مقدمة

مقدمة

إن ظاهر الإرهاب من الظواهر حديثة النشأة كمصطلح قانوني ، قديمة الوجود كسلوك في المجتمع وبالتالي فهي أكثر الظواهر انتشارا داخل المجتمعات البشرية لأنها تهدد حياة الإنسان في أي مكان في العالم ، ولأي سبب،كما تتجلى خطورتها في مساس الأفعال الإرهابية بالأمن العام للشعوب والدول وإلحاق أضرار شديدة في الممتلكات نظرا لتعدد الوسائل المستخدمة في النشاط الإجرامي.

إن التطور السريع في مجال المعلوماتية وتكنولوجيا الاتصالات والاستخدام المتزايد للحاسب الآلي في كافة مجالات الحياة اليومية، أدى إلى ظهور أنواع جديدة من الجرائم المرتبطة باستخدام هذه الوسائل التكنولوجية لذلك تم تخصيص هذا النوع من الجرائم بوصف "الجريمة ألالكترونية [1]، التي تختلف عن الجرائم التقليدية في أطرافها ومكانتها وموضوعها وأساليب ارتكابها،ولعل جريمة الإرهاب الالكتروني تعتبر من أخطرها، نظرا لما تخلفه من خسائر جسيمة،فقد أصبح الإرهاب الالكتروني هاجسا يخيف العالم برمته نظرا لاتساع نطاق شبكة الانترنت ،ولجوء الجماعات الإرهابية لاستخدام شبكات التواصل عبرها للترويج لأفكارهم وتجنيد الشباب والشابات من مختلف جنسيات العالم لدوافع أهمها تقليل العبء المادي.

وتكمن خطورة الإرهاب الالكتروني في قدرته على إلحاق الضرر بالبني المعلوماتية الأساسية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات أو الأموال والمنشئات العامة والخاصة، و تجنيد عناصر جديدة داخل المنظمات الإرهابية للحفاظ على بقائها واستمرارها، فبات من السهل على هؤلاء الإرهابيين اعتماد شبكة الانترنت في تجنيد الشباب واستقطابهم للمنظمات الإرهابية في ظل بيئة رقمية تخلق العديد من التحديات التي تعيق الدول في مكافحة هذه الظاهرة.

و أمام هذا الوضع المعقد والخطير تعالت الأصوات المنددة بهذه الجريمة غير الوطنية والعابرة للحدود، والتي تهديد استقرار المجتمعات بالنظر إلى سرعة انتشارها وحداثة آلياتها مطالبة بضرورة التصدي لها، وإيجاد آليات والميكانيزمات فعالة من شانها الحد من خطورتها[2].

[1] . الجريمة الالكترونية :هي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعلها

[2] . مرين يوسف، إرهاب الانترنت عندما تتحول التقنية إلى وسيلة للإجرام، مقال نشر في، مجلة الدراسات القانونية والسياسية، المجلد الرابع، العدد2،جوان2018، ص206.

أسباب اختيار الموضوع:

تعود أسباب اختيار هذا الموضوع إلى أسباب ذاتية وأخرى موضوعية، فمن الأسباب الذاتية 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 أسباب الموضوعية فتتلخص في أن الإرهاب الالكتروني أصبح قضية خطيرة وواقعا مفروضا على الدول المختلفة ،فالإرهاب ليس موجودا بالجزائر فقط بل تقع الأحداث الإرهابية بمختلف دول العالم مما يجعلها أزمة دولية تستدعي التكاتف من اجل الوصول لحلول جذرية لخطر الإرهاب.

أهمية الدراسة:

في ظل ازدياد خطورة هذا النوع الجديد من الإرهاب بات من الضروري تظافر الجهود الدولية و الوطنية لمكافحته، من خلال تقديم المزيد من الجهود عن طريق إبرام العديد من الاتفاقيات الدولية العالمية الإقليمية التي تهدف إلى الحد من خطورة الإرهاب الالكتروني بكل صوره وأشكاله ، ومتابعة الجناة باستحداث قوانين جنائية ووطنية وفق معايير دولية موحدة.

الدراسات السابقة:

تطرقت بعض الدراسات السابقة إلى موضوع الإرهاب الالكتروني والتي يمكن إيجازها فيما يلي:

- ✓ إسراء طارق جواد كاظم الجابري ،جريمة الإرهاب الالكتروني دراسة مقارنة ،رسالة لنيل درجة الماجستير في القانون العام ، كلية الحقوق جامعة النهرين 2012 ،وقد توصلت الدراسة إلى انه لا يوجد حتى اليوم تعريف متفق عليه دوليا للإرهاب الالكتروني ،وان خطورة العمل الإرهابي هي السبب الرئيسي الذي يجعل العالم ألان مهتما بالتعاون لمكافحة هذا النوع من الإرهاب.
- ✓ مصطفى سعد حمد مخلف ، جريمة الإرهاب عبر الوسائل الالكترونية دراسة مقارنة بين التشريعين الأردني والعراقي،رسالة ماجستير في القانون العام ،قسم القانون العام ،كلية الحقوق ،جامعة الشرق الأوسط ،كانون الثاني 2017 ، تهدف هذه الدراسة إلى التعرف على الجرائم الالكترونية بشكل عام وجرائم الإرهاب الالكتروني بشكل خاص ،وموقف المشرع الأردني والمشرع العراقي منها،إضافة إلى بيان العقوبات المقررة على الجرائم الإرهاب بالوسائل الالكترونية في كل من القانون العراقي والأردني،وتوصلت الدراسة إلى أن الإرهاب باستخدام الوسائل الالكترونية هو العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الارهابين باستخدام الوسائل الالكترونية بهدف الإخلال بالأمن والنظام العام وابتزاز السلطات بالاستيلاء على الأموال العامة وإلحاق الضرر بالممتلكات.

✓ غلاف كريمة وجرلال زهرة، جريمة الإرهاب الالكتروني ، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، جامعة عبد الرحمان ميرة بجباية السنة الجامعية 2019/2018 وكان الهدف من هده الدراسة الوقوف على تحديد مفهوم جريمة الإرهاب الالكتروني وإبراز خصائصها وبيان أهم الدوافع المؤدية إلى ارتكابها ، وقد توصلت الدراسة إلى عدم وجود تعريف جامع مانع لجريمة الإرهاب الالكتروني ،وان المشرع الجزائري تبنى سياسة مزدوجة للتصدي لجريمة الإرهاب الالكتروني بحيث تم تعديل الجوانب الموضوعية من جهة والجوانب الإجرائية من جهة أخرى.

✓ شاشوة ياسمينة ، الإرهاب الالكتروني بين مخاطره واليات مكافحته ، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية ، جامعة أكلي محند اولحاج ، البويرة، السنة الجامعية 2020/2019 والتي كان الهدف منها إلقاء الضوء على ظاهرة وبيئة الإرهاب الالكتروني وعرض أهم مخاطر وأثاره بهدف توعية وتنبيه الأفراد والمجتمعات منه، وتوصلت الدراسة إلى أن جرائم الإرهاب الالكتروني ما هي إلا امتداد للجريمة الإرهابية المادية التقليدية ، وان المجتمع الدولي لم يتوصل إلى تعرف جامع مانع للإرهاب الالكتروني.

✓ علي بوعمرة،جريمة الإرهاب الالكتروني ، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية جامعة العربي التبسي، تبسه، السنة الجامعية 2021/2020 والتي كان هدفها تسليط الضوء على ظاهرة الإرهاب الالكتروني وإبراز الحماية الجنائية المكفولة للدول والشعوب حيال هذه الظاهرة وإجراءات التبعة لمكافحته، وقد توصلت الدراسة إلى حرص الدولة الجزائرية على الحفاظ على امن وسلامة الشعب والمجتمع من خلال محاصرتها لهذه الظاهرة من كافة الجوانب ، وان الإرهاب الالكتروني يقوم باستغلال الإمكانيات العلمية والتقنية واستخدام وسائل الاتصال والانترنت في ارتكاب وتنفيذ جرائمه بشكل سهل يصعب تعقبه وإثباته.

أهداف الدراسة:

تهدف الدراسة إلى بيان أركان وخصائص جرائم الإرهاب الإلكتروني واليات مكافحته على المستوى الدولي والإقليمي على اعتبار أنها جرائم حديثة النشأة، بحيث أصبحت تستخدم من قبل الدول والأشخاص والمنظمات الإرهابية بشكل كبير، خاصة في ظل غياب تشريع دولي رادع يجرم اللجوء إلى مثل هذه الجرائم التي ترتكب بوسائل الكترونية مختلفة.

مشكلة الدراسة:

ساهم التطور التقني في تغيير أساليب ارتكاب الجرائم وخصوصا تلك التي تتم عبر الانترنت والحاسوب ووسائل التواصل الاجتماعي والتي تتطلب إصدار قوانين جزائية تحدد أركان وعناصر الجرائم الإلكترونية ووضع قوانين تساهم في الحد من هذه الجرائم ، فالإشكالية المطروحة تم صياغتها وفق التساؤل التالي:

.إلى أي مدى ساهمت النصوص القانونية الدولية والوطنية في مكافحة جرائم الإرهاب الالكتروني؟

وتتفرع عن هذه الإشكالية تساؤلات فرعية نذكر منها:

ما هو مفهوم جريمة الإرهاب الالكتروني؟

وما هو الأطر القانونية الدولية والوطنية لها؟

وما هي استراتيجيات مكافحتها؟

منهجية الدراسة

تم اعتماد المنهج الوصفي والمناسب لمثل هذه الدراسة من خلال وصف جرائم الإرهاب الالكتروني وتحديد مفهومها وأركانها وخصائصها وتوضيح الأطر القانونية الدولية لمكافحتها، وكذلك المنهج التحليلي القائم على تحليل مضمون النصوص القانونية ذات الصلة بالموضوع والوقوف على فعاليتها في الحد من هذه الجرائم، كما أخدنا بالمنهج المقارن على سبيل الاستئناس في بعض المواضع نظرا لما تقتضيه الضرورة.

خطة الدراسة

اعتمدنا في خطة الدراسة على التقسيم ، إلى فصليين يندرج الفصل الأول تحت عنوان الإطار النظري لجريمة الإرهاب الالكتروني كمبحث أول ، وتبيان الإطار القانوني لهذه الجريمة كمبحث ثاني ، أما الفصل الثاني فكان تحت عنوان إستراتيجية مكافحة جرائم الإرهاب الإلكتروني والذي تضمن الأطر القانونية الدولية لمكافحة الإرهاب الإلكتروني كمبحث أول ، والحماية الإجرائية ضد الإرهاب الالكتروني كمبحث ثاني.

الفصل الأول

الإطار النظري لجريمة الإرهاب الإلكتروني

المبحث الأول:الأحكام العامة لجريمة الإرهاب الالكتروني

المبحث الثاني : الإطار القانوني لجريمة الإرهاب الالكتروني

تمهيد

إن النشاطات الإرهابية من أهم التهديدات التي تواجه أمن الأفراد والجماعات والمجتمعات وسلامتها بشتى صورها، فقد وفرت البيئة الرقمية للجماعات الإرهابية آليات ووسائل ساعدتها في بث نشاطها من خلال اعتماد الانترنت،فاكتسبت بذلك خصائص جديدة غيرت ملامح الإرهاب التقليدي وطرائقه،فأصبح أكثر ضراوة باعتماده على احدث تكنولوجيات الاتصال والمعلومات فينشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة، والإخلال بالنظام العام والأمن ألمعلوماتي وزعزعة الطمأنينة إضافة إلى تهديد السلطات العامة والمنظمات الدولية وابتزازها بتعريض سلامة المجتمع وأمنه للخطر .

كما تكمن خطورة الإرهاب الالكتروني في قدرته على إلحاق الضرر بالبني المعلوماتية الأساسية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات، أو الأموال والمنشئات العامة والخاصة، واخبرا تجنيد عناصر جديدة داخل المنظمات الإرهابية للحفاظ على بقائها واستمرارها، فبات من السهل على هؤلاء الإرهابيين اعتماد شبكة الانترنت في تجنيد الشباب واستقطابهم للمنظمات الإرهابية في ظل بيئة رقمية تخلق العديد من التحديات التي تعيق الدول في مكافحة هذه الظاهرة.

و أمام هذا الوضع المعقد والخطير لجريمة الإرهاب الالكتروني تعالت الأصوات المنددة بهذه الجريمة غير الوطنية والعابرة للحدود،والتي تهدد استقرار المجتمعات بالنظر إلى سرعة انتشارها وحداثة آلياتها مطالبة بضرورة التصدي لها، وإيجاد آليات والميكانيزمات فعالة من شانها الحد من خطورتها[1].

إن وضع إطار قانوني ملائم وفعال لمكافحة جرائم الإرهاب الالكتروني يتطلب أولا فهم هذه الظاهرة والإحاطة الجيدة بأهم أحكامها خاصة من الناحية النظرية والفقهية ثم دراسة القواعد المنظمة لها والتي تميزها عن باقي الجرائم الأخرى.

المبحث الأول : الأحكام العامة للإرهاب الالكتروني

يتسم تعريف الإرهاب بغموض كبير لتعدد صوره وأشكاله واختلاف مفهومه وفقا للعلم الذي يتولى تحديده، حتى أصبح ذلك مشكلة يصعب حلها، وتكمن الصعوبة في الآراء المتباينة بشأن شرعية وعدم شرعية التنظيمات الإرهابية، ونشاطها تبعا لاختلاف مصالح الدول ومبادئها، الأمر الذي أدى إلى إثارة مشكلة تعريف الإرهاب والمعيار المميز للعمل الإرهابي، والقواعد الموضوعية والإجرائية الواجبة التطبيق على المجرمين الإرهابيين.

[1] . مرين يوسف، إرهاب الانترنت عندما تتحول التقنية إلى وسيلة للإجرام، مقال نشر في، مجلة الدراسات القانونية والسياسية، المجلد الرابع، العدد2،جوان2018، ص206.

المطلب الأول : مفهوم الإرهاب الالكتروني

لم يتفق معظم الباحثين على تعريف دقيق ومحدد لمصطلح الإرهاب الإلكتروني بالنظر لطبيعة الأعمال الإرهابية واختلاف وجهات النظر حول هذه الأعمال، لذا سنحاول في الفرع التعرف عل مفهوم الإرهاب الالكتروني ومعرفة أبعاده كمصطلح قانوني وظاهره لها خطورتها في المجتمع.

الفرع الأول : تعريف الإرهاب الالكتروني:

سنحاول من خلال هذا الفرع التعرف على مختلف التعاريف اللغوية والفقهية والتشريعية المتعلقة بالإرهاب الالكتروني.

1. التعريف اللغوي للإرهاب الالكتروني

الإرهاب الإلكتروني كلمة من شقين الأولى إرهاب والثانية الكتروني،فالإرهاب مصدره رهب، ومعنى رهب وارهب في اللغة العربية أخاف وافزع[1]وأرهبه وأستر هبه أي أخافه،و(الراهب) معروف ومصدره (الرهبة) و(الرهبانية) بفتح الراء والترهب (التعبد)[2]، ونقول ركب (الرهب) و هو ما استعمل في السفر من الجمال،ويقال "ارهب عنه الناس باسه ونجدته " أن باسه ونجدته حملا الناس على الخوف منه و(الإرهاب)لا مفرد لها ما لا يصيد من الطير أما (الإرهاب) تعني الأخذ بالتعسف والتهديد وتعني أيضا نظام قائم على أعمال العنف، والإرهابي صفة تطلق على الشخص الذي يلجا إلى الإرهاب بالقتل أو إلقاء المتفجرات أو التخريب لإقامة سلطة أو تفويض،والحكم الإرهابي نوع من الحكم الاستبدادي يقوم على سياسة الشعب بالشدة والعنف بغية القضاء على النزاعات والحركات التحررية أو الاستقلالية.

والشريعة الإسلامية بدورها جرمت فعل الإرهاب بجميع سلوكياته وصوره المختلفة،واعتبرته من أشكال الفساد في الأرض ونهت عن الاعتداء على النفس البشرية دون وجه حق، والقول الراجح أن الإرهاب هو إثارة للرعب والخوف وليس القتل كما جاء في قوله تعالى "وَإِيَّايَ فَارْهَبُون"[3]وفي قوله أيضا "قَالَ أَلْقُوا فلَمَّا أَلْقُوا سَحَرُوا أَعْيُنْ النَّاسِ وَاسْتَرْهَبُوهُمْ وَجَاءُوا بِسِحْرٍ عَظِيمٍ"[4]،كما وردت كلمة الإرهاب في القران الكريم بدلالات مختلفة (ارهب،يرهب،إرهابا) وكلها تفيد معنى التخويف وإثارة الرعب في قلوب الناس،وجاءت أيضا بمعنى الاستعداد لمواجهة العدو والمشركين والحد من اعتداءاتهم في قوله عز وجل "وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللهِ وَعَدُوَّكُمْ "[5].

[1]. ينظر ابن محمد بن مكرم الإفريقي المصري، لسان العرب مجلد الأول، دار صادر، بيروت، دون سنة طبع، ص436.

[2]. انظر الشيخ محمد بن أبي بكر عبد القادر الرازي مختار الصحاح دار الرسالة، الكويت، سنة 1983 ، ص259.

[3]. أخر الآية 40 من سورة البقرة.

[4]. الآية 116 من سورة الأعراف.

[5]. الآية 60 من سورة الأنفال.

أما كلمة الكتروني فقد وردت في معجم المنجد باللغة العربية المعاصرة "خاص بالإلكترون "،"حشوه الكترونية،"حقل إلكتروني أما كلمة إلكترون فتعني عنصر دقيق للغاية، ذو شحنة كهربائية سلبية وهو أحد العناصر التي تؤلف الذرة[1].

ويتألف مصطلح الإرهاب الالكتروني (CYBER TERRORISME) في اللغة الأجنبية من كلمتين كلمة (CYBER) تعني الانترنت و(TERRORISME) تعني الإرهاب، وفي اللغة الأجنبية القديمة كاليونانية واللاتينية فإن لمصطلح الإرهاب "TERREUR" يعبر عن حركة من الجسد تفزع الآخرين ، ثم نقل هذا المعنى إلى اللغات الأجنبية الحديثة ، فكلمة الإرهاب في القاموس الفرنسي "لاروس" TERRORISMEالمشتق من الكلمة TERRORالذي يفيد الهلع ،الخوف ، الرهب ، القلق الغير مألوف، أما قاموس اللغة الانجليزية أكسفوردTERRORتفيد الخوف أو العنف أو الفزع الذي قد يمارسه شخص أو منظمة ضد حكومة أو فرد أو أطفال .

2. التعريف الاصطلاحي للإرهاب الالكتروني

ظهر مصطلح الإرهاب الالكتروني لأول مرة في فترة الثمانينات، وعرف هذا المصطلح رواجا واسعا من طرف الباحثين قبل أن تتم عملية عولمته وتجريمه بشكل رسمي لاحقا حيث عرفته موسوعة المعرفة بأنه "استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية "[2].

