي للمعارف، القاهرة، مصر، 2015.

20- صادق عادل، الأمن السيبيراني، د ط، المركز العربي لأبحاث الفضاء الإلكتروني، الأردن، 2017.

21- طارق عزت رخا، المنظمات الدولية المعاصرة، ط، دار النهضة العربية ' مصر، 2006.

22- طاهر داوود، جرائم نظم المعلومات، ط3،دار الكتاب العلمي، الرياض، المملكة العربية السعودية، 2008.

23- عادل عبد الصادق، الإرهاب الإلكتروني وتأثيره على الدول، ط1، دار الأهرام للنشر والتوزيع، القاهرة: مصر، 2014.

24- عادل عبد الصادق، مكافحة الإرهاب الإلكتروني، ط1، دار الكتاب الحديث، القاهرة، مصر، 2017.

25- عبد الصبور عبد القوي، الجريمة المعلوماتية، ط1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 2013.

26- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، ط1، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2015.

27- عبد الله عبد الكريم، جرائم المعلوماتية و الإنترنت، د ط، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

28- عطية محمد، الإرهاب الإلكتروني وطرق مواجهته، ط 2، دار الحسن للنشر والتوزيع، عمان،الأردن،2017.

29- عفيفي كامل عفيفي، جرائم الكمبيوتر، ط 2، دار الثقافة للطباعة والنشر والتوزيع، القاهرة، مصر، 2012،.

30- علي جابر، جرائم الانترنت، د ط، مكتبة زين الحقوقية، لبنان، 2018.

31- علي عدنان الفيل، الإجرام الإلكتروني، ط 1، مكتبة زين الأدبية والحقوقية، لبنان، 2011.

32- علي يوسف شكري، المنظمات الدولية، د ط، دار الصفاء للنشر والتوزيع . الأردن، 2016،.

33- غادة نصار، الإرهاب والجريمة الإلكترونية، ط 2، دار العربي للنشر والتوزيع، القاهرة، مصر،2019.

34- فتحي شمس الدين، الإرهاب الإلكتروني وخطره على المستقبل، د ط، منشأة المعارف، الإسكندرية، مصر،2017.

35- محمد إبراهيم زيد، الإرهاب والجرائم المعاصرة، د ط،دار الهدى للطباعة والنشر، القاهرة، مصر، 2009.

36- محمد القاسم وآخرون، تجارب الدول في مكافحة الجرائم المعلوماتية، ط2، المركز الأمني للدراسات الاستراتيجية ' الدوحة، قطر، 2019.

37- محمد أمين الشوابكة، جرائم الحاسوب والانترنت، ط 3، دار الثقافة للنشر والتوزيع، الأردن، 2012.

38- محمد أمين بشرى، التحقيق في الجرائم المستحدثة، ط 4، مركز الدراسات والبحوث، المملكة العربية السعودية، 2012.

39- محمد حافظ الزهوان، مواجهة الإرهاب الحديث، ط3، دار هلا للنشر والتوزيع، القاهرة، مصر،2012.

40- محمد فتحي، تفتيش شبكة الإنترنت بضبط جرائم الاعتداء على الآداب العامة، ط1، المركز القومي للإصدارات القانونية، الجزائر، د س ن.

41- محمد مسعود قيراط، استراتيجيات مكافحة الإرهاب، ط 1، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية،2010.

42- محمد معمري، الإرهاب في صوره الحديثة، ط 1، منشأة المعارف، الإسكندرية، مصر، 2017.

43- محمد حسن براوري، غسيل الأموال وعلاقته بالجرائم المعلوماتية، ط2، دار القنديل للنشر والتوزيع، الأردن، 2017.

44- مصطفى محمد موسى، جرائم الكمبيوتر، ط1، المركز العربي للدراسات القانونية، مصر،2009.

45- ناصر بن محمد، مكافحة جرائم الإرهاب المعلوماتي، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2010.

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

47- هشام محمد، جرائم الإرهاب المعلوماتية، ط 2، المركز العربي للإصدارات القانونية، مصر، 2016.

ثالثا- الأطروحات والرسائل

1- حكبم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 03، 2014.

2- وليد الكشباطي، جرائم اختراق الأنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة المنار، تونس، 2014.

3- سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2013.

4- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

5- نور الله تلة، الإرهاب بالوسائل الإلكترونية، مذكرة ماجستير، كلية الحقوق، جامعة دمشق، 2016.

6- نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر، 2012.

رابعا- المجلات والدوريات

1- إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، الجزائر، العدد 630، 2016.

2- بارة سمير، الأمن السيبيراني في الجزائر، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جامعة باتنة، الجزائر، 2017.

3- بلهول نسيم، فهم المذهب العسكري الجزائري لثنائية بيئة الضبط العملياتي والدين في مكافحة الإرهاب، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، العدد الأول، 2015.

4- حسن بن احمد الشهري، الإرهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، العدد الثامن، 2015.

5- سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مقال منشور في مجلة كربلاء العلمية، جامعة اليرموك، العراق، العدد 14، 2014.

6- سامر مؤيد عبد اللطيف ونوري الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مقال منشور في مجلة كربلاء العلمية، جامعة اليرموك، العراق، العدد 18، 2018.

7- سلوى أحمد ميدان، الإرهاب والجهود الدولية لمكافحته، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، العدد الخامس، 2016.

8- عبد القادر جعيجع وزهرة تيغزة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة، مجلة دفاتر السياسة والقانون، المجلد13 العدد الأول، الجزائر، 2021.

9- عقيلة هادي عيسى وإسراء جواد حاتم، الإرهاب المعلوماتي وطرق مكافحته، المجلة السياسية والدولية، الجامعة المستنصرية، العراق، العدد 16.

10- محمد بن عبد العزيز بن محمد العقيل، التحريض الإلكتروني على الإرهاب، مقال منشور في مجلة الفقه والقضاء السعودي، كلية الأمير نايف للعلوم الأمنية، جامعة الرياض، المملكة العربية السعودية،2011.

11- محمد عبد المحسن سعدون، مفهوم الإرهاب وتجريمه في التشريعات الوطنية والدولية، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، العدد السادس، 2016.

12- ميلود صولي، السياسة الجزائرية في مواجهة المضامين الإلكترونية الإرهابية عبر شبكات التواصل الاجتماعي، مجلة الاتصال والصحافة، الجزائر، العدد التاسع، 2018.

13- عبد المجيد الحلاوي، التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، مداخلة مقدمة في الدورة تدريبية حول مكافحة الجرائم الإرهابية المعلوماتية أيام 09-14 أفريل 2006، جامعة محمد الخامس، الرباط، المغرب.

فهـرس المحتويات

الملخـــــــص

الملخـص

شـهدت الجزائـر فـي الفتـرة الأخيـرة انتشـارا واسـعا للعمليـات الإرهابيـة فـي المجـال الإلكترونـي ، مـا دفـع بالمشـرع إلـى المسـارعة فـي سـن قـوانين تهـدف إلـى مكافحـة الإرهـاب الإلكترونـي والحـد منـه، مـع اتخـاذه للعديـد مـن التدابيـر الوقائيـة لمواجهتـه، لـذلك كـان لابـد مـن دراسـة هـذه الظـاهرة وتعريفهـا وإبـراز خصـائصـها وصـورها والتحـديات الأمنيـة والقانونيـة لمكافحتهـا والحـد مـن انتشـارها وشـيوعها نظـرا لآثارهـا الوخيمـة علـى الشـعوب والمجتمعـات والـدول، كمـا أتـه يجـب علـى الـدول التكاتـف لمحاربـة الإرهـاب الإلكترونـي خاصـة وأنـه يتميـز بأنه من الجرائم العابرة للحدود الوطنية ولا يمكن محاربته إلا بالإتحاد.

Abstract

Algeria has recently witnessed a wide speed of terroriste opérations in the electronic field, which prompted the legislator to hasten the exactement of laws aimed at combating and limiting electronic terrorism, while taking many preventive measures to confront it, so it was necessary to study and define this phenomenon and highlight its characteristics, images and security challenges. And legal and legal to combat it and limit its spread and prevalence due to its dire effects on peoples, societies and states, and states must unite to combat electronic terrorisme, especially since it is characterized as a transnational crime and can only be fought by the union.