كما عرفه دوروثي دينينج "على انه "هجوم غير شرعي يستهدف أجهزة الحاسوب والشبكات والمعلومات المخزنة فيها، بحيث يؤدي القيام بذلك ترويع حكومة ما أو إجبار مواطنيها لتأييد أهداف سياسية أو اجتماعية[3].

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

---

[1]. أنطوان نعمة وآخرون، معجم المنجد في اللغة المعاصرة، طبعة 2، دار المشرق، بيروت،2001، ص37.

[2]. سعد عطوة الزنط، الإرهاب الالكتروني وإعادة صياغة استراتيجيات الأمن القومي، ورقة مقدمة إلى مؤتمر الجرائم المستحدثة وكيفية إثباتها ومواجهتها المركز القومي للبحوث الاجتماعية والجنائية، مصر،15 و16 ديسمبر2010 ، ص2.

[3]. بيتر غرابوسكي، جرائم الحاسب الآلي الأبعاد العالمية، مركز البحوث والدارسات الأمنية القيادة العامة ابوظبي، ط1،سنة 2006،ص238.

[4]. علي عدنان الفيل، الإجرام الالكتروني، مكتبة زين الحقوقية والأدبية، الطبعة1، لبنان، سنة2011، ص60.

كما عرفه محمد محمد الألفي على أنه "القدرة على اختراق شبكات الانترنت لتحقيق أهداف عدوانية ذات طابع سياسي في أغلب، وإن خلف وراءه أثارا سلبية تنال كثيرا من جوانب الحياة الأخرى"[1].

أما جعفر حسن حاسم الطائي فقد عرفه على أنه " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة عن الدول أو الجماعات أو الأفراد على الإنسان دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض"[2].

والملاحظ من خلال هذه التعريفات أن الإرهاب الالكتروني لا يختلف في معناه عن الإرهاب التقليدي، وإن اختلف عنه في الوسيلة وبعض الأهداف حيث ينظر كول مانCOLMANإلى أن إرهاب الانترنت على أنه ببساطة طلب الإرهاب على الانترنت، وعليه يمكن تعريف الإرهاب الالكتروني على أنه " التوظيف السلبي لشبكة الانترنت من خلال استخدام التقنيات الرقمية لإثارة الفزع والتخويف أو التهديد أو العدوان بغرض تحقيق أهداف معينة.

3: التعريف التشريعي للإرهاب الالكتروني

تعددت التعريفات لجريمة الإرهاب الالكتروني سواء كان ذلك في التشريعات المقارنة أو في الاتفاقيات الدولية ويرجع ذلك إلى حداثة الجريمة من حيث التشريع وسرعة الأساليب الحديثة المستعملة فيها.

أولا: تعريف الإرهاب الالكتروني حسب ما ورد في الاتفاقيات الدولية:

برزت الحاجة لذا المجتمع الدولي إلى ضرورة التصدي إلى ظاهرة الإرهاب الالكتروني مع مطلع القرن الحالي بعد تداول مصطلح الإرهاب الالكتروني على نطاق واسع ،الذي تعددت وسائله وأهدافه حيث أصبح يهدد السلم والأمن الدوليين على نطاق واسع نظرا لسهولة انتشاره مع تطور التقنيات التكنولوجية ، وفي هذا الصدد تعد اتفاقية بودابست الأولى من نوعها التي تتعلق بالجرائم الالكترونية والتي تم اعتمادها سنة2001 في العاصمة المجرية، ونصت على عدة جرائم في الفضاء السيبراني ومع ذلك لم تتطرق الاتفاقية لمفهوم الإرهاب الالكتروني بشكل خاص، أما "اتفاقية الأمن ألمعلوماتي شنغهاي" عرفته" بأنه استخدام مصادر المعلومات و التأثير عليها في فضاء المعلومات لأغراض إرهابية ،ويكمن مصدر هذا التهديد في المنظمات الإرهابية ،والأشخاص الضالعين في أنشطة إرهابية الذين يقومون بأعمال غير مشروعة، وتشمل سماته استخدام شبكات المعلومات من قبل المنظمات الإرهابية للقيام بأنشطة إرهابية واستقطاب مؤيدين جدد إلى صفوفها".

أما "الاتفاقية العربية لمكافحة الإرهاب" فقد عرفته على أنه" كل فعل من أفعال العنف أو التهديد بها أيا كانت دوافعه أو أغراضه،يقع تنفيذا لمشروع إجرامي فردي أو جماعي،ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم، أو

[1]. محمد محمد الألفي مكافحة جرائم الإرهاب عبر الانترنت، المؤتمر الدولي لمكافحة عملية الإرهاب، مؤسسة الأهرام المصرية، نشر يوم 2007/4/4، القاهرة، متوفر على الرابط http://www.maghress.com/hespress/655 تم الاطلاع عليه يوم 2023/1/2.

[2]. جعفر حسن جاسم الطائي، الإرهاب المعلوماتي واليات الحد منه، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة ديالي، العراق،2016، ص492.

تعريض حياتهم أو حرياتهم للخطر،أو إلحاق الضرر بالبيئة أو بأحد المرافق الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها،أو تعريض الموارد الوطنية للخطر[1].

والملاحظ في هذه التعريفات هو عدم وجود اتفاق جامع مانع لمصطلح الإرهاب يمكن الأخذ به واعتماده دوليا حيث نرى أن اتفاقية بودابست الأولى استعملت عبارات عامة ولم تحدد بدقة الفعل الإجرامي المشكل للإرهاب، أما تعريف اتفاقية شنغهاي فقد كان أكثر دقة،أما تعريف الاتفاقية العربية فقد كان بمثابة أول خطوة ساهمت في تحديد معنى الإرهاب بشكل واضح.

ثانيا: التعريف المقارن للإرهاب الالكتروني

إن تباين الفقه الجنائي في الوصول إلى تعريف موحد للإرهاب تزامن مع اختلاف تشريعي على مستوى الأنظمة الجنائية المختلفة، الأمر الذي انعكس واضحا على الجريمة الإرهابية وتحديدها لاختلاف صور الإرهاب من دولة لأخرى حيث عرفه التشريع البريطاني على أنه "استخدام العنف لتحقيق سياسية بما في ذلك أي استخدام للعنف بغرض إشاعة الخوف بين أفراد الشعب أو بين قطاع منهم"[2] ، أما قانون مكافحة الإرهاب المصري رقم94سنة2015 : المادة الثانية منه "يقصد بالعمل الإرهابي كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج،بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو مصالحة، أو أمنة للخطر أو أداء الأفراد أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر[3].

أما المشرع الجزائري لم يقدم تعريفا للإرهاب بالمفهوم التقليدي، وإنما اكتفى بذكر مجموعة الأفعال الإجرامية عن طريق تعديل قانون العقوبات بالقانون 16-02 وخصص قسما للجرائم الموصوفة بأفعال إرهابية أو تخريبه وعدد صورها في المادة 87 مكرر من قانون العقوبات، ويعتبر فعلا إرهابيا أو تخريبيا، في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي:

- ✓ . خلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص
- ✓ . بث الرعب في أوساط السكان أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المس بممتلكاتهم.
- ✓ . عرقلة حركة المرور وحرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية.
- ✓ . الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور.

[1]. انظر المادة الأولى الفقرة الثانية من الاتفاقية العربية لمكافحة الإرهاب المبرمة بين وزراء العدل والداخلية العرب القاهرة حررت بتاريخ 1998/4/22.

[2]. عبد الله نوار شعت التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي، الطبعة الأولى مكتبة الوفاء القانونية، الإسكندرية، سنة2017، ص50.

[3]. قانون رقم 94 لسنة 2015 المتضمن قانون مكافحة الإرهاب المصري، ج.ر، عدد 33 مكرر، المؤرخ في 10 أغسطس، سنة 2015.

- ✓ . الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون أي مسوغ قانوني.
- ✓ . الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.
- ✓ . عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات .
- ✓ . تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل، إتلاف منشآت الملاحة الجوية أو البحرية أو البرية،تخريب أو إتلاف وسائل الاتصال احتجاز الرهائن.
- ✓ . الاعتداءات باستعمال المتفجرات أو المواد البيولوجية أو الكيمائية أو النووية أو المشعة وتمويل إرهابي و منظمة إرهابية[1]

كما جاء في قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، حيث نصت المادة 2 على جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية، فالمشرع أعطى تعريفا عاما للجريمة الواقعة على النظام ألمعلوماتي ،نظام المعالجة الآلي للمعطيات، وهو تعبير فني تقني متطور يصعب إدراك تقنيته فهو خاضع للتطورات السريعة المتلاحقة في مجال الحاسبات الآلية والرقمية.

والملاحظ أن جل التعريفات التي أسلفنا الذكر تتفق على أن الإرهاب الالكتروني يكون باستخدام الوسائل الالكترونية ويجب أن تحتوي أفعال المجرمة فيه على عناصر الإرهاب فحتى يتحقق لابد من توفر العناصر التالية:

- ✓ . استخدام العنف أو التهديد باستخدامه، يراد بالعنف العدوان على الأشخاص باستخدام الوسائل الالكترونية.
- ✓ . أن يقع العنف أو التهديد تنفيذا لعمل فردي أو جماعي أو حتى دولي.
- ✓ . أن يكون من شان العنف المخطط له أو التهديد بيه إيقاع الرعب بين الناس وترويعهم
- ✓ . أن يكون الهدف من استعمال العنف والمخطط لهاو التهديد باستخدامه للإخلال بالنظام العام أو تعريض سلامة المجتمع للخطر.

[1]. الأمر رقم 156/66، المؤرخ في 1966/6/8، المتضمن، ق.ع.ج المعدل والمتمم بالأمر 02/16 المؤرخ في 19 يونيو 2016، ج.ر، عدد37 الصادر بتاريخ 22 يونيو 2016.

[2] . القانون رقم 04/09 المؤرخ في شعبان 1430 الموافق ل 05 غشت سنة 2009يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47 صادر في 2009/02/16.

الفرع الثاني : خصائص جريمة الإرهاب الالكتروني وتميزها عن غيرها من الجرائم المشابهة

إن الانتقال من العالم المادي إلى عالم الرقمي غير من خصوصية الجريمة الواقعة في نظامه، فأعطى للجريمة التي تستخدم فيها الوسائل الالكترونية سمات خاصة تتحكم فيها الرقميات من جهة، وسيمات مرتكبيها من جهة أخرى، وهذا ما سنحاول تبيانه في هذا الفرع.

1. خصائص الإرهاب الالكتروني:

يعتبر الإرهاب الالكتروني سليل الإرهاب التقليدي إلا انه يختلف عنه من حيث الخصائص، والتي سوف نتطرق إليها فيما يلي :

ا. صعوبة الإثبات:

إن اكتشاف واثبات الجرائم الإرهاب الالكتروني ليس بالأمر السهل ، فهي تقع في بيئة غير تقليدية تتمثل في الحاسوب وشبكة الانترنت ، كما أن وسائل المعاينة التقليدية لا تفلح غالبا في إثبات هذه الجرائم نظرا لطبيعتها الخاصة ، حيث تكون البيانات عبارة عن نبضات وذبذبات الكترونية تنساب عبر الأثير ، [1]وبالتالي النشاط الإجرامي فيها يكون غير محسوس وباستطاعة المجرم الالكتروني اختراق كمبيوتر المجني عليه فيدمر نظامه أو المعطيات المخزنة فيه أو يتلاعب بها أو يطلع على مضمونها من جهة، ومن جهة أخرى قد تؤثر مشكلات استخلاص الدليل الرقمي لإثبات الجريمة الالكترونية على مبدأ الاقتناع الشخصي للقاضي الجزائي ، وبالتالي عدم الأخذ به مما يسمح بإفلات المجرم من العقاب ، حيث يستطيع المجرم ألمعلوماتي التخلص من الآثار المادية لجريمته بفضل التقنية المعلوماتية ، التي تسمح له بامتلاك الوقت الكافي لتغيير أو تدمير الأدلة التي تثبت تورطه دون أن يتم التعرف عليه ، وفي وقت لا يكاد يذكر يحتسب [2].

ب . أداة ارتكاب الجريمة

لا يتصور ارتكاب هذه الجرائم من دون حاسب ألي خصوصا في نطاق جرائم الانترنت،وذلك لأن شبكة الانترنت إحدى التقنيات الحديثة التي أفرزها تطور الحاسوب،ولذلك فإن ارتباطها بالحاسب الآلي أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي وإن كنا اليوم نعاصر إمكانية استعمال الانترنت عبر الهاتف الخلوي.

[1] . محمد حماد مرهج الهيتي، الجريمة المعلوماتية، دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية مصر، الإمارات 2014، ص95.

[2]. محمد حماد مرهج الهيتي، الجريمة المعلوماتية المرجع السابق، ص96.

ج. جرائم غير عنيفة

تتسم الجرائم الناشئة عن استخدام الانترنت بأنها غير عنيفة لخفتها ولكونها مستترة في أغلبها ،كما أن الضحية لا يلاحظ ارتكابها، رغم أنها تقع أثناء وجوده على الشبكة ،فالإرهاب الالكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة وإنما كل ما يحتاج إليه هو جهاز حاسب ألي،وبعض البرامج وشبكات الانترنت ولذلك يطلق عليها (الجرائم الناعمة) لأنها لا تتطلب عنفا ، ذلك أن نقل بيانات من حاسب إلى أخر أو السطو الالكتروني على أرصدة بنك ما، لا يتطلب أي عنف أو تبادل إطلاق النار مع الأمن ، ويظهر ذلك جليا في مختلف المواقع الالكترونية ومنتديات قراصنة الهاكرز التي تضمن لهم الاتصال فيما بينهم بهدف تبادل الخبرات في مجال القرصنة من اجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن[1].

هـ. مدى التعاون بين مرتكبي الجريمة

بصفة عامة فان هذه الجرائم. التي تعد من جرائم التكنولوجيا الحديثة. تتميز بان مرتكبيها قد يحدث بينهم تعاون على ارتكابها إضرار بالجهة المجني عليها، وغالبا ما يكون فيها متخصص في الحاسبات يقوم بالجناب الفني من المشروع الإجرامي، وشخص أخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

ك. جريمة عابرة للقارات:

ذلك لقدرة تقني المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم ما جعل مسرح الجريمة مكشوفا عالميا، فهي تتجاوز الحدود الجغرافية باعتبار تنفيذها يتم عبر شبكة المعلوماتية وهو ما يثير في كثير من الأحيان إلى تحديات قانونية إدارية وفنية بل وسياسية بشأن مواجهتها خصوصا فيما يتعلق بإجراءات الملاحقة الجنائية القيام بإعداد البرامج في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم[2].

د. من حيث الجسامة والخطورة

الإرهاب الالكتروني يعد من الجرائم غير التقليدية حيث يتسم بالخطورة البالغة نظرا لأغراضه المتعددة وحجم الخسائر الناجمة عنه قياسا بالجرائم التقليدية، فالاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال في شتى المجالات مما ضاعف من الإضرار والخسائر التي تخلفها الاعتداءات على معطيات الحاسب.

[1]. أسامة مهمل، الإجرام السيبراني، مذكرة لنيل شهادة الماستر، فرع القانون الجنائي قسم الحقوق، كلية العلوم السياسية والقانونية جامعة محمد بوضياف، المسيلة، سنة 2018/2017، ص12.

[2]. أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الالكترونية، مذكرة لنيل درجة ماجستير في القانون العام، كلية الدراسات العليا جامعة النجاح الوطنية نابلس، فلسطين 2018، ص11.

2: الإرهاب الالكتروني والجرائم المشابهة

إن مصطلح الإرهاب الالكتروني يتشابه ومترابط نوعا ما بعض المصلحات التي تتمثل في الجريمة الالكترونية ،والجريمة المنظمة، وحرب المعلومات.

أولا: الإرهاب الالكتروني والجريمة الالكترونية

لا شك أن التطور الكبير الحاصل في مجال وسائل الاتصال والانترنت ساهم بطريقة أو بأخرى في تطور أنواع الجرائم وانتشارها بسرعة رهيبة،وأطلق عليها عدة تسميات منها جرائم المعلوماتية جرائم الكترونية ، جرائم التقنية ولقد خصص لها المشرع الجزائري القسم السابع من القانون15/04 المعدل والمتمم لقانون العقوبات في المواد 394 مكرر إلى 394 مكرر 8 بعنوان " المساس بأنظمة المعالجة الإلية للمعطيات".

كما أطلق المشرع الجزائري على الجريمة المعلوماتية مصطلح تكنولوجيا الإعلام والاتصال واستحدث القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [1]حيث عرفها في المادة الثانية منه" جرائم المساس بأنظمة المعالجة للمعطيات" المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات الالكترونية، فعند استقراء المادة أعلاه نلاحظ أن الجريمة الالكترونية وجريمة الإرهاب الالكتروني يشتركان في الخصائص التالية :

- ✓ . كلاهما من الجرائم المستحدثة والعابرة للحدود الوطنية والإقليمية
- ✓ . كلاهما يتشابه في الوسيلة المستعملة أي استعمال التكنولوجيا الحديثة
- ✓ . كلاهما من الجرائم المستحدثة في العا لم
- ✓ . كلاهما من الجرائم الناعمة والسلمية لأنهما لا تتطلبان العنف والقوة[2]
- ✓ . يسهل ارتكابهما بالنظر لطبيعة شبكة الانترنت مع قلة تكلفتها

لكن بالرغم من هذا التداخل الكبير بين الجريمتين إلا أن هناك فروق بينهما يمكن أن نوجزها فيما يلي:

. تهدف الجريمة المعلوماتية في الغالب إلى تحقيق الربح المادي أما جريمة الإرهاب الالكتروني ففي الغالب تكون أهدافها سياسية أو دينية وثقافية.... الخ، كذلك هناك اختلاف من حيث الخطورة فالمجرم ألمعلوماتي اقل خطورة من المجرم الإرهابي ألمعلوماتي فالأول قد يتواجد داخل المنظومة المعلوماتية سواء عن طريق الصدفة أو لمجرد التسلية واللهو أما الثاني يتواجد فيها للبحث عن

[1]. القانون رقم 04/09، المرجع السابق.

[2]. موسى دياب، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، ورقة مقدم في الدورة التدريبية: مكافحة الجرائم المعلوماتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية عمان، خلال الفترة، 2014/4/2 ص20.

مصادر التمويل أو لنشر الفكر الإرهابي الهدام أو لاستقطاب أعضاء جدد أو لسهولة التواصل فيما بين أعضاءها للتخطيط والتنسيق للعمليات الإرهابية.

ثانيا: جريمة الإرهاب الالكتروني والجريمة المنظمة

تقوم الجريمة المنظمة على هيكل تنظيمي صارم يحكمها نظام داخلي قاسي وأعضاءها يتسمون بالولاء للمنظمة وكذلك الاستمرارية في أنشطتها واعتبر الفقه أن كل جريمة إرهابية جريمة منظمة ولكن ليس كل جريمة منظمة حدثا إرهابيا...."'ولهذا يمكننا القول إن كلا الجريمتين تتشابه فيما يلي:

- ✓ . كلاهما من الجرائم المتطورة التي تعتمد وسائل الاتصال الحديثة.
- ✓ كلاهما من الجرائم العابرة للحدود.
- ✓ . كلاهما يسعى إلى بث الرعب والخوف في نفوس الناس.
- ✓ . كلاهما يتشابه في القواعد التي تحكم نظامهما الداخلي من حيث التعاون والتخطيط.
- ✓ . كلاهما في سعي دائم لاستقطاب أعضاء جدد والبحث عن ممول للأعمال الإجرامية.

أما عن نقاط الاختلاف الجوهرية بينهما فهي كالأتي:

- ✓ غاية وهدف الجريمة المنظمة استخدام العنف لكسب المصالح الشخصية وأرباح مادية أما الإرهاب أهدافه غير محددة فقد تكون سياسية أو دينية أو مادية.
- ✓ . الجريمة الإرهابية تشترط عنصر الاستمرارية والجماعة على عكس الإرهاب الذي يمكن أن يرتكب في إطار فردي.

. الجريمة المنظمة ترتكب بسرية أما الأعمال الإرهابية فيتم التشهير بها عن طريق الإعلام.

- ✓ . اعتراف الدول بالإرهاب ككيان من خلال التفاوض مع مجرمي على عكس الجريمة المنظمة.

ثالثا: الإرهاب الالكتروني وحرب المعلومات

يمكننا تعريف حرب المعلومات وهي استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل الخصم وعماليته مبنية على المعلومات والنظم المعلوماتية وشبكات الحاسب الآلي الخاصة به ، وكذلك الحماية من خطر الهجوم من قبل الخصم لإحراز التقدم على الأنظمة العسكرية والاقتصادية و تنقسم إلى نوعين :

. حرب معلومات هجومية : تقوم بها في الغالب الدول أو أجهزة استخباراتها لأهداف سياسية وعسكرية او غيرها حيث يستحوذ المهاجم على المعلوماتية ونظامها ويقوم بسرقة البرامج الكمبيوترية او يقوم بتخريب أو تعطيل نظم معلوماته.

. أما حرب المعلومات الدفاعية تعمل على حدود الوقاية من أعمال تخريبه التي قد تتعرض لها وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الأضرار التي قد تحدثها[1].

ومن ابرز أوجه التشابه بينها وبين الإرهاب الالكتروني:

- ✓ . هي عمليات تتم عبر شبكة الانترنت وبواسطة الحاسب الآلي.
- ✓ . صعوبة اكتشافها وفي الغالب ما يلفت المجرم من العقاب بسبب غياب الأدلة .
- ✓ . قلة التكلفة.
- ✓ . ذكاء وخبرة مرتكبيها

ورغم العلاقة الوثيقة التي تظهر بينهما إلا انه هناك اختلاف بينها ،حيث أن حرب المعلومات ما هي إلا أداة يمكن لفاعلون في الإرهاب الالكتروني استخدامها في تنفيذ أهدافهم، ويمكن أن تتحول بحد ذاتها إرهابا الكترونيا بناء على من يقف وراء استخدامها كجماعات الإرهابية ، وليس كل سوء استخدام للفضاء الالكتروني إرهابا.[2]

المطلب الثاني: أنواع الإرهاب الالكتروني

شهدت العديد من دول العالم هجمات الكترونية شكلت تهديدا لأمن واستقرار الدول، إذ قامت العديد من التنظيمات المتطرفة باستخدام الانترنت في بث خطابات الكراهية، إذ تشير المعطيات إلى أن الجماعات الإرهابية استغلت المزايا التكنولوجية كعنصر حيوي لدعم وتحقيق أهدافها وانتشرت نوعية خطيرة من الهجمات والجرائم الالكترونية تعتمد على تقنيات متقدمة تدمر البنية التحتية والحيوية للدول، ونتيجة لهذه التطورات الهائلة في عالم الحاسوب والاتصالات، ودخول العالم في العصر الرقمي أي عصر السرعة والانتشار السريع لشبكة الانترنت العالمية ومع استخدام الحاسب الآلي وتطبيقاته، خاصة في مجال التجارة الالكترونية بكل أنشطتها وخدماتها، حدث تغير في إدارة شؤون الدول، فبفضل هده التقنيات الحديثة أصبحت حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، وقد ظهر الارتباط بين الانترنت والإرهاب بشكل واضح بعد أحداث 11 سبتمبر 2001 حيث تحولت الحروب الواقعية إلى حروب رقمية، فلقد وجد نشطاء الانترنت في الشبكة وسيلة حديثة ذات كفاءة عالية في إطار التقنية الفنية التي يستخدمونها في ارتكاب جرائمهم التي يصعب اكتشافها، وتحديد مصدرها، وحولت الانترنت إلى ارض خصبة ومجال امن في تمويل الإرهاب، وتجنيد الجماعات الإرهابية[3]وأسفر هذا على وجود أشكال وأنواع عديدة للإرهاب الالكتروني سوف نتطرق إليها في هذا المطلب،الذي

[1] ـ مصطفى يوسف كافي، الإدارة الالكترونية، د.ط،دار ومؤسسة رسلان لطباعة والنشر ، سوريا، دمشق،2011،ص441.

[2] ـ نور الله تله، الإرهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي ، كلية الحقوق ،جامعة دمشق ،2015-2016 ،ص 26

[3]. فايز بن عبد الله الشهري، ثقافة التطرف والعنف على شبكة الانترنت: الملامح والاتجاهات، الندوة العلمية، استعمال الانترنت في تمويل الإرهاب وتجنيد الإرهابيين، جامعة نايف العربية للعلوم الأمنية مركز الدراسات والبحوث الطبعة الأولى، الرياض،2012 ص. ص 24-25.

قسمناه إلى فرعين ، حيث تناولنا في الفرع الأول جرائم الإرهاب الالكتروني التي تمارس بواسطة النظام ألمعلوماتي ، وفي الفرع الثاني تطرقنا إلى جرائم الإرهاب الالكتروني الواقعة على النظام ألمعلوماتي.

الفرع الأول: جرائم الإرهاب الالكتروني التي تمارس بواسطة النظام المعلومات

اتخذ الصراع الالكتروني أدوات وأشكالا عديدة ومتجددة في عصر الثورة المعلوماتية،ومثل الفضاء الالكتروني ساحة لنقل الصراعات من خلاله، أو استخدامه كوسيلة من وسائل الصراع، وبالتالي فالصراع الالكتروني هو الذي يمكن أن ينشا في بيئة الفضاء الالكتروني ويمتد الصراع عبر الفضاء الالكتروني إلى شتى المجالات، ويتجاوز الصراع الالكتروني الحدود التقليدية وسيادة الدول، وذلك يؤثر على امتداد الصراع ونطاقه ومن ثم تفاقم تداعياته وأثاره، ومن أبرز صور ذلك ما يلي:

1. إنشاء واستحداث مواقع على الانترنت (المواقع الالكترونية)

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة الانترنت للدعوة إلى أفكارهم المتطرفة والإعطاء التعليمات وللتدريب الالكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد تم إنشاء مواقع إرهابية الكترونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية الفتاكة وشرح طرق اختراق البريد الالكتروني وكيفية اختراق وتدمير المواقع الالكترونية،والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ..الخ[1]، فلم تعد النشاطات الإرهابية تقتصر على المجال المادي الواقعي فحسب، وإنما انتقل إلى الفضاء الالكتروني أيضا، ويظهر ذلك جليا في الانتشار الكبير للمواقع المعتمدة من قبل الإرهابيين ، فقد كان عدد مواقع الانترنت التي تروج للفكر المتطرف والإرهاب سنة1998 اثنتا عشرة موقعا12، ووصل العدد سنة 2018 إلى 580 ألف موقعا وهدا وفقا للاتحاد الأوروبي[2]، أما على المستوى العربي وحسب تقرير مجلس وزراء الداخلية العرب ،فان عدد المواقع يصل لأكثر من 720 موقع وصفحة ، تستهدف تضليل المواطن العربي، وهذا الرقم الخاص بمواقع وصفحات الانترنت الإرهابية يتغير بصفة شبه مستمرة ، نظرا لقيام معظم الدول العربية بحجب مواقع الانترنت الإرهابية لكن سرعان ما تعود تلك المواقع والصفحات الإرهابية مرة أخرى وهكذا.[3]

[1]. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الانترنت، المنعقد بالقاهرة في المدة من2 الى4 يونيو 2008.

[2]. مرين يوسف، إرهاب الانترنت عندما تتحول التقنية إلى وسيلة للإجرام، السابق، ص214.

[3]. منيرة غلوش، دراسة عن مواجهة استخدام الإرهابيين لشبكة الانترنت، دون تاريخ النشر ،متوفر على الرابط: http://gomhuriaonline.com/main.asp?-articl-id-204832 تم الاطلاع عليه بتاريخ 2023/2/3

2. التهديد الالكتروني:

أصبحت الجماعات الإرهابية تستغل شبكة الانترنت العالمية من اجل بث الرعب والخوف في نفوس الأفراد والدول بأساليب مختلفة ،مثل التهديد باغتيال شخصيات سياسية أو تهديد بتفجير مراكز سياسية أو هيئات حكومية أو التهديد بإطلاق الفيروسات التي من شانها تدمير أنظمة المعلومات بالكامل[1]كما أنه يستخدم وسائل الاتصال والانترنت من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم،وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار،ونشر الإشاعات الكاذبة بين الناس مما يؤدي إلى الخوف والهلع بين الجمهور[2]، ومن أمثلة التهديد الالكتروني ما قام به شاب أمريكي يدعى (جاهر بر جويل) البالغ 18 عاما حيث هدد كلا من مدير شركة (مايكروسوفت) والمدير التنفيذي لشركة (M .P.I) بنسف شركتيهما إذا لم يتم دفع خمسة ملاين دولار، وقد قامت الشركة بتفتيش منزل المذكور بعد القبض عليه وعثروا في حاسبه الآلي على ملفات رقمية عدة تحتوى على معلومات عن تصنيع القنابل تم إنزالها عبر الانترنت.

3. البريد الالكتروني:

يعتبر البريد الالكتروني من أهم الخدمات التي تقدمها شبكة الانترنت كصندوق للبريد بحيث يستطيع المستخدم إرسال الرسائل الالكترونية إلى شخص أو عدة أشخاص من مستخدمي الانترنت، فهو يسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات،ويتميز بالسرعة في إيصال الرسالة وسهولة الاطلاع عليها في أي مكان فهي لا ترتبط بمكان معين فلهذا يعتبر من أكثر الوسائل استعمالا من قبل الإرهابيين لتهديد الأشخاص حول العالم للانضمام إليهم أو الحصول على تمويل.

4. توظيف التنظيمات الإرهابية لشبكات التواصل الاجتماعي:

إن أشهر مواقع التواصل الاجتماعي فيسبوك وتوتير والتي تستغلها التنظيمات الإرهابية في نشر ثقافتها المتطرفة واستقطاب الشباب وكسب تعاطف الآخرين معها، كما تستخدمها في الترويج لأهدافها وللدعاية الخاصة بها من أجل الانضمام إلى صفوفها، فتنظيم القاعدة على سبيل المثال له العديد من المواقع الالكترونية والصحف الالكترونية والتي تصدر بلغات مختلفة.

الفرع الثاني: جرائم الإرهاب الالكتروني الواقعة على النظام ألمعلوماتي

استخدمت الجماعات والتنظيمات الإرهابية الانترنت للترويج والدعاية للفكر الإرهابي المتطرف، فشبكة الانترنت اليوم أصبحت الفضاء الواسع لهم، ومن بين هذه الأساليب أو الآليات نذكر ما يلي:

[1]. هشام محمد جرائم الإرهاب المعلوماتية ط 1 المركز العربي للإصدارات القانونية مصر2016 ص 127.

[2]. علي جابر، جرائم الانترنت، مكتبة زين الحقوقية، لبنان، 2018 ص316.

1. التجسس الالكتروني

هو سرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات والتجسس على هذه المعلومات أيا كان نوعها يأخذ أبعادا مختلفة فتعددت أهدافه من معلومات شخصية إلى معلومات اقتصادية وسياسية وعسكرية، وهو من أقدم واخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب ، وعرف تطورا كبيرا بعد الثورة التي حققتها تكنولوجيا الإعلام والاتصال واستخدام الحواسيب الإلية وشبكات الانترنت، وأصبح الهاجس الأكبر للدول من أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات[1] ولا تكمن خطورته في استخدام الانترنت ،بل في ضعف الوسائل الأمنية المختصة في حماية الشبكات الخاصة بالمؤسسات والهيئات، وتستهدف عمليات التجسس الإرهابي ثلاث أهداف رئيسية وهي:

- ✓ . التجسس العسكري
- ✓ . التجسس السياسي
- ✓ . والتجسس لاقتصادي

حيث تقوم التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة بحصول على أسرار ومعلومات الدول من ثم إفشائها لدول أخرى معادية أو استغلالها بما يضر المصلحة العامة للوحدة الوطنية، حيث يقوم الإرهابيون المبرمجون الذين يسمون (الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسيب الالكترونية باستخدام برامج للتجسس على الشبكات والأنظمة الالكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء بما في ذلك البريد الالكتروني واشتراكات المستخدمين وما إلى ذلك.

2. تدمير واختراق المواقع الالكترونية

تكون عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترقت فيها المواقع ، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الالكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي[2]، وكذلك الحال بالنسبة إلى تدمير المواقع فهو دخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام ألي أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو

[1]. بن بادة عبد الحليم،بوحاده محمد سعد، جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن الدول متوفر على الموقع:
https://www.elmizaine.com/2020/07/blog-post-3.html?=1 تم الاطلاع علية يوم 2023/2/5

[2]. سعيد عطوة الزنط،الإرهاب الالكتروني وإعادة صياغة استراتيجيات الأمن القومي،المرجع السابق

النظام ،وذلك باستخدام الفيروسات الالكترونية بقصد الحصول على معلومات متعلقة بالأماكن والمنشئات الحيوية لاستهدافها بالعمليات الإرهابية أو من اجل تدمير أو تعطيل في برامج الحاسوب، ومن الأساليب المستخدمة لتدمير المواقع أيضا ضخ كميات هائلة من الرسائل الالكترونية إلى الموقع المستهدف بالتدمير مما يؤثر على سعته التخزينية , ويؤدي في نهاية المطاف إلى تفجير الموقع وتشتت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه.

3. تدمير أنظمة المعلومات:

هو محاولة اختراق شبكة المعلومات الخاصة بالأفراد أو الشركات العالمية بهدف تخريب نقط الاتصال أو النظام عن طريق تخليق أنواع من الفيروسات الجديدة والتي تسبب كثيرا من الضرر لأجهزة الكمبيوتر والمعلومات التي تم تخزينها على هذه الأجهزة، ومن أهم أدوات ووسائل المستعملة في ذلك:

أ. الفيروسات:VIRUSES

الفيروس هو برنامج له القدرة على الدخول والاختباء في أي من البرامج الأخرى الموجودة على حساب أيا كان نوعها دون أن يكون صاحب الجهاز على علم بوجودها، أما عن طريقة تشغيل الفيروسات فهي أما أن تكون لها القدرة على تشغيل نفسها أو أن يكون تشغيلها بواسطة صاحب الجهاز دون أن يكون على علم انه يبدأ تشغيل الفيروس إذ أن الفيروس يمكن أن يكون قد تم ضبطه على أن يبدأ التشغيل إذا ما تم إجراء أمر معين على الجهاز فيكون صاحب الجهاز هو من شغله دون أن يكون على دراية بذلك، و سمي الفيروس بهذا الاسم لتشابه آلية عمله مع تلك الفيروسات التي تصيب الكائنات الحية بعدد من الخصائص[1].

ب **. الديدان:**DEFINITION

نوع آخر من أنواع الفيروسات ولكنها تمتاز بخصائص معينة تعطي لها ميزة إمكانية إلحاق الضرر بمستخدمي شبكة الانترنت،وتلك الديدان لها خاصية سرعة الانتشار والتوالد بمعنى أن لها القدرة على نسخ برنامجها بسرعة كبيرة والانتشار يعطي لها ميزة التغلغل، ويمكن تعريفها على أنها "برامج صغيرة قائمة بذاتها وغير معتمد على غيرها وصنعت للقيام بأعمال تدميرية أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم على شبكة الانترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم وتلك الديدان WORMS تتميز بسرعة الانتشار وفي نفس الوقت يصعب التخلص منها نظرا لقدرتها الفائقة على التلون والتناسخ والمراوغة"[2].

[1]. منير محمد الجنبيهي وممدوح محمدالجنبيهي، امن المعلومات الإلكترونية ،ط2، دار الفكر الجامعي، الإسكندرية ،2006ص 48.

[2]. منير محمد الجنبيهي وممدوح محمد الجنبيهي، امن المعلومات الالكترونية، المرجع نفسه، ص 61.

ج -القنابل المنطقية أو الزمنية

القنبلة المنطقية bombe logique عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل مشروع.

أما **القنبلة الزمنية** bombe à retardementفهي عكس القنبلة المنطقية فهي تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة. ويتم إدخالها في برنامج وتنفذ في جزء من الفمتوثانية أو الملي ثانية (1) أو ثواني أو دقائق وفقا للتاريخ المحدد سلفا. وبمعنى آخر يمكن لأي خبير في صناعة البرامج أن يقوم بزراعة الفيروس إذا كان يضمر شرا للنظام المستهدف.[1]

د -**برنامج حصان طروادة** TROJAN HORSES PROGRAM

ويعتبر برنامج حصان طروادة من البرامج الخطرة DANGEROUS PROGRAMSعلى الإطلاق التي تستخدم في عمليات اختراق أجهزة الحاسبات الإلية COMPUTERSنظرا لتمتعه بعدة مميزات تجعل منه الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه لذلك فقد اكتسب هذا البرنامج شهرة كبيرة في مجال اختراق أجهزة الحاسبات الإلية[2].

المبحث الثاني: التكييف القانوني لجريمة الإرهاب الالكتروني

تنازع الفقه الجنائي والدولي بخصوص التكيف القانوني للإرهاب الالكتروني، فالتكيف القانوني هو عملية ذهنية هدفها إعطاء الفعل الوصف القانوني الذي ينطبق عليه من بين كافة الأوصاف التي يتضمنها القانون، وفيما يخص جريمة الإرهاب الالكتروني نجد ثلاثة أوصاف قانونية : الأول عن وجهة نظر المشرع الوطني ويرى الإرهاب الالكتروني جريمة جنائية قائمة بذاتها ، والثاني يعبر عن وجهة نظر المجتمع الدولي، ويعد الإرهاب الالكتروني جريمة دولية والثالث يعبر عن قرار سياسي داخل المجتمع الدولي،ويعد الإرهاب الالكتروني نزاعا مسلحا يواجه بالحرب، ويخضع الوصف الأول للإرهاب الالكتروني للشرعية الدستورية التي تحكم القانون الوطني بخلاف الوصفين الثاني والثالث فيخضعان للشرعية الدولية المتمثلة في أحكام القانون الدولي.[3]

وفيما يأتي نعرض هذه الأوصاف القانونية للإرهاب الالكتروني في مطلبين نكرس الأول لعرض الإشكاليات القانونية الموضوعية لجرائم الإرهاب الالكتروني،أما الثاني نتطرق فيه لبيان أركان جريمة الإرهاب الالكتروني.

[1]. منير محمد الجنبيهي وممدوح محمد الجنبيهي،جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، د.ط، دار الفكر الجامعي، الإسكندرية،2006، ص55.

[2]. محمد علي عريان، الجرائم المعلوماتية، د.ط، دار الجامعة الجديدة للنشر الإسكندرية، 2004، ص99.

[3]. إسراء طارق جواد كاظم الجابري . جريمة الإرهاب الالكتروني . دراسة مقارنة . رسالة لنيل درجة الماجستير في القانون العام كلية الحقوق في جامعة النهرين العراق 2012، ص131.

المطلب الأول: الإشكاليات القانونية الموضوعية لجريمة الإرهاب الالكتروني

إن جريمة الإرهاب في الفضاء الالكتروني جريمة معقدة إذ نجدها جريمة لا ترى بالعين المجردة إلا أن مسالة وجودها أمر حقيقي وواقعي ومعترف به دوليا، فهي جريمة تتعدى ذلك المفهوم التقليدي للجرائم الذي نعرفه ، إضافة إلى أن توسعها وتوزعها وعدم استئثارها على دولة بعينها،خاصة وأن مسالة اختلاف الأنظمة المعلوماتية مسالة تختلف من دولة إلى دولة أخرى، الأمر الذي يثير جدلا فقهيا بشان التكييف القانوني لجريمة الإرهاب الالكتروني حول ما إذا كانت جريمة الإرهاب الالكتروني جريمة دولية أم أنها جريمة عالمية أو هي جريمة وطنية؟.

الفرع الأول: جريمة الإرهاب الالكتروني جريمة دولية

يرى بعض فقهاء القانون الجنائي أن جريمة الإرهاب الالكتروني جريمة دولية لأنها مخالفة للقواعد الدولية والتي تترتب على مخالفتها المسؤولية الجنائية الشخصية، سواء كانت من القواعد المنصوص عليها في الاتفاقيات الدولية أو في القواعد الدولية العرفية،إضافة إلى أنها تتعدى الدولة الواحدة مما قد يشكل اعتداء على حقوق الإنسان وحرياته الأساسية، وتهديد البني التحتية للدول مما قد يؤدي إلى تغيرات خطيرة في الأوضاع الدولية بشرط توافر مجموعة من الخصائص اذكر منها:

. تجاوز الحدود الوطنية للدولة، أي إن جريمة الإرهاب الالكتروني لا تقتصر على دولة واحدة بعينها، سواء فيما يتعلق بالمجرمين أو بالوسيلة المستخدمة فيها أو بالأهداف المرجوة منها[1].

. أن تتم الأعمال الإرهابية بدعم الدولة أو بتشجيعها أو موافقتها، التي يوجد فيها مرتكبو هذه الأعمال أو بدعم دولة أجنبية وهو ما جاء في المادة الثانية من اتفاقية المعاقبة على تمويل الإرهاب في ديسمبر1996 ومن قبيل ذلك استخدام بعض وسائل الإعلام لخدمة أهدافها.

- ✓ . أن تتجاوز الآثار الإرهابية حدا كبيرا من الجسامة وذلك نتيجة استخدام التكنولوجيا الحديثة الأمر الذي يجعل من هذه الإعمال الإرهابية أعمالا ضد الإنسانية برمتها وليس ضد مجموعة من الأفراد.
- ✓ . أن يشكل الإرهاب الالكتروني تهديدا للمجتمع الدولي بأسره وللدولة التي يقع عليها على حد سواء، وقد وصفه بعضهم بأنه ذلك العدو الأكثر ضراوة الذي يسعى إلى تحقيق أهدافه بغض النظر عن الآثار المدمرة التي قد تحدث جراء أفعاله.

ويتنازع الإرهاب الالكتروني بوصفه جريمة دولية ثلاثة أنواع من الأوصاف القانونية وفقا للقانون الدولي:

الأول: بصفته مجرد جريمة دولية: هذا الوصف لا يتوفر إلا إذا وقع في أثناء السلم متى توافرت فيه عناصر الجريمة الدولية كما بينها أنفا.

[1]. معمري خديجة وخليفاوي خليفة الإشكالات القانونية لجريمة الإرهاب الالكتروني . مجلة القانون، المجتمع والسلطة، المجلد 11 العدد1 السنة2022، ص133.

الثاني: بصفته جريمة ضد الإنسانية يتحقق هذا الوصف إذا ارتكبت الجريمة بحق السكان المدنيين بواسطة جماعات من الأفراد لا تعد من أجهزة الدولة.

الثالث: بصفته جريمة حرب إذا ما وقع في أثناء النزاع المسلح متى استخدمت وسائل إرهابية في القتال عن طريق نشر الرعب بين السكان المدنيين.

ولقد ثار الخلاف بوجه خاص في الأعمال التي تمارسها جماعات التحرير في أثناء الحرب وما إذا كانت تعد إرهابا أو جريمة حرب، ولعل هذا من الأسباب التي أدت إلى عدم الوصول إلى تعريف عام للإرهاب في مشروع عقد اتفاقية عامة للإرهاب بواسطة الأمم المتحدة، وحيث جاء في نص المادة 2 من الاتفاقية العربية لمكافحة الإرهاب 1998 على انه" لا تعد جريمة الكفاح بمختلف الوسائل بما في ذلك الكفاح المسلح ضد الاحتلال الأجنبي والعدوان من اجل التحرر وتقرير المصير وفقا لمبادئ القانون الدولي.

وبناءا على ما سبق يمكن القول ، بما أن أساس الجريمة الدولية هو تشكيل خرق لقواعد القانون الدولي الذي ترتكبه الدولة فقط عند انتهاكها لحالة السلم والأمن الدوليين لتقع ضد أشخاص المجتمع الدولي من الدول فقط ، بمعنى أن الجرائم الدولية لا يمكن أن يرتكبها إلا افردا بوصفهم أعضاء دولية في حين أن من سمات جريمة الإرهاب الالكتروني أنها جريمة يمكن أن يقوم بها فردا واحد أو جماعة معينة من اجل تحقيق أهداف شخصية محددة [1] ،وعليه فان مساءلة الأفراد عن الجرائم التي يرتكبونها بصفتهم الخاصة حتى ولو تشكل انتهاكا للقيم الأخلاقية والمصالح الدولية عن كونها جرائم دولية منافية للواقع ،إلا إذا افترضنا قيام دولة تلك الأفراد باعتبار تلك الأفعال من شانها زعزعة استقرارها وقتها فقط يمكن اعتبار جريمة الإرهاب الالكترونية جريمة دولية، و كما ورد في بيان مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين[2] ،والذي جاء فيه إن من أهم صور الجريمة العالمية جرائم العنف والإرهاب وجرائم متعلقة بالحاسوب (الإرهاب الالكتروني إحدى هذه الجرائم) ،والذي تم اختتامه بضرورة التعاون الثنائي والإقليمي والدولي في مجال منع الجريمة والعدالة الجنائية ،والتنسيق بين الدول في مكافحة الجريمة العالمية والذي يفهم من خلاله أن جريمة الإرهاب الالكتروني جريمة عالمية وليست جريمة دولية.

الفرع الثاني: جريمة الإرهاب الالكتروني جريمة عالمية

يعتقد جانب من فقهاء القانون الجنائي الدولي أن جريمة الإرهاب الالكتروني جريمة عالمية بالنظر لطبيعتها و الوسائل المستعملة فيها والنتائج المترتبة عنها ، خاصة وان ما يميز الجريمة العالمية أنها جرائم الأفراد لا جرائم الدول ، كما أنها لا

[1]. زين العابدين عواد كاظم الكردي، جريمة الإرهاب ألمعلوماتي،بيروت: منشورات الحلبي الحقوقية 2018، ص86.

[2]. محمد علي سويلم، جرائم الإرهاب الالكتروني (دراسة مقارنة)، د ط، القاهرة دار المصرية للنشر والتوزيع، سنة2018، ص377.

تشكل مساسا بالنظام الداخلي المشمول بالحماية الدولية وعليه فان جريمة الإرهاب الالكتروني وفق منظور هؤلاء الفقهاء جريمة عالمية ، مؤسسين حججهم على امتداد أثار جريمة الإرهاب الالكتروني لأكثر من دولة، وتعدد جناته واختلاف جنسياتهم أو اختلاف جنسيات المعتدى عليهم، وبالتالي فالإرهاب الالكتروني يعد جريمة من جرائم الإفراد لا جرائم الدول.

وعليه يمكنا أن نوجه انتقاد لهذا الاتجاه على النحو التالي: طالما أن مرتكبي الجريمة العالمية أفرادا لا دولا أي أنها جرائم أفراد لا جرائم دول،ولا تشكل مساسا بالنظام الدولي تحت طائلة الحماية الجنائية الدولية كما سبق الذكر، فما هو الوضع في مساءلة الإرهاب الالكتروني المرتكب من طرف دولة أو أكثر ضد مواطنيها أو ضد دولة أخرى؟

إن من بين أهم التصورات المحتملة للإرهاب الالكتروني المتعارف عليها ،والتي تتمثل في التهديد والترويع والتجسس الالكتروني واستهداف النظم العسكرية والبني التحتية الحساسة خاصة الحيوية منها [1]،مسالة تهديد الأمن والسلم الدوليين وهذا استنادا(المادة 39)من ميثاق الأمم المتحدة والذي لا يفهم من خلالها أن أي عمل يمس السلم والأمن الدوليين يندرجان وفق مفهوم الجريمة الدولية ،وان مفهوم الأمن وفق هذه المادة مسالة تتغير وتتطور وفق التطورات الدولية الحاصلة في مجال العلاقات الدولية ، والتي يمكن أن تندرج تحت طائلة هذا المفهوم جل الجرائم الالكترونية خاصة جريمة الإرهاب الالكتروني ،التي أصبحت في وقتنا الحاضر تشكل تهديدا خطيرا في العلاقات الدولية والواقع الدولي خير مثال عن ذلك.[2]

و بناء على ما تم عرضه فان جريمة الإرهاب الالكتروني في نظرنا الخاص جريمة عالمية، وذلك استنادا لطبيعتها ووسائلها المستعملة فيها، مما يفرض على الدولة حماية أفرادها المنتمين لها وإلزامها بمنع الأعمال الإرهابية ومكافحتها والتصدي لها وتقديم مرتكبيها إلى العدالة ' إلا أنها وفي هذا الإطار يجب إلا تغفل تلك الدول عن حقيقة أن التدابير الفعالة لمكافحة الإرهاب الالكتروني لا تكون ناجعة إذا لم يكن هناك تضافر جهود دولية مكملة لبعضها البعض.

الفرع الثالث: الإرهاب الالكتروني جريمة وطنية

يرى المشرع الوطني (المشرع الجزائري) أن الإرهاب الالكتروني جريمة جنائية نظرا لما يتوفر فيها من أبعاد مختلفة من الجرائم مثل القتل واستخدام المتفجرات والاغتصاب والسطو والسرقة والإتلاف ، ويتطلب التكيف القانوني لجريمة الإرهاب تعريفا قانونيا للجريمة يحدد أركانها ، يتبناه المشرع وفقا لمبدأ شرعية الجرائم والعقوبات مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب للأفعال التي يتضمنها هذا التعريف ،و إن مسالة دراسة موقف المشرع الجزائري تجاه جريمة

[1]. محمد علي سويلم، المرجع نفسه صفحة 378.

[2]. محمد علي سويلم،جرائم الإرهاب الالكتروني (دراسة مقارنة)، المرجع السابق،ص378.

الإرهاب الالكتروني كجريمة وطنية ، مسالة يصعب تحديدها وذلك لعدم فصله بعد في موقفه اتجاه جريمة الإرهاب الالكتروني رغم انه لم يعد بمنأى عن مخاطرها ، فلقد باتت الجزائر تعرف الكثير الهجمات من السيبرانية (الالكترونية) التي استهدفت مواقع حكومية تابعة لمؤسسات اقتصادية وحيوية إستراتيجية، وتكوين شبكات إجرامية منظمة تشن حملات تحريضية تهدف من خلالها إلى ضرب استقرارها وزرع الفتنة بين أفراد الشعب الواحد خصوصا عبر وسائل التواصل الاجتماعي ولقد ازدادت هذه الهجمات حدة وكثافة في المدة الأخيرة.

فإذا اعتبرنها جريمة إرهابية تقليدية لكنها ارتكبت بوسائل الكترونية حديثة وبالتالي تخضع في تكييفها لوصف الجرائم الموصوفة بأفعال إرهابية وتخريبية ضمن القسم الرابع من قانون العقوبات الجزائري بالوصف الذي أقرته المادة 87 مكرر، أو يمكن اعتبار أنها صورة من إحدى صور الجرائم الماسة بالأنظمة المعالجة الإلية للمعطيات المدرجة ضمن القسم السابع مكرر من قانون العقوبات خاصة المادة 394 مكرر3، أو أنها من إحدى الجرائم المستحدثة المدرجة في قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 5 أوت 2009 خاصة المادة 15 من الفصل السادس.

وبناءا ما سبق يمكننا القول إن عدم وجود نص صريح وواضح يجرم الإرهاب الالكتروني في المنظومة التشريعية الجزائرية لا يمنع استحسان موقف المشرع الجزائري باعترافه لهذا النوع من الجرائم المستحدثة[1].

المطلب الثاني: أركان جريمة الإرهاب الالكتروني

جريمة الإرهاب الالكتروني كغيرها من الجرائم الأخرى لها ثلاثة أركان تقوم عليها: الركن الشرعي والركن المادي والركن المعنوي، وسوف نرجئ الحديث عن الركن الشرعي إلى الفصل الثاني عند تناول الحماية الموضوعية ضد الإرهاب الالكتروني، لذا سنكتفي في هذا المطلب بدراسة الركن المادي والركن المعنوي لهذه الجريمة.

الفرع الأول: الركن المادي في جريمة الإرهاب الالكتروني

يمثل الركن المادي الوجه الخارجي الظاهر للجريمة، وبه يتحقق الاعتداء على المصلحة المحمية، وعن طريقه تقع الأعمال التنفيذية للجريمة وحتى تنهض الجريمة مكتملة وتامة لابد من توافر ثلاث عناصر هي السلوك الإجرامي، والنتيجة الضارة والعلاقة السببية، وهي نفس عناصر جريمة الإرهاب الالكتروني إلا أنها تختلف باختلاف سلوك مرتكبيها وشخصيته وكذا صور الاعتداء.

[1]. معمري خديجة وخليفاوي خليفة الإشكالات القانونية لجريمة الإرهاب الالكتروني، المرجع السابق، ص 153.

1. عناصر الركن المادي:

يعتبر الركن المادي جسم الجريمة حسب مبدأ "لا جريمة دون الركن المادي" وهو ذلك الفعل المحظور الذي يخرج إلى العالم الخارجي ويشكل اعتداء على الحق الذي يحميه القانون ويهدد النظام والأمن العام ويتكون من عناصر أساسية مترابطة فيما بينها ولابد من اجتماعها.

ا. السلوك الإجرامي

السلوك هو العنصر الرئيس للركن المادي في أي جريمة ، ويعرف بأنه النشاط المادي الخارجي المكون للجريمة وبالتالي لا جريمة من دونه لان القانون لا يعاقب على مجرد النوايا والرغبات[1]، ويجب التميز بين نوعين من السلوك ، السلوك السلبي و يتحقق في حالة إحجام الشخص عن إتيان فعل ايجابي معين يوجب القانون على القيام بيه رعاية للحقوق التي يحميها بشرط أن يكون في استطاعة الممتنع القيام بيه وبالنسبة لجرائم الإرهاب الالكتروني لا يمكن أن تقع بالامتناع ففي الغالب تتم بفعل الجاني والذي يستخدم الوسائل التي سبق ذكرها أما السلوك الايجابي فهو القيام بفعل يجرمه القانون ويؤدي إلى إحداث اثر مادي معين، مثل قيام شخص باستخدام يده بإدخال معلومات عبر الانترنت لتحريض أفراد مجتمع ما على القيام بأعمال إرهابية ضد النظام السياسي في ذلك المجتمع ، وعليه فإن صور السلوك الإجرامي في جريمة الإرهاب الالكتروني هو الفعل الذي يقوم به الجاني والذي من خلاله يهدد سلامة المجتمع وأمنه وسلامة الدولة بصورة عامة ، حيث يقوم الركن المادي لهذه الجريمة على الأفعال الآتية:

أ . الترويج للجرائم الإرهابية (الإشادة والتشجيع) حيث يتمثل فعل الإشادة في التنويه بالأفعال الإرهابية والثناء عليها أما فعل التشجيع يعني الحث وبعث الرغبة في القيام بالأعمال الإرهابية كإلقاء الخطب والكتابة والرسم .... الخ أو ما يسمى بالتمويل المعنوي.

ب. تمويل المنظمات الإرهابية ويقصد بالتمويل المادي كتوفير الأموال في صورتها النقدية أو العينية كمل يجب أن يكون النشاط الإجرامي وفقا لمقتضيات المادة87 مكرر وتتعدد الوسيلة المستعملة مثل التلفاز الفيديو الجرائد المجلات...الخ كما يحمل فعل الترويج معنى العلانية.

ج . وقد يكون السلوك إدخال بطريق الغش معطيات في نظام المعالجة الإلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها كما جاء في نص المادة 394 مكرر 1مثلا،أو قد يكون تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا

[1]. خلفي عبد الرحمان، محاضرات في القانون الجنائي، دار الهدى، عين مليلة، الجزائر، 2012، ص101

القسم[1]، أو قد يكون السلوك حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[2]

ونجد أن المشرع الجزائري جرم أيضا بعض الأفعال إذا ارتكبت لغرض إرهابي في نص المادة 87 مكرر11 والمادة 87 مكرر12 من قانون العقوبات الجزائري وأعطى لها وصف الإرهاب الالكتروني في حالة ما ارتكبت باستخدام تكنولوجيات الإعلام والاتصال.[3]

وبناءا عليه نستخلص أن السلوك الإجرامي في جريمة الإرهاب الالكتروني لا يمس فردا من الأفراد إنما يمس سلامة المجتمع،فهو يعتمد استخدام شبكة المعلومات العالمية (الانترنت) لتحريض الأفراد على مقارعة السلطة في دولة أو رفع شعارات الجهاد والمقاومة المسلحة ضد رموز السلطة أو للاقتتال الطائفي أو العرقي أو الديني أو من خلال استخدام الانترنت للاتجار غير المشروع بالمخدرات أو الأطفال).

ب . النتيجة الضارة:

يقصد بها التغيير الذي يحدث في العالم الخارجي أثرا للسلوك الإجرامي فيحقق عدوانا ينال مصلحة أو حقا قدر الشارع جدارته بالحماية، مما يعني أن النتيجة الضارة مدلولين أحدهما مادي، وهو التغير الناتج عن السلوك الإجرامي في العالم الخارجي، والأخر قانوني هو العدوان الذي ينال مصلحة أو حقا يحميه القانون.

فجريمة الإرهاب الالكتروني هي من الجرائم التي تهدد سلامة الأمن والمجتمع ،والنتيجة الضارة عنصر من عناصر الركن المادي للجريمة ليست ضرورية التحقق في جميع الجرائم لتمام تحقق الركن المادي فيها ،إذ أن الركن المادي يتحقق من دون الحاجة لوقوع النتيجة الضارة[4]،واختلف الفقه فيما إذا كانت نتيجة الفعل الإجرامي في العالم الافتراضي أم في العالم الخارجي الحقيقي ،وكلاهما محتمل الحدوث وكذا النقاش حول مكان وزمان تحقق النتيجة الإجرامية ، وتزداد خطورة النتيجة في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال ،حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها أو التحكم في خطوط الملاحة الجوية والبرية والبحرية ،أو شل محطات إمداد الطاقة والماء أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية[5].

---

[1]. المادة 394 مكرر 2 الفقرة1 من ق.ع.ج.

[2]. لمادة 394 مكرر2 الفقرة 2 من ق.ع.ج.

[3]. غلاف كريمة وجرلال زوهرة . جريمة الإرهاب الالكتروني، المرجع السابق، ص 35.

[4]. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الالكترونية، المرجع السابق، ص56.

[5]. علي عسيري، الإرهاب والانترنت، ط1 . مكتبة جامعة نايف العربية للعلوم الأمنية، الرياض .2006، ص91.

كما يفرق الفقه أيضا بين جرائم الخطر التي تشكل خطرا على امن المجتمع وسلامته، فهي اعتداء فعلي على مصلحة المجتمع الذي يستوجب عقابا، فالأولى المقصود بها الخطر الذي يواجهه الأفراد، والنوع الثاني من الجرائم هو جرائم الضررو التي هي سلوك إجرامي يترتب عليه إحداث فعل إجرامي يتمثل فيها العدوان الفعلي على حق يحميه القانون وتحقيق النتيجة فيها شرط لتوافر الركن المادي سواء كانت الجريمة عمديه أو غير عمديه فلا قيام لها ما لم تتحقق نتيجتها.

ج . العلاقة السببية بين السلوك والنتيجة:

هي الصلة بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى النتيجة ، فمثلا تشغيل الجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله على المعلومة ، فالعلاقة السببية في جرائم الإرهاب الالكتروني هي العلاقة التقنية بين مرتكب الجريمة وبين الآلة محل الجريمة، وهي الأساس لتحديد نطاق المسؤولية الجزائية في كل الجرائم الالكترونية العمدية ، ويقع عبئ الإثبات وجود الرابطة السببية من عدمها على النيابة العامة بما يقدم إليها من أدلة وبيانات واستماع الشهود في مثل هذا النوع من الجرائم المستحدثة [1]، والملاحظ أن جريمة الإرهاب الالكتروني لا يشترط فيها البحث عن العلاقة السببية، ، أي انه لا يشترط فيها البحث عن نسبة البحث الفعل إلى الفاعل لأنها من جرائم الخطر فلا يشترط لاكتمال الجريمة تحقيق النتيجة الإجرامية.

2 . المساهمة والاشتراك في جريمة الإرهاب الالكتروني

قد ترتكب الجريمة من قبل شخص واحد أو من قبل عدة أشخاص وفي هذا الافتراض لا تثور أية صعوبة، لأن الجاني ينطبق عليه نص القانون الذي عاقب على الجريمة المرتكبة ويتحمل وحده كل المسؤولية الناشئة عنه، أما إذا تعاون مع الجاني شخص أو أشخاص متعددون وقاموا في سبيل إتمامها بأدوار تتفاوت أهميتها فهنا يثور موضوع الاشتراك الجرمي، والذي يفترض ارتكاب عدة أشخاص لجريمة واحدة، وهده الأدوار تتفاوت من حيث مقدار مساهمة كل منها في تحقيق عناصر الجريمة[2].

عادة ما تتم جريمة الإرهاب الالكتروني من شخص لديه معرفة فنية في مجال الحاسوب ،والذي يكون له دور ايجابي في الشروع الإجرامي ، فمثلا يقوم الشخص المتخصص في تقنيات الحاسوب والانترنت بالجانب الفني من الجريمة

[1]. ضرغام جابرعطوش ال مواش . جريمة التجسس ألمعلوماتي دراسة مقارنة المركز العربي للنشر والتوزيع، مكتبة دار السلام القانونية السعودية، الطبعة الأولى،2017 ص 33.

[2]. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الالكترونية، دراسة مقارنة بين التشريع الأردني والعراقي، قدمت استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط، كانون الثاني ،2017، ص54.

،وبالتعاون مع شخص أخر من محيط المؤسسة المجني عليها أو من خارجها ،لتغطية عملية التلاعب وتحويل المكاسب إليه، فعلى صعيد عمل المصاريف يقوم موظف البنك بتزويد العصابات بالبيانات الخاصة ببطاقات الائتمان الصحيحة والمتداولة ،وذلك لغرض مساعدتهم في تقليد أو اصطناع هذه البطاقات وبالتالي تتحقق الجريمة باصطناع أو تقليد بطاقات ائتمان مزورة، فالاشتراك بالجريمة المعلوماتية قد يكون ايجابيا،وهو الغالب ويكون بتقديم مساعدة فنية أو مادية وقد يكون الاشتراك سلبيا بعدم الإبلاغ من جانب من علم بوقوع الجريمة محاولة منه تسهيل إتمامها.

ولقد نصت المادة (394مكرر5) ق.ع.ج كل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"، وما يمكن أن نستخلصه من نص المادة:

- ✓ . إذا ارتكب العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر، كما يجب أن تتجه هذه الإرادات إلى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات[1].
- ✓ . المشرع حدد الصفة الجريمة حينما حصرها في الإعداد بأفعال مادية للجرائم الماسة بالمعالجة الآلية للمعطيات بموجب نص المادة 394مكرر5، كما لا يعني هذا ضرورة الإعداد لكافة الجرائم المشمولة بهذا القسم، بل يكفي الإعداد والتحضير لواحدة فقط، وهو ما يستفاد من نص المادة سالفة الذكر التي تنص "...لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم..."يكفي أن يتم التحضير بفعل مادي مثل: تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور (most de passé) أو رمز الدخول (code daces)[2]
- ✓ . ولم يكتف المشرع الجزائري بتجريم الاتفاق بل تعداه لتجريم فعل الاشتراك في مجموعة أو في اتفاق بهدف الإعداد لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حسنا فعل بسب أن هذه الجرائم تتم عادة في إطار مجموعات ، وتحسبا لسهولة الاتفاق وسرعته بين المجرمين في هذا المجال حتى وان لم يكن بينهم معرفة مسبقة أو اتصال مباشر[3]،كما وسع المشرع من نطاق العقوبة حينما اخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي ، وذلك بهدف ردع مجرمي هذا النوع المستحدث من الجرائم ، وبمفهوم المخالفة تعتبر الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بهذا النص[4].

[1]. يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري،د. ط، دار الجامعة الجديدة: الإسكندرية، 2019،ص98.

[2]. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط1، 2006، ص131.

[3]. زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دون ذكر الطبعة، دار الهدى، عين مليلة، الجزائر،2011، ص105.

[4]. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع نفسه، ص132.

3. الشروع في جريمة الإرهاب الالكتروني:

الفعل الإجرامي لا ينفذ دفعة واحدة، وإنما يسبق التنفيذ عدة مراحله يمكن إيجازها فيما يلي:

- ✓ . المرحلة الأولى: التفكير في الجريمة والتخطيط والعزم على ارتكابها، لا يعاقب القانون على هذه المرحلة ما لم تظهر الأفكار في شكل أفعال مادية تحدث تغييرا في العالم الخارجي.
- ✓ . المرحلة الثانية: التحضير ويقصد بها عداد الوسائل التي تستعمل في ارتكاب الجريمة. الأصل أن القانون لا يعاقب على هذه المرحلة إلا في حالات كشراء سلاح بدون رخصة.
- ✓ . المرحلة الثالث: تتمثل في البدء في التنفيذ وهو ما يعبر عنه بالشروع في الجريمة والتي يعاقب عليها القانون[1].
- ✓ . المرحلة الرابعة: إذا استنفذ الجاني كل نشاطه الإجرامي وتحققت النتيجة نكون بصدد جريمة تامة.

و نص المشرع الجزائري على الشروع تحت مصطلح المحاولة، وعرفه في نص المادة 30 من قانون العقوبات " كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها نتيجة لظروف مستقلة عن إرادة مرتكبها حتى وان لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها، وتتفق جريمة الشروع التام مع جريمة الشروع الناقص في عدم تحقق النتيجة النهائية التي لا تتم الجريمة إلا بها ، ولكنها تختلف عنها في أن جريمة الشروع الناقص يبدأ الجاني بتنفيذ الجريمة ثم يوقف هذا التنفيذ قبل اكتماله رغما عن الجاني ، بينما الشروع التام يكون الجاني قد استنفذ كل نشاطه الإجرامي في سبيل تنفيذ الجريمة ولكن لم تتحقق الجريمة رغما عن إرادة الجاني[2]، ويعتبر قانون العقوبات الجزائري المحاولة في الجناية كالجناية نفسها ، ويعاقب عليها بنفس العقوبات حتى وان لم ينص عليها القانون ، في حين لا يعاقب على الشروع في الجنحة إلا بنص صريح في القانون ، وذلك متى لمس خطورتها، وما تمكن أن تؤدي إليه من أضرار في حال تمامها ، وهذا ما لمسه المشرع في الجريمة محل الدراسة [3]، حيث انه ونظرا لكون جميع جرائم الاعتداء على نظم المعالجة الآلية ذات وصف جنحة ، تدخل المشرع الجزائري ليقرر العقاب عليها بمثل الجريمة نفسها وهذا بموجب المادة 394مكرر7"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "هذا إذا اعتبرنا أن جريمة الإرهاب الالكتروني جنحة ، فما بالك إذا أخذت وصف الجناية.

---

[1]. عمر خوري، شرح قانون العقوبات القسم العام ، محاضرات، جامعة الجزائر1 كلية الحقوق السنة الجامعية 2011/2010.

[2] . مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الالكترونية،المرجع السابق، ص 90.

[3]. ليلة مرزوق، جرائم المساس بأنظمة المعالجة الآلية للمعطيات على ضوء الاتفاقيات الدولية والتشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة العربي بن مهيدي، كلية الحقوق والعلوم السياسية، السنة الجامعية 2017/2016.

الفرع الثاني: الركن المعنوي في جريمة الإرهاب الالكتروني

إلى جانب الركن المادي لا بد من توافر ركن ثاني لقيام الجريمة والذي يتمثل في الركن المعنوي، فلا يكفي لقيام المسؤولية الجنائية أن يصدر من الجاني السلوك الإجرامي وان تتحقق النتيجة مع قيام علاقة سببية بينهما، بل لا بد من توافر الركن المعنوي والذي يتخذ في التشريعات العقابية إحدى الصورتين: صورة القصد الجنائي أو صورة الخطاء غير ألعمدي. وبالنسبة لجريمة الإرهاب الالكتروني لا يتصورا لخطاء غير ألعمدي فيها.

1. عدم تصور الخطأ غير ألعمدي في جريمة الإرهاب الالكتروني:

لم يعرف المشرع الجزائري ما هو الخطأ غير ألعمدي وإنما عرفه القضاء بتعاريف مختلفة ومن بينها" الخطأ هو كل فعل أو ترك إرادي ترتب عليه نتائج لم يردها الفاعل مباشرة أو بطريقة غير مباشرة ولكنه كان بوسعه اتخاذ واجبات الحيطة والحذر لمنع النتيجة الضارة التي كان بوسعه توقعها وتجنبها".[1]

ومن هذا التعريف نستنتج أن الخطأ هو النتيجة التي تتحقق بسبب إهمال الجاني وعدم اتخاذ الاحتياطات اللازمة التي يدعو إليها الحذر، ولا يعتد بالفعل الذي يحدثه الجاني وعليه لا يمكن تصور الخطأ في جريمة الإرهاب الالكتروني التي لا يشترط تحقيق النتيجة فيها[2]، وبالتالي فان الركن المعنوي لجريمة الإرهاب الالكتروني يقوم على القصد الجنائي العام والقصد الجنائي الخاص.

2. القصد الجنائي العام

يعتبر القصد الجنائي اخطر صورتي الركن المعنوي لأن إرادة الجاني تنصرف إلى ارتكاب الفعل والى تحقيق النتيجة معا ،ولم يتعرض المشرع الجزائري إلى تعريف القصد الجنائي إلا انه اشترط في الكثير من النصوص توافر القصد الجنائي لقيام المسؤولية الجنائية عندما استعمل عبارة "عمد" وهذا ما أكدته المادة 394مكرر2 في قواها "كل من يقوم عمدا وعن طريق الغش بما يأتي:.....الخ ، وعرف الفقه القصد الجنائي بأنه " انصراف إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها كما يطلبها القانون "[3]، ونستخلص من التعريف بأنه لقيام القصد الجنائي لا بد من توفر عنصرين:

ا. عنصر الإرادة في جريمة الإرهاب الالكتروني:

الإرادة هي عبارة عن نشاط نفسي يتجه إلى تحقيق غرض عن طريق وسيلة معينة، فالإرادة ظاهرة نفسية وهي المحرك لأنواع السلوك ذات الطبيعة المادية، تحدث في العالم الخارجي من الآثار ما يشبع به الإنسان حاجاته المتعددة[4]، كما

[1]. منصوري رحماني، الوجيز في قانون الجنائي العام، د.ط، دار العلوم لنشر والتوزيع، عنابة 2006 ص125

[2]. غلاف كريمة وجرلال زوهرة . جريمة الإرهاب الالكتروني،المرجع السابق، ص47.

[3]. عمر خوري . شرح قانون العقوبات القسم العام، المرجع السابق.

[4]. المجاني نظام، شرح قانون العقوبات القسم العام، ص342.

تعرف الإرادة أيضا على أنها تلك القوة النفسية التي توجه الإنسان إلى تحقيق غاية يتوخاها، ولكي تكون الإرادة معتبرة قانونا يجب توفر شرطين هما: أن تكون هذه الإرادة مميزة وان تكون الإرادة حرة الاختيار.

ولكي يتوفر القصد الجنائي في جريمة الإرهاب الالكتروني يجب أن يكون الجاني عالما بحقيقة الواقعة الجريمة، سواء كان ذلك من حيث القانون أو الوقائع، ذلك انه بدون هذا العلم لا يمكن قيام الإرادة، فهي تقوم على أساس العلم بالقانون والواقعة الجرمية.

ب . عنصر العلم في جريمة الإرهاب الالكتروني:

لتوافر القصد الجنائي لا يكفي أن تتجه إرادة الجاني إلى ارتكاب الفعل وتحقيق النتيجة وإنما يجب على الجاني أن يكون على علم بتوافر الأركان والعناصر التي تقوم عليها الجريمة والتي يطلبها ويشترطها القانون، أي أن يدرك الجاني بأن عناصر هذا الفعل معاقب عليها من طرف القانون باعتبارها اعتداء على حق أو مصلحة محمية فإذا تخلف عنصر العلم ينتفي القصد الجنائي وبالتالي ينعدم الركن المعنوي فلا تقوم الجريمة[1].

ويعرف عنصر العلم على انه الحالة الذهنية وقدر من الوعي يسبق تحقيق الإرادة ويعمل على إدراك الأمور على نحو سليم، ومطابق للواقع حتى تتمثل سلفا من قبل الجاني، ويمكن القول بتوفرها فالعلم يرسم للإرادة اتجاهها وحدودها في تحقيق الواقعة الإجرامية، فعنصر العلم في جريمة الإرهاب الالكتروني يتطلب العلم بالقانون من ناحية والعلم بالواقعة من جهة أخرى وعليه فالركن المعنوي في جريمة الإرهاب الالكتروني يتمثل في اتجاه إرادة الجاني للارتكاب صورة من صور جرائم الإرهاب الالكتروني مع علمه بان المشرع قد جرمها.

3. القصد الجنائي الخاص:

هو الغاية أو المصلحة التي تدفع الجاني إلى ارتكاب الجريمة، وهذا القصد يطلبه القانون في بعض الجرائم إلى جانب القصد العام[2] ،ويتحقق في هذه الجريمة في اتجاه نية مجرم الإرهاب الإلكتروني إلى القيام بإحدى السلوكيات المشكلة للركن المادي للجريمة بغرض ارتكاب أفعال إرهابية،ومن أهم الأسباب التي تدفع الشباب من مختلف أنحاء العالم للانضمام إلى الجماعات الإرهابية منها ما هو دافع مادي كالفقر والبطالة ، أو دافع سياسي كالشعور بغياب العدالة الاجتماعية والإحساس بالظلم وسلب حقوقه من طرف السلطة الحاكمة ، أو قد يكون الدافع ديني أو ما يسمى التأثير الوجداني حيث تسعى المنظمة الإرهابية إلى تفسير النصوص الشرعية في غير حقيقتها[3].

[1]. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الالكترونية، المرجع السابق، ص79.

[2]. غلاف كريمة وجرلال زوهرة . جريمة الإرهاب الالكتروني، المرجع السابق، ص 48.

[3]. إسراء طارق جواد كاظم الجابري . جريمة الإرهاب الالكتروني . المرجع نفسه ص72.

خلاصة الفصل الأول

خلال هذا الفصل حاولنا التعرف على مفهوم الإرهاب الالكتروني،ولاحظنا أن التشريع لم يقم بوضع تعريف له، تاركا ذلك للفقه الذي لم يوفق في إيجاد تعريف موحد إلى حد الساعة، كما تطرقنا أيضا إلى مختلف صور وأشكال الإرهاب الالكتروني ووسائل التي يعتمد عليها لتحقيق أهدافه، كما قمنا بتبيان الإطار القانوني لهذه الجريمة، من خلال التعرض إلى مختلف أركانها عند تصنيفها كجريمة وطنية.

الفصل الثاني

إستراتيجيات مكافحة الإرهاب الالكتروني

المبحث الأول:الأطر القانونية الدولية لمكافحة الإرهاب الالكتروني

المبحث الثاني: الحماية الإجرائية ضد الإرهاب الالكتروني

تمهيد

إن الإرهاب الالكتروني هو إحدى صور الجرائم الالكترونية المرتكبة على النظام ألمعلوماتي ، فالنظام ألمعلوماتي هو محل الجريمة وتستهدف هذه الجرائم إما المكونات المادية أو المنطقية(برامج) للنظام ألمعلوماتي أو المعلومات المدرجة فيه ،مما يؤدي إلى تهديد الأمن الوطني والدولي على حد سواء ،وفي ظل ازدياد خطورة هذا النوع الجديد من الإرهاب بات من الضروري تظافر الجهود الدولية والإقليمية والعربية وحتى الوطنية لمكافحته ، وذلك عن طريق وضع إستراتيجية أمنية قضائية عالمية من شانها ملاحقة وتفكيك الإرهاب الالكتروني والحد من أثاره الوخيمة إلا أن هناك العديد من العقبات التي تقف في سبيل مكافحته ولعل أبرزها[1].

- ✓ . عدم وجود نموذج موحد لجرائم الإرهاب الالكتروني الذي يقتضي توحيد النظم القانونية.
- ✓ . عدم وجود معاهدات دولية فعاله لمواجهة المتطلبات الخاصة بالجرائم الالكترونية.
- ✓ . اختلاف مفاهيم الجريمة باختلاف الحضارات وعدم الوصول إلى مفهوم عام وموحد حول النشاط الذي يمكن الاتفاق على تجريمه.
- ✓ .عدم وجود اتفاق عام مشترك .

المبحث الأول : الأطر القانونية الدولية لمكافحة الإرهاب الالكتروني

إن غالبية التشريعات الجنائية المقارنة تعتد بمبدأ الشرعية الجنائية وتعتبره من أبرز المبادئ التي تحكم التجريم والعقاب والذي يقصد به ، حصر مصادر التجريم والعقاب في نصوص القانون، فتحديد النشاط أو السلوك الذي يعد جريمة جزائية ، وكذلك تحديد العقوبات المقررة لها، سواء من حيث نوعها أو مقدارها هو من اختصاص المشرع وحده وما على القضاء إلا تطبيق ما يضعه المشرع من نصوص في هذا الشأن[2] وبذلك يتبين أن مبدأ الشرعية الجزائية يرسم الحدود بين ما يعتبر في نظر المشرع الجنائي من سلوكيات تخل بأمن الجماعة ونظامها وسكينتها فتكون لديه جديرة بالتجريم والعقاب، ولهذا اكتسبت جريمة الإرهاب الالكتروني الطابع العالمي باعتبارها من الجرائم العابرة للحدود، مما أدى بأعضاء المجتمع الدولي إلى التصدي لها ، سواء من خلال الاتفاقيات الدولية والإقليمية، أو من خلال سن قوانين داخلية تتماشى مع هذه الاتفاقيات .

[1]. الطاهر بن يحي ناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية وفريضة شرعية، متحصل عليه من الرابط: ص 4.
http://www.alukah.net/Books/Files/book6138/BookFile/erhab.pdf

[2]. طه زكي صافي، القواعد الجزائية العامة فقها واجتهادا، د.ط، المؤسسة الحديثة للكتاب، طرابلس، لبنان 1997 ص119.

المطلب الأول: التشريعات **الدولية والإقليمية والوطنية لمكافحة الإرهاب الالكتروني**

أدركت الدول والمنظمات الدولية أهمية التعاون الدولي في صد الهجمات الالكترونية وجرائمها فعمدت إلى عقد الكثير من الاتفاقيات لتسهيل مهمة التحقيق في الهجمات السيبراني،حيث انقسمت الجهود الدولية في مكافحة الإرهاب الالكتروني إلى عدة أنماط :

- ✓ النمط الأول يتعلق بالعمل على إدخال تلك الجريمة ضمن الجرائم الالكترونية والعمل على إصدار تشريعات وطنية تكافح الظاهرة.
- ✓ أما النمط الثاني : فهو سعى عدد من الدول أو التكتلات الإقليمية إلى التعاون فيما بينها في مكافحة الإرهاب والجريمة عبر الانترنت .
- ✓ أما النمط الثالث فيتمثل في العمل على حث الأمم المتحدة على القيام بدور في المكافحة عن طريق فرض سيطرتها على إدارة الانترنت وإقرار ثقافة عالمية للأمن الالكتروني.

الفرع الأول: الجهود الدولية والإقليمية لمكافحة بالإرهاب الالكتروني

تعد المعاهدات والمؤتمرات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة جرائم الإرهاب الالكتروني، وقد تم عقد العديد من المعاهدات والمؤتمرات وفي هذا مجال وسوف نتطرق في هذا الفرع إلى أهمها:

1: دور الأمم المتحدة في مكافحة الإرهاب الالكتروني

تلعب العديد من المنظمات وعلى رأسهم منظمة الأمم المتحدة دورا هاما في تعزيز العمل المشترك بين الدول للحد من انتشار الجرائم، ولقد أكد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين بميلانو بإيطاليا سنة1985 على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا و في كل مكان لصالح الجمهور، وبالتالي منع الجريمة على نحو فعال، كما أكد أيضا على أن التكنولوجيا قد تولد أشكالا جديدة من الجريمة " فانه ينبغي اتخاذ تدابير ملائمة ضد حالات إعادة الاستعمال الممثلة لهذه التكنولوجيا كما..."، وأقر المؤتمر وجوب اعتماد ضمانات ملائمة لصون السرية كما أكد عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم[1].

كما أقر المؤتمر الثامن للأمم المتحدة بهافانا سنة1990عدة مبادئ أهمها : تحديث القوانين و الإجراءات الجنائية بما في ذلك اتخاذ تدابير من اجل ضمان أن الجزاءات والقوانين الراهنة بشان سلطات التحقيق وقبول الأدلة في الإجراءات القضائية

[1]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، طبعة 2017م/1438هـ، دار الخلد ونية، الجزائر ص115.

تنطبق على الجرائم المعلوماتية وإدخال تغييرات مناسبة عليها إذا دعت الضرورة إلى ذلك[1] ، كما أشار إلى ضرورة النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة بحيث تدعو بذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي، ومضاعفة الأنشطة التي تبذلها الدول الأعضاء على الصعيد الدولي من اجل مكافحة الجرائم المتصلة بالحاسبات ،كما نصح القرار ذاته الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية انطباقا كافيا على الأشكال الجديدة للإجرام، كما اقترح المؤتمر أيضا ضرورة تعزيز مسار التعاون الفعال عن طريق ، وضع أو تطوير ،معايير دولية لأمن المعالجة الآلية للبيانات ،وتدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود ، إضافة إلى اتفاقيات دولية تنطوي على نصوص تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود في الأنشطة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق الأفراد وحرياتهم وسيادة الدول[2].

ثم انعقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين للأمم المتحدة بالقاهرة في سنة 1995 وأكد في توصياته على وجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا،ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها،وفي عام 2000 عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين في بودابست " المجر" وأكدت على وجوب العمل الجاد للحد من جرائم الحاسب الآلي المتزايدة والمستحدثة واتخاذ تدابير للحد من أعمال القرصنة[3].

وعملت الأمم المتحدة على اتخاذ تدابير جماعية لدحض تهديدات السلام والأمن الدولي، حيث اعتمدت الدول الأعضاء في الأمم المتحدة بتاريخ 08 سبتمبر 2006استراتيجية موحده لمكافحة الإرهاب بجميع أشكاله وأنواعه، حيث أشارت الفقرة1 من المادة 12 إلى تنسيق الجهود على الصعيدين الدولي والإقليمي، تضمنت تعزيز قدرة الدول على مكافحة التهديدات الإرهابية وتحسين تنسيق أنشطة الأمم المتحدة في مجال مكافحة الإرهاب.

2: دور المنظمات الإقليمية الأوربية والعربية في مكافحة الإرهاب الالكتروني

تلعب المنظمات الإقليمية الأوروبية والعربية دورا فعالا في مكافحة جرائم الإرهاب الالكتروني،ويعتبر المجلس الأوربي المجلس الوحيد الذي تناول بشكل متعدد الأطراف قضية الاستخدام الإرهابي للإنترنت ، وتحت رعايته اعتمدت اتفاقية

[1]. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط 1، 2008، الأردن، ص52.

[2]. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط1، دار النهضة العربية 2001، مصر، ص 362.

[3]. علي جبار ألحسناوي، جرائم الحاسوب والانترانت، دار اليازوري العلمية للنشر والتوزيع ،2009 الأردن، ص148.

بودابست اتفاقية الجرائم الالكترونية 2001 ، وانضمت 54 دولة إلى الاتفاقية بما في ذلك المملكة المتحدة البريطانية، وقامت الاتفاقية بتدوين وتنظيم الجرائم في الفضاء الالكتروني ، بما في ذلك التزوير باستخدام تكنولوجيات الحاسوب ، الاحتيال باستخدام تكنولوجيا الكمبيوتر ..... ، إلا أن الاتفاقية لم تدون جريمة الإرهاب الالكتروني، وتم التوقيع على تلك الاتفاقية من قبل المسئولين في الدول الأوربية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا بعد مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية لشكل الاتفاقية ، ومن ثم التوقيع عليها من جميع الأطراف.

وكذلك منظمة التعاون الاقتصادي والتنمية(OECD)والتي تضم في عضويتها 29 دولة حتى أواخر 2000 وغرضها الرئيسي تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية، ومع ظهور هذا النوع الجديد من الجرائم التي تهدد الأمن ألمعلوماتي، أقرت المنظمة قواعد إرشادية وتوصيات للدول الأعضاء في تشريعاتها الوطنية حيث نصت على عقاب جنائي في حالة مخالفتها، وفي بداية 1983 اتجهت المنظمة إلى الاهتمام بالجريمة المعلوماتية ككل من خلال عقد الاجتماعات والمؤتمرات لبحث تلك الظاهرة الإجرامية[1]، ففي سبتمبر 1985 تم تشكيل لجنة لدراسة الجريمة المعلوماتية قامت بإجراء مسح لهذه الجريمة بالدول الأعضاء بالمنظمة، كما أسفر عمل اللجنة عن صدور تقرير في 1986 بعنوان جرائم الحاسب الآلي والذي أوصى الدول الأعضاء بضرورة مواجهة المشكلات الناجمة عن الجريمة المعلوماتية في قوانينها الداخلية[2]، واتجهت المنظمة بعد ذلك إلى الاهتمام بحماية أنظمة وشبكات المعلومات، وذلك بإصدار التوصيات الخاصة بالتدابير والإجراءات الأمنية المفروض على الدول الأعضاء الأخذ بها لحماية أنظمة المعلومات.

ولا ننسى اتفاقية تعاون الدول الأعضاء في الكومنولث الدول المستقلة في مجال امن المعلومات،التي اعتمدت في سنة 2013 والغرض من هذه الاتفاقية هو القيام بأعمال مشتركة ومنسقة تهدف إلى ضمان امن المعلومات في الدول الأطراف في هذا الاتفاق وان هذه الاتفاقية لم تحتوي على نص صريح عن جريمة الإرهاب الالكتروني سوى المادة الثانية التي عرفت الإرهاب ألمعلوماتي على انه "استخدام موارد المعلومات أو التأثير عليها في الفضاء المعلومات للأغراض الإرهابية".[3]

أماعن الجهود العربية المبذولة من أجل الحماية من جرائم المعلوماتية فهي ، اعتماد القانون الجزائي العربي الموحد كقانون نموذجي بموجب القرار رقم 299 لسنة 1996 كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية وفي عام 1997 تم اعتماد " الإستراتيجية العربية لمكافحة

[1]. شاشوة ياسمينة، الإرهاب الالكتروني بين مخاطره واليات مكافحته، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة اكلي محند، البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، سنة2019/2020، ص84.

2. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، المرجع السابق ص120.

[3]. ناصر العلي، الجهود الدولية في مكافحة الإرهاب الالكتروني، ص35.

الإرهاب " وتتجلى مجالات ومقومات هذه الإستراتيجية على سن سياسات وطنية تشمل الوقاية وتحديث التشريعات وتعزيز البحث العلمي لتوظيف التقنيات الحديثة في العمل الأمني، وتعزيز التعاون العربي . الدولي من خلال المشاركة في المؤتمرات الدولية ، المساهمة في وضع مدونة دولية لقواعد سلوك الدول في مكافحة الإرهاب بمختلف أشكاله وأنواعه[1].

وتواصلت الجهود العربية في مكافحة جرائم الإرهاب الالكتروني بانعقاد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وتوجت بتوقيع اتفاقية عربية لمكافحة تقنية المعلومات في نهاية سنة 2010، وتتكون من 43مادة تضمنت الأحكام الموضوعية المتمثلة في تجريم الأفعال المكونة لجرائم تقنية المعلومات كالاختراق والاعتراض والاعتداء على سلامة البيانات وغيرها،كما تناولت قضايا مكافحة الإرهاب الالكتروني، حيث نصت المادة 15 الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات كالأتي:

- ✓ . نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
- ✓ تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
- ✓ نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

ولقد صادت الجزائر على هذه الاتفاقية بموجب المرسوم الرئاسي رقم14-252 المؤرخ في 2014/09/08.

وفي سنة 2012 تم اعتماد وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون الخليجي، وقد نصت المادة29 على ضرورة معاقبة من يقوم بإنشاء مواقع الكترونية أو نشر معلومات عن طريق الشبكة الالكترونية أو إحدى وسائل تقنية المعلومات من أجل تسهيل الاتصالات بين أعضاء جماعة إرهابية أو بقصد ترويج أفكارها أو تمويلها، أو نشر كيفية صناعة الأجهزة الحارقة أو المتفجرة أو أية أدوات أخرى يمكن استخدامها في أعمال إرهابية.

الفرع الثاني: أهم التشريعات الوطنية المقارنة المتعلقة بمكافحة الإرهاب الالكتروني

تصنف الجريمة المعلوماتية أنها ذات تشعب على المستوى العالمي، فهي صنعت ما يسمى بالنطاق المصطنع الذي تشابكت فيه العلاقات القانونية،والاقتصادية والاجتماعية والسياسية[2]،و إذا كان المنطق يحتم أن يقع واجب الردع على الدولة التي يتم فيها استخدام الوسائل الالكترونية بشكل عام إلا أن الآمر لا يسير بهذا المنطق البسيط ذلك أن المستخدم قد يكون على اتصال مع عدة أشخاص وفي عدة دول ويتبادل معهم حوارا إلكترونيا خاصة إذا علمنا أن الاشتراكات في شبكة الانترنت تجاوزت مائة مليون في هدا الوقت وهدا ما يدعوا للتدخل وبشكل جدي لإيجاد قواعد تضبط هده

[1]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، ص130.

[2]. محمد السيد رشدي، الانترنت والجوانب القانونية لنظم المعلومات، مجلة الفتوى والتشريع، العدد 9، مجلس الوزراء، مايو 2000، ص108.

الفوضى، فجل التشريعات المقارنة نصت عن الجرائم الالكترونية ولم تذكر الإرهاب الالكتروني وتصنفه كجريمة قائمه بذاتها، وانسجاما مع متطلبات هده الدراسة سنتطرق أولا لتشريعات الدول الأجنبية ، ثم بعض التشريعات العربية .

1: أهم التشريعات الأجنبية المتعلقة بمكافحة الإرهاب الالكتروني:

اتجهت كافة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم تلك الجرائم الالكترونية الجديدة على قوانينها التقليدية القديمة وعليه فقد صاغت تلك الدول نصون قانونية جديدة قادرة على التعامل مع تلك الجرائم الجديدة والمتطورة تكنولوجيا.

وتعتبر دولة السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الانترنت والحاسب الآلي، لتستطيع أن تعاقب المتهمين بارتكاب تلك الجرائم الالكترونية، حيث أصدرت أول قانون خاص بها سمي بقانون(البيانات) عام 1973، وعالج هذا القانون قضايا الاحتيال عن طريق الانترنت بالإضافة إلى كونه يشتمل على فقرات عامة من نصوصه تتعلق بجرائم الدخول غير المشروع على البيانات الالكترونية أو تزوير المعلومات الالكترونية أو تحويلها أو الحصول غير المشروع عليها[1].

وكانت الولايات المتحدة من الدول السباقة في محاربة ظاهرة الإرهاب بوسائل الكترونية من خلال قوانينها الوطنية حيث صدر قانون جرائم الحاسب الآلي الفيدرالي عام 1984 بناءا على جهود الكونغرس بهذا الخصوص، وأطلق على هدا القانون (قانون الاحتيال وإساءة استخدام الحاسب الآلي (the computer frond and abuse Act) وفي سنة 1998 تم وضع مشروع القانون الأمريكي لجرائم الكمبيوتر والانترنت وأشار فيه صراحة إلى جرائم الانترنت ضد الحكومة وتشمل جرائم تعطيل الأعمال الحكومية وتنفيذ القانون والحصول على معلومات سرية ، والعبث بالأدلة القضائي والتأثير فيها وبث بيانات من مصادر مجهولة وتهديد السلامة العامة والإرهاب الالكتروني ،كما عمد البنتاغون سنة 2005 إلى إنشاء وحدة عسكرية متخصصة ، عهد إليها بمهمة تحصين الفضاء ألمعلوماتي الأمريكي وتامين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة[2]، وخولت وزارة العدل الأمريكية في عام 2000 خمس جهات حكومية للتعامل مع جرائم الانترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي (F B I) ،كما أصدرت بعدها عدة قوانين لمكافحة الإرهاب الالكتروني،ففي أكتوبر 2001 أصدرت اتفاقية لمكافحة الإرهاب ألمعلوماتي ، والتي وسعت من خلالها

[1]. منير محمد الجهني وممدوح محمد الجهني، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص187.

[2]. عبد المجيد حلاوة، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية، مكافحة جرائم الإرهاب ألمعلوماتي، في فترة 9. الى2006/04/13، ص 22.

سلطات البحث والتحقيق والمراقبة الإلكترونية وتعمل الحكومة الفيدرالية الأمريكية جاهدة على سن تشريعات متطورة لمكافحة هده الأنماط المستجدة للظاهرة الإرهابية ، وهناك العديد من الخطوات التي اتخذتها نذكرها بإيجاز:[1]

- ✓ إصدار قانون تعزيز امن المعلومات 2002
- ✓ . وضع إستراتيجية الوطنية لتامين الفضاء الالكتروني 2003
- ✓ . أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الالكتروني
- ✓ . تم إنشاء لجنة حماية البنية التحتية الحساسة والتي أطلق عليها مركز حرب المعلومات
- ✓ . إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات، وغيرها من المبادرات.

أما في بريطانيا فهي ثالث دولة تسن قانون خاص بها فيما يتعلق بجرائم الانترنت، حيث أقرت قانون لمكافحة التزوير والتزييف عام 1981،الذي شمل في تعار يفه الخاصة أداة التزوير ووسائط التخزين الحاسوبية المتنوع[2]،ثم جاء قانون 2000 لمكافحة الإرهاب والمعروف (terrorism act) والدي دخل حيز التنفيذ في فبراير 2001، وقد طرا عليه مجموعة من التعديلات منها:

- ✓ . تعديل سنة 2009 حيت أضاف هدا التعديل أفعال جديدة عدت تشجيعا للإرهاب مثل نشر التصريحات التي يمكن أن تفهم من الجمهور بأنها تشجيع مباشر أو ير مباشر آو تحريض على الإرهاب أو التجنيد الأعمال إرهابية كما تضمن أيضا جرائم التدريب على الإرهاب والتحضير له.
- ✓ . وفي سنة 2012 قرر مجلس النواب البريطاني طرح ومناقشة قانون يسم بموجبه لأحد وكالات المخابرات البريطانية بمراقبة كل الاتصالات الهاتفية والرسائل الالكترونية والنصية والأنشطة التي تمارس على شبكة الانترنت لمعالجة ظاهرة الإرهاب الالكتروني، مما أثار جدلا واسعا حول انتهاك الحرية الشخصية سواء في بريطانيا أو في العالم[3].

كما تعتبر التجربة الفرنسية في مكافحة الإرهاب من بين أهم التجارب التي يحتدا بها على الصعيد الإقليمي (الاتحاد الأوربي) ، حيث سن المشرع الفرنسي القانون رقم 88/19 المؤرخ في 5 فيفري 1988 والخاص بالجرائم المعلوماتية والحريات ولقد جرمت المادة 462 منه مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريقة ير مشروعة ، كما شددت العقوبة في الأحوال التي ينجم فيها عن هدا الولوج المحو أو التعديل في معطيات الآلية، واستعمال ألمستندات كما عاقب على هده الجرائم بعقوبة السجن أو الغرامة ، وخضع هدا القانون لتعديلات منها عام 1993 بحيث وسع من نطاق السلوكيات محل

[1]. شاشوة ياسمينة، الإرهاب الالكتروني بين مخاطره واليات مكافحته، المرجع السابق ، ص69.

[2]. صباح كزيز، أمال كزيز، الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم1،العدد8 ،2008، ص321.

[3]. منير محمد الجنبيهي وممدوح محمد الجنبيهي،جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق 188.

التجريم إضافة إلى فرض المزيد من العقوبات لتحقيق المزيد من الأبعاد الردعية[1] وتوالى إصدار القوانين المتعلقة بمكافحة الإرهاب منها قانون 2009 الذي سمح بمراقبة الهواتف والانترنت وزرع كاميرات مراقبة في الأماكن العامة وملاحقة أي فرنسي يسافر للتدرب على الأعمال الإرهابية خارج البلاد حتى ولو لم يرتكب جرما في فرنسا وقد أكد على هدا تعديل نوفمبر 2014 الذي نص على منع الفرنسيين من السفر للانضمام للجماعات الجهادية في سوريا, وفي مارس 2015 خرج إلى النور قانون جديد باسم (تعزيز مكافحة الإرهاب) والدي نص على جواز اختراق من وصفهم بالإرهابيين المحتملين ومراقبتهم دون الحاجة إلى موافقة قضائية عن طريق وضع ميكروفونات وكاميرات تجسس و غيرها، وفي تاريخ 23أبريل2015 تم إبرام اتفاق بين الحكومة الفرنسية وكبار مشغلي الانترنت لمكافحة الإرهاب الالكتروني التصدي للمواقع الجهادية، ويهدف الاتفاق إلى التصدي لمحاولات نشر التطرف والتعصب على الانترنت .

2: أهم التشريعات العربية المتعلقة بمكافحة الإرهاب الالكتروني:

سعت الدول العربية هي الأخرى لمكافحة الجرائم المستحدثة من ضمنها الإرهاب الالكتروني ودلك بسن تشريعات وقوانين جديدة خاصة بها لتستوعب المستجدات الإجرامية الحديثة، ولقد حققت دول مجلس التعاون لدول الخليج العربية تقدما ملحوظا في مجال استخدامات تكنولوجيا المعلومات.

وحظيت دولة الإمارات العربية المتحدة بموقع ريادي في هدا المجال، فهي تعتبر دولة أول دولة عربية تسن قانونا مستقلا لمكافحة الجرائم المعلوماتية ، وفي هدا السياق نصت المادة 21 من القانون الاتحادي رقم 2 لسنة2006 في شان مكافحة جرائم تقنية المعلومات على انه" 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 وسيلة تستخدم في الأعمال الإرهابية ، يعاقب بالحبس مدة لا تزيد على الخمس سنوات[2]،كما نصت في المادة 7 من قانون 1 لسنة 2004 بشان مكافحة الإرهاب على معاقبة كل من يقوم بتدريب شخصا أو أكثر على استعمال الأسلحة التقليدية أو غير التقليدية أو وسائل الاتصال السلكية واللاسلكية أو الالكترونية أو أية وسيلة اتصال أخرى أو علمه فنونا حربية أو أساليب قتالية أيا كانت بقصد الاستعانة به لتنفيذ عمل إرهابي بالسجن المؤبد أو المؤقت.

[1]. رائد عدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية حول توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ص.ص16 -17.

[2] . محمد أمين بشرى، التحقيق في الجرائم المستحدثة مركز الدراسات والبحوث، جامعة نيل العربية للعلوم الأمنية، الرياض،2004، ص293.

أما المملكة العربية السعودية فقد احتلت المركز السادس عالميا بين الدول التي تنطلق منها الهجمات الالكترونية نسبة إلى عدد مستخدمي الانترنت في البلاد فكان لابد لها من إصدار تشريع خاص بدلك ، حيث سبقت المملكة العربية السعودية نظراتها من الدول العربية في إصدار بعض الأنظمة واللوائح والتعليمات لمواجهة الاعتداءات الالكترونية والإرهاب الالكتروني ونصت على عقوبات في حال المخالفة لهده الأنظمة والتعليمات واللوائح ، كقرار مجلس الوزراء رقم (163) في 1417/10/24هـ الذي ينص على إصدار الضوابط لمنظمة لاستخدام شبكة الانترنت والاشتراك فيها، و يعد هدا القرار مبادرة من المملكة السعودية وسعيا منها لتنظيم التعاملات الالكترونية وضبطها[1]، ثم صدر المرسوم الملكي م/17في 1428/3/8هـ بناءا على قرار مجلس الوراء 79 ، حيث تضمن بيان معاني المصطلحات والمسميات ومنها الجريمة المعلوماتية والذي فرض عقوبات بالسجن والغرامة أو كليهما على كل شخص ينشأ موقعا لمنظمات إرهابية على شبكة المعلوماتية أو احد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أو نشر كيفية صنع المتفجرات.

أما في قطر فقد صدر القانون رقم 14 لسنة 2014 المتعلق بمكافحة الجرائم الالكترونية والذي نصت المادة 5 منه على أن "يعاقب القانون بالحبس مدة تتجاوز 3 سنوات والغرامة 500 ألف ريال لإدارة موقع يتبع تنظيما إرهابيا أو نشر أخبار تعرض الدولة لخطر أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية.

وفي عمان صدر المرسوم السلطاني رقم2007/8 الخاص بقانون مكافحة الإرهاب والذي يشير بصورة ضمنية للإرهاب الالكتروني كأحد صور الإرهاب، والمرسوم السلطاني رقم 2008/69 الخاص بقانون المعاملات الالكترونية كما أصدرت السلطنة قانون مكافحة جرائم الحاسب الآلي.

وكذلك الحال بالنسبة للمشرع الأردني، الذي أصدر قانون منع الإرهاب الصادر 2006/11/01 والدي شمل في طياته تعريف الإرهاب الإلكتروني وبتعدد الجرائم جرائم أنظمة المعلومات الالكترونية واتساع نطاقها اضطر المشرع الأردني لإصدار قانون خاص رقم 30 لسنة 2010 حيث نصت المادة 10 من هدا القانون 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 الترويح لإتباع أفكارها أو تمويلها يعاقب بالإشغال الشاقة المؤقتة"[2].

[1]. سامر مؤيد عبد اللطيف ونوري الشافعي، الإرهاب الالكتروني وسبل مواجهته، بحث منشور في مجلة كربلاء العلمية، العدد 14 العراق، العراق 2016، ص22.

[2]. على بوعمرة، جريمة الإرهاب الالكتروني، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، سنة 2021/2020، ص51.

وتفطن المشرع المغربي أيضا لخطورة انتشار الأجرام ألمعلوماتي وأثر دالك على امن واستقرار المجتمع المغربي وقد ظهر دالك فصدر ظهير شريف القانون رقم 01-07-129 في 30 نوفمبر 2007 لتنفيذ القانون رقم 53/05 المتعلق بالتبادل الالكتروني للمعطيات والقانونية وكذلك القانون رقم 03/03 المتعلق بمكافحة الإرهاب الصادر في 28 مايو 2003 الذي عرف الإرهاب بجميع أشكاله وأشار في البند السابع 7 منه إلى الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.[1]

أما في سوريا صدر قانون التوقيع الالكتروني وخدمات الشبكة، فضلا عن تقديم قانون مكافحة الإرهاب في 26 جوان 2012 إلى مجلس الشعب السوري، والذي يعرف المنظمة الإرهابية ويجرم العمل الإرهابي وتمويل الإرهاب فيها استعمال وسائل الاتصال والمعلومات.[2]

3. جهود المشرع الجزائري في مواجهة الإرهاب الالكتروني

حاول المشرع الجزائري سن قوانين داخلية مستنبطا من الجهود الدولية والاتفاقيات العالمية حتى يتفادى الوقوع في تنازع القوانين من جهة وسهولة توقيع العقاب من جهة أخرى غير انه لم يلم بالشكل الكافي بكل الجرائم المستحدثة بنظام المعطيات ، حيثعرف المشرع الجزائري الإرهاب بالأفعال الإرهابية أو التخريبية في القسم الرابع مكرر من قانون العقوبات تحت عنوان الجرائم الموصوفة بأفعال إرهابية أو تخريبه ، من خلال نص المادة 87 مكرر من ق ع ج التي سبق ذكرها في الفصل الأول[3]، كما أشار المشرع إلى جريمة الإشادة بالأفعال الإرهابية بموجب نص المادة87مكرر4 التي تنص على: يعاقب بالسجن المؤقت من خمس 5سنوات إلى عشر10سنورات وبغرامة ماليه من 100000دج الى500000دج كل من يشيد بالأفعال المذكورة في المادة87مكرر أو يشجعها أو تمويلها بأية وسيلة كانت، فالبر جوع إلى نص المادة استعمل المشرع عبارة (بأية وسيلة كانت) رغبة منه في توسيع مفهومها واحتواء جميع الوسائل التقنية التي ستظهر مستقبلا ، فنظريا يمكن تطبيق نص المادة على أفعال الإرهابية التي تتم باستعمال تكنولوجيا الإعلام والاتصال الحديثة كالهاتف النقال وشبكة الانترنت.....الخ ، ومع ذلك يبقي نصوص هذه المواد غير قادر على استيعاب كافة أشكال الإجرام الالكتروني بما يفرض على المشرع تعديلها لتصبح بأي وسيلة تقنية أو معلوماتية كانت أو التجريم بموجب نص جديد.

كما قام المشرع بتعديل قانون العقوبات رقم 15/04 المؤرخ في 11/10/ 2004 وأدرجها تحت اسم المساس بأنظمة المعالجة الآلية للمعطيات (المواد من 394مكرر الى394 مكرر7)،وعرف المشرع الجزائري المنظومة المعلوماتية في المادة 2 فقرة

[1]. على بوعمرة، جريمة الإرهاب الالكتروني، المرجع السابق، ص50.

[2]. شاشوة ياسمينة، الإرهاب الالكتروني بين مخاطره واليات ومكافحته، المرجع السابق ص91.

[3]. قانون 15/04 المؤرخ في 2004/11/10، المرجع السابق.

ب من القانون 04/09 بأنها" أي نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[1]، ويمكن إيجاز مختلف صور الاعتداءات على النحو التالي:

ا . الدخول الاحتيالي إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات أو البقاء فيه بنص المادة394مكرر، ويعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 20000الى50000 دج.

. وتضاعف العقوبة إذا ترتب على ذلك جدف أو تغير لمعطيات المنظومة.

. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 30000 إلى 50000 دج.

ب . الإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها المادة 394 مكرر1: يعاقب بالحبس من ستة أشهر إلى 3 سنوات وبغرامة من 400000 إلى 500000دج.

ج . تصميم أو بحث أو تجميع أو اتجار أو توفير أو نشر معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية . حيازة أو إفشاء أو نشر أو استعمال لأي غرض كلن المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم المادة 394 مكرر2: يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1000000 إلى 10000000دج كل من يقوم بها عمدا أو عن طريق الغش.

د . إضافة إلى أن المشرع في المادة 394 مكرر5 قرر نفس العقوبة المقررة للجريمة ذاتها لكل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر وكان هذا التحضير مجسدا بفعل أو عدة أفعال.

وقد ضاعف المشرع العقوبة في حالة ما إذا:

. استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام فتطبق عقوبات اشد المادة 394 مكرر3

. كما يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها غرامة تعادل 5 أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي المادة 394 مكرر4.

. كما لم يغفل المشرع عن الحكم في الأجهزة والبرامج والوسائل المستخدمة وكذا المواقع والمحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم صاحبها من مصادرة وإغلاق دون المساس بالغير حسن النية المواد 394مكرر6 ومكرر7.

ولقد عملت السلطات العليا في الدولة على سن جملة من النصوص القانونية وتعديل أخرى حتى تتكيف مع تطورات الممارسات الإرهابية متعددة الأبعاد ، و هذا ما اقره منطوق المادة 87 مكرر12ق .ع "يعاقب بالسجن المؤقت من خمس

[1] . نص المادة 2 فقرة ب من القانون04/09، المرجع السابق.

سنوات إلى عشر سنوات وبغرامة 100000 دج إلى 500000دج كل من يستخدم تكنولوجيا الإعلام والاتصال كشبكات التواصل الاجتماعي لتهديد الأشخاص لصالح عمل 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"[1]

كل هذه التعديلات إلا أنه لازال هناك قصور في الحد من هذه الجرائم مما دفع المشرع إلىإصدارر قانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،والذي جمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصادرها والتعرف على مرتكبيها-، وعلى صعيد أخر اصدر تم القانون06/15 المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب[2]، والمرسوم تنفيذي رقم 113/15 في 12 مايو 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 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".

المطلب الثاني: الإطار المؤسساتي الدولي لمكافحة الإرهاب الالكتروني

إن مبدأ التعاون الدولي في العالم المعاصر من أهم المبادئ القانونية الدولية الحديثة، وبرز هذا المبدأ بشكل كبير في مجال مكافحة الجريمة مع تعدد وتشعب التطورات التي لحقت بها وبأساليب ارتكابها ويجري التعاون الدولي التشريعي لمكافحة الجرائم الالكترونية، ومن ضمنها الإرهاب الالكتروني من خلال إبرام الاتفاقيات الدولية وتشكيل المؤسسات الشرطية والأمنية المتخصصة لمواجهتها.

الفرع الأول: دور المؤسسات الدولية والإقليمية في مكافحة الإرهاب الالكتروني

في سبيل تنفيذ الاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب أنشئ مكتب فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب الذي اكتسب طابعا مؤسسيا في إدارة الشؤون السياسية التابعة للأمم المتحدة في ديسمبر2009

[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]. القانون رقم 06/15 المؤرخ في 15 فبراير2015 يعدل ويتمم القانون رقم 01/05 المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها المعدل والمتمم.

عبر قرار الجمعية العامة A/RES/64/235،وفي سبتمبر 2011أنشئ مركز الأمم المتحدة الدولي لمكافحة الإرهاب من اجل تعزيز التعاون الدولي لمكافحة الإرهاب ودعم الدول الأعضاء في تنفيذ الاستراتيجية العالمية لمكافحة الإرهاب[1]

كما اعتمدت الجمعية العامة القرار 71/291والمؤرخ في 15 يونيو عام 2017 بإنشاء مكتب الأمم المتحدة لمكافحة الإرهاب ،الذي يقع على عاتقه التزام حسب المهام المخولة في الميثاق أن يتخذ كل ما في وسعه لمكافحة الإرهاب الدولي بجميع أشكاله وأنواعه ، ولعل أشهر قرار اتخذه مجلس الأمن القرار رقم 1373 والذي نص على جملة من التدابير الملزمة للدول أهمها التزام جميع الدول بتحريم تقديم المساعدة للأنشطة الإرهابية وعدم توفير الدعم للجماعات الإرهابية وضرورة تبادل المعلومات بشان الجماعات التي تخطط لشن هجمات إرهابية كما اتخذ مجلس الأمن القرار 1535 في مارس 2004 والذي نص على إنشاء المديرية التنفيذية للجنة مكافحة الإرهاب من اجل تقديم المساعدة التنفيذية للبلدان فضلا عن توثيق التعاون والتنسيق داخل منظومة مؤسسات الأمم المتحدة وفيما بين الهيئات الإقليمية والحكومية الدولية.

1. منظمة الشرطة الجنائية الدولية الانتربولF B I

تم إنشاؤها في 1923/09/07 وتعد من أهم المنظمات الناشطة في مجال مكافحة الجريمة نظرا لما تقدمه من إمكانية تعقب وضبط مرتكبي الجرائم على اختلاف أنواعها أينما وجدوا وتسليمهم إلى الهيئات المختصة بغية محاكمتهم وتوقيع العقوبة المناسبة عليهم، تضم حاليا 190 بلد عضو ويعمل لديها 541 موظف من 79 جنسية مختلفة ومقرها الحالي ب "ليون" فرنسا، وان من أبرز صور وأشكال ووسائل التعاون بين أجهزة الشرطة ما يلي:[2]

- ✓ . التعليم والتدريب الشرطي المتخصص والمعونات الفنية وتبادل المراجع والخبرات والبحوث.
- ✓ . ربط شبكات الاتصال والمعلومات حيث يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة عن طريق إنشاء شبكة اتصالات خاصة.
- ✓ . بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة جرائم الانترنت.

وقد انضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية أثناء انعقاد الجمعية العامة للإنتربول بهلسنكي / فنلندا ، خلال شهر أوت 1963 ، بمشاركة53 بلدا ممثلة بالمكتب المركزي الوطني ،حيث يعمل المكتب المركزي الوطني تحت الوصاية المباشرة لمديرية الشرطة القضائية/المديرية العامة للأمن الوطني يباشر مهامه وفقا لنصوص التشريعات الوطنية، ومن مهامه مباشرة التحقيقات الدولية من والى الخارج الوطن بالتنسيق مع المصالح الوطنية ونظيراتها الأجنبية، تقديم الدعم الفني والتقني

[1].ناصر العلي، الجهود الدولية في مكافحة الإرهاب الإلكترون، المرجع السابق، ص 38.

[2]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية،المرجع السابق، ص148.

إلى كافة الأجهزة والمصالح المكلفة بإنفاذ القانون ، التبادل السريع والاني للمعلومات الشرطة والجنائية ما بين المكاتب المركزية الوطنية ، بالتنسيق مع الأمانة العامة لمنظمة الانتربول، ملاحقة المجرمين المبحوث عنهم دوليا بغرض الإيقاف والتسليم بالإضافة إلى ألتقص والتحري في جوازات السفر المزورة محل بحث دولي أو وطني .

2. المكتب الأوروبي للشرطة الأور وبولEuropol

أنشأ المجلس الأوروبي في لكسمبورج منظمة الشرطة الأوروبية"اليوروبول" عام 1999، في سبيل تحسين التعاون الشرطي بين الدول الأعضاء في الاتحاد الأوروبي من اجل مكافحة كل الأشكال الخطيرة للأجرام الدولي ويقوم في سبيل ذلك بما يلي:[1]

- ✓ . تسهيل تبادل التعاون بين الدول الأعضاء، وتجميع وتحليل المعلومات
- ✓ . تبليغ المصالح المختصة الأعضاء بالمعلومات التي تخصهم حول مختلف الأنشطة الإجرامية.
- ✓ . تسهيل التحقيقات في الدول الأعضاء، إضافة إلى تسيير جمع المعلومات.

3. المكتب العربي للشرطة لجنائية

أنشأ مجلس وزراء الداخلية العرب ، هدفه تامين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة ، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء، ومن ضمن مهامه القيام ببعض العمليات الشرطية والأمنية المشتركة كتعقب مجرمي المعلوماتية عامة وشبكة الانترانت خاصة ، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية.[2]

4 . منظمة الشرطة الجنائية الأفريقية(الافريبول):

هي منظمة تسهل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والإرهاب والمخدرات والاتجار بالأسلحة في إفريقيا ، وهي اكبر منظمة شرطة في القارة الإفريقية أنشئت يوم 13 ديسمبر 2015 في الجزائر مكونة من قوات الشرطة ل 41 دولة مقرها الرئيسي في أعالي بن عكنون ،وتلعب هذه المنظمة دورا ايجابيا في :

- ✓ ردع الإجرام الالكتروني على مستوى القارة الافريفية.

[1] . عبيد حسام، التعاون الشرطي في مكافحة الجريمة مذكرة لنيل شهادة الماستر تخصص جريمة وامن عمومي، جامعة العربي تبسي، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية2020 /2021، ص16.

[2]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية،المرجع السابق، ص 148

- ✓ ونشر الوعي الإفريقي بخطورة الإجرام الالكتروني وتجلى هذا في إبرام اتفاقيات وعقد ندوات إقليمية بغية وضع حد لهذه الظاهرة الخطيرة.
- ✓ كما أنها تعمل على تكوين وإعادة تأهيل أجهزة الشرطة ببعض البلدان الإفريقية التي تعاني نقصا في هذا المجال .
- ✓ وتلعب أيضا دورا أساسيا في تعزيز التعاون بين إفريقيا ومنظمة الانتربول وأجهزة الشرطة في القارات الأخرى.

مما سبق يتبين أن المنظمات والهيئات الدولية والإقليمية الخاصة بتتبع الجرائم المعلوماتية والكشف عنها وإلقاء القبض على مرتكبيها لها دور فعال في التصدي لهذه الجرائم، لكن يبقى دورها قاصرا عن تتبع كل الجرائم وهذا راجع إلى إحجام المجني عليهم عن التبليغ من جهة، والطابع العالمي لهذه الجرائم مما يستدعي تعاونا دوليا لتحقيق قانون جنائي موضوعي وإجرائي للحد من هذه الجرائم العابرة للقارات.

الفرع الثاني: دور المؤسسات الوطنية في مكافحة الإرهاب الالكتروني

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 الحديث، وعلى هذا الأساس تم تعديل واستحداث مؤسسات أوكلت إليها مهمة التصدي لمثل هذه الجرائم المستحدثة.

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نصت المادة 13 من القانون رقم 04/09 على إنشاء هيئة وطنية للوقاية من هذه الجرائم، وهي تعد سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساسا أعضاء من الحكومة معينين ومسئولي مصالح الأمن وقاضيين اثنين من المحكمة العليا كما تضم قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية الدرك الوطني والأمن الوطني. وتتولى هذه الهيئة مهام خاصة هي حسب المادة 14 من نفس القانون:

- ✓ . تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
- ✓ . مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن ذات الصلة بتكنولوجيات الإعلام والاتصال.
- ✓ . ضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئة وطنية أخرى[1].

[1]. انظر المادة 14 من القانون 04/09، المرجع السابق.

2. الهيئات القضائية الجزائية المتخصصة:

بموجب القانون 04/14 المؤرخ في 10 نوفمبر 2004 تم إنشاء هيئات قضائية[1]، تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد(32،37،40) من قانون الإجراءات الجزائية، تتمتع بمباشرة مهامها في دائرة الاختصاص الإقليمي الموسع، بحيث تنظم في القضايا المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا، وإذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني (المادة15من القانون 04/09).

نص المشرع الجزائري على توسيع اختصاص كل من قاضي التحقيق ووكيل الجمهورية وتوسيع محاكم الجنح:

- ✓ طبقا للمادة37 ق اج ج يتحدد الاختصاص المحلي لوكيل الجهورية ومساعديه بنطاق المحكمة التي يباشرون فيها مهامهم، ولكن في حالة الجرائم الخطيرة يتم تمديد الاختصاص الإقليمي للنيابة العامة للأقطاب القضائية الأربعة وهي محاكم سيدي محند، وهران وقسنطينة ورقلة التي دائرة اختصاص عدة مجالس قضائية أخرى في الجرائم المنصوص عليها بالمادة 2/37 ق. ا.ج ج على أن يكون ذلك عن طريق التنظيم[2]

فإذا اعتبر النائب العام لدى المجلس القضائي الذي تقع باختصاصه المحكمة ذات الاختصاص الموسع أن الإجراءات تتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات يطالب بالإجراءات ويجوز له المطالبة بها أثناء جميع مراحل سير الدعوى ، وفي حالة فتح التحقيق قضائي يصدر قاضي التحقيق امرأ بالتخلي عن الإجراءات لصالح قاضي التحقيق لدى المحكمة المختصة المذكورة بالمادة 40 مكرر من ق.ا. ج ويحتفظ الأمر بالإيداع أو أمر القبض في حالة صدورهما بالقوة التنفيذية إلى حين الفص فيها من طرف المحكمة المختصة بإتباع الإجراءات الجزائية العادية[3]

- ✓ يتحدد الاختصاص المحلي لقاضي التحقيق حسب المادة 40 فقرة 1وفقا ل: مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم أو محل القبض على احد هؤلاء الأشخاص حتى ولو كان هذا القبض حصل لسبب أخر، و بموجب الفقرة الثانية من نفس المادة وسع المشرع الاختصاص المحلي لقاضي التحقيق كلما تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الإلية للمعطيات، وبالتالي يصبح لقاضي التحقيق التابع لهذه المحكمة اختصاص إقليمي يتجاوز أخصاصه العادي.
- ✓ كما يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة329ق. ا.ج .ج إما بمكان وقوع الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم، غير أن المشرع بموجب التعديل 14/04 أضاف فقرة أخرى وسع فيها الاختصاص المحلي للمحكمة إلى محاكم أخرى عن طريق التنظيم في حالة الجرائم الماسة بالمعالجة الآلية للمعطيات.

---

2. القانون 04-14 المؤرخ في 2004/11/10، المتضمن ق ا.ج.ج، جريمة الرسمية عدد17 العدد49، المعدل والمتمم.

[2]. روابح فريد، محاضرات في قانون الإجراءات الجزائية كلية الحقوق والعلوم السياسية، جامعة لمين دباغين، سطيف 2.

[3]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية،المرجع السابق ص214

وعزز المشرع الجزائري بموجب القانون 22/06 نشاط الضبطية القضائية بإجراءات خاصة لمواجهة بعض الجرائم ، عرفها الفقه على أنها الإجراءات والتقنيات التي تتخذها الشرطة القضائية بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات وجمع الأدلة والكشف عن مرتكبيها وذلك دون علم ورضا الأشخاص المعنيين[1]وقسم المشرع هذه الأساليب وحصرها بالصور التالية: المراقبة واعتراض المراسلات وتسجيل الأصوات والتقاط الصور ثم التسرب، وأضاف القانون 01/06المتضمن قانون الفساد بمقتضى المادة 56 منه الصور التالية إذا تعلق الأمر بجرائم الفساد والتسليم المراقب والترصد الالكتروني والاختراق.

إن هذه التعديلات الواردة بقانون الإجراءات الجزائية والمتعلقة بتوسيع اختصاص جهات المتابعة والتحقيق وبالتالي الحكم كلما تعلق الأمر بجرائم المساس بنظام المعالجة الآلية للمعطيات كانت بهدف وضع إطار إجرائي متماسك بإمكانه التحري والفصل في هذا النوع من القضايا بكل مهنية لإنجاز هذا الغرض يفترض أن تكون هذه الجهات معززة بقضاة متخصصين في جميع المجالات[2]

3. الوحدات التابعة للمدرية العامة للأمن والدرك الوطني

تلعب الوحدات التابعة للمدرية العامة للأمن الوطني والدرك الوطني دورا هاما في مكافحة جرائم الإرهاب الالكتروني،حيث تتكون المديرية العامة للأمن الوطني من مصلحة مركزية وفرق محلية، إضافة إلى المخبر المركزي للشرطة العلمية بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران وتحتوي على فروع تقنية من بينها خلية الإعلام الآلي.

أما الوحدات التابعة للدرك الوطني فإن الدرك يضع وحدات متنوعة وعديدة على مستوى القيادة العليا أو على مستوى القيادات الجهوية والمحلية وذلك حفاظا على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها (المصالح والمراكز العلمية والتقنية ، هياكل التكوين المركزي للتحريات الجنائية ، المعهد الوطني لعلم الإجرام) ،و يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببيشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام وإلكترونيك الذي يقوم بالتحقيق في الجرائم الالكترونية بتحليل الأدلة وذلك من خلال تحليل الدعامة الالكترونية ، وانجاز المقاربات الهاتفية ، وتحسين التسجيلات الصوتية والفيديو والصور وذلك لتسهيل استغلالها ، بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مرداس والتابع لمديرية الأمن العمومي للدرك الوطني[3].

[1]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية،المرجع نفسه، ص215.

[2]. بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، المرجع السابق، ص82.

[3]. بن كثير بن عيسى، الإجراءات الخاصة المطبقة على الإجرام الخطير، المرجع السابق، ص82.

فعلى سبيل المثال سنة 2016 سجلت مديرية الشرطة القضائية بالمديرية العامةللأمن الوطني وجود 11 قضية متعلقة بالإرهاب الالكتروني اغلبها خاصة بتهديدات داعش الإرهابي، وبالبحث والتحري بين مختلف القطاعات المختصة تم توقيف 58 شخص متورط في قضايا الإرهاب الالكتروني تمت إحالتهم على القضاء وقد استطاع أيضا الجيش الالكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا، من خلال فك شفرات الرسائل المتبادلة عبر الفايس بوك والتوتير.

المبحث الثاني: الحماية الإجرائية ضد الإرهاب الالكتروني

سوف نتناول في هذا المبحث الحماية الإجرائية ضد الإرهاب الالكتروني كأساس لمنع وقمع الإرهاب الالكتروني، في المطلب الأول تحت عنوان آليات التعاون الدولي لمكافحة الإرهاب الالكتروني أما المطلب الثاني سوف نتطرق إلى المواجهة الإجرائية للإرهاب الالكتروني في التشريع الجزائري كمطلب ثاني.

المطلب الأول: آليات التعاون الدولي لمكافحة جريمة الإرهاب الالكتروني:

يتحقق التعاون الدولي عن طريق وسائل وطرق عديدة يمكن اللجوء إليها لمنع وقوع العمليات الإرهابية أو الحد منها والتي أصبحت اليوم هاجس يهدد العلاقات الدولية، ذلك أن خطورة الأعمال الإرهابية تكمن في اعتمادها على تقنيات متقدمة مثل أجهزة تصنت على شبكات الاتصال وبرمجيات التشفير وبرمجيات اختراق أنظمة امن الشبكات والحاسبات.

الفرع الأول: آليات التعاون الإجرائي لمكافحة جريمة الإرهاب الالكتروني

وتختلف وسائل المنع باختلاف نوع العمل الإرهابي والهدف الذي يوجه إلية ومن هذه الوسائل والإجراءات التي يمكن اتخاذها لمنع جرائم الإرهاب هي:

1. المساعدة المتبادلة بين أجهزة الشرطة الجنائية المختصة:

أسهم تبادل المعلومات بين أجهزة الشرطة المعنية في العديد من الدول إلى إحباط العديد من المخططات الإرهابية على مديري هذه العمليات ويمكن أن تتم المساعدة المتبادلة بين أجهزة الشرطة من خلال المنظمة الدولية للشرطة الجنائية(الانتربول) ، كما يمكن أن تتم في إطار العلاقات الثنائية بين الدول أو من خلال المنظمات الإقليمية عن طريق تنسيق جهود الأعضاء فيها لمكافحة ظاهرة الإرهاب[1]، كما يهتم الانتربول بمواجهة الجرائم الالكترونية وعلى رأسها الإرهاب الالكتروني ، حيث تعمل هذه المنظمة على تحليل وسائل التواصل الاجتماعي للوصول إلى البيانات والأدلة التي تدين الارهابين وتدل

[1]. رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، مجلة الحقوق والعلوم السياسية، المجلد3، العدد3، جامعة زيان عاشور بالجلفة كلية الحقوق والعلوم السياسية، ص187.

على أماكن تواجدهم لتسهيل الوصول أليهم ومنع هذه العلميات الإرهابية سواء التي تتم على ارض الواقع أو تلك الالكترونية، وكثيرا ما يسهم التعاون الدولي بين أجهزة الشرطة في تحقيق المساعدة القضائية المتبادلة وذلك عندما تكلف مثلا أجهزة الشرطة بالقيام ببعض المهام في دولة أخرى بناء على أمر صادر من السلطة القضائية ، أو عند القيام بالبحث عن الأشخاص بناء على أوامر القبض الصادرة من المحاكم.[1]

ونصت عليها المادة 16 من القانون 04/09 على انه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكشف مرتكبيها،يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني.

2. تبادل المعلومات المتعلقة بالأشخاص والمنظمات الإرهابية

غالبا ما نجد هذه الوسائل والإجراءات منصوص عليها في بعض الاتفاقيات الدولية المتعلقة بمكافحة الإرهاب، والتي تفرض التزاما على الدول الأطراف فيها باتخاذ التدابير الملائمة لمنح حدوث الجرائم الإرهابية ومن بينها ضرورة تبادل المعلومات المتعلقة بهذه الجرائم وبمقترفيها والإجراءات التي اتخذت ضدهم ، وغير ذلك من المعلومات التي قد تباعد على إجهاض مخططات الإرهاب وضبط التنظيمات الإرهابية، وهذا ما اقره الإعلان الخاص الذي صدر عن لجنة وزراء مجلس أوربا سنة 1978 والذي تضمن الإشارة إلى ضرورة التزام الدول الأعضاء منح الأولوية لتحسين وسائل الإخطار السريع للمعلومات المتعلقة بالحوادث الإرهابية إلى الدول المعنية ،والظروف المحيطة بها والإجراءات التي اتخذت ضد مرتكبيها.

3. اتخاذ عدد من الإجراءات والتدابير الوقائية

وقد تكون وسيلة التعاون عن طريق اتخاذ عدد من الإجراءات والتدابير الوقائية على مستوى الموانئ والحدود والمطارات، وذلك عن طريق تكثيف فحص وتفتيش المسافرين والتأكد من طبيعة ما يحملونه، ولقد نص القرار الصادر عن الجمعية العامة للمنظمة الدولية للطيران المدني على حظر حمل الأسلحة من قبل الأفراد على متن الطائرة والتفتيش عنها، كما يجيز قرار الجمعية العامة لهذه المنظمة لموظفي الآمن حق الاطلاع على جوازات السفر في أي وقت للتحقق من شخصية المسافرين[2].

أ. الحفظ العاجل للبيانات المعلوماتية الأمر بتسليمها

يقصد بالتحفظ العاجل للبيانات المعلوماتية توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية

[1]. رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، المرجع السابق، ص188

[2].احمد رفعت وصالح بكر الطيار،الإرهاب الدولي، مركز الدراسات العربي الأوروبي، سنة1988 ص 241

ويشمل إجراء الحفظ: المعلومات أو الصور أو الوسائل أو الأصوات التي عادة يتم تخزينها ومعالجتها ونقلها بواسطة تقنية المعلومات، كالأرقام والرموز والأحرف[1].

ب . تفتيش المعلومات المخزنة

ومن اجل الكشف عن الجرائم ومتابعة مجرمي الإرهاب الالكتروني لا بد من تفتيش البيانات المخزنة في تقنية المعلومات أو جزء منها أو إحدى وسائط تخزين المعلومات الالكترونية شريطة للتقيد بالضوابط القانونية للتفتيش واحترام الحياة الخاصة للأشخاص، وفي هذا الصدد تلزم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بضرورة تفتيش المعلومة المخزنة[2].

ج . اعتراض بيانات المحتوى:

تعد من التدابير الإجرائية لردع الإرهاب الالكتروني اعتراض بيانات المحتوى الذي نصت علية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات دون تعريفه في حين عرفته اتفاقية بودابست ل سنة2001على أنها (بيانات كومبيوتر متعلقة باتصال عن طريق نظام كومبيوتر والتي تنشان عن طريق نظام كومبيوتر يشكل جزءا في سلسلة الاتصالات توضح المنشأ والوجهة والزمن والتاريخ والحجم والمدة ونوع الخدمة الأساسية.

الفرع الثاني: التعاون القضائي لمكافحة الإرهاب الالكتروني

يقصد بالتعاون القضائي، تعاون السلطات القضائية في مختلف الدول لمكافحة الجريمة، ويهدف هذا التعاون إلى التقريب في الإجراءات الجنائية من حيث إجراءات التحقيق والمحاكمة إلى حين صدور الحكم على المتهم وضمان عدم إفلاته من العقاب نتيجة لارتكابه جريمته في عدة دول، والتنسيق بين السلطات القضائية في هذا الشأن يجري للاتفاق على معايير موحدة[3].

1. تسليم المجرمين

عرفت المعاهدة النموذجية لتسليم المجرمين الصادر بقرار الجمعية العامة للأمم المتحدة رقم116/45 تسليم المجرمين على انه "مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم علية إلى دولة أخرى ليحاكم بها أو ينفذ فيها الحكم الصادر عليه من محاكمتها " وفي هذا الشأن ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتسليم مرتكبي الجرائم الالكترونية بما فيها الإرهاب الالكتروني ، وأجازت أيضا الامتناع عن

[1]. بوعنادة فاطمة الزهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول 2013، ص 71.

[2]. المادة 02 من الاتفاقية العربية لمكافحة تقنية المعلومات لسنة 2010.

[3]. محمد تقي ومحمد أمين، التعاون الدولي في مواجهة جريمة الإرهاب الالكتروني، المرجع السابق، ص190

تسليم مواطنيها على أن تتعهد للدول الأطراف الأخرى التي تتقدم إليها بطلب الملاحقة بالمتابعة القضائية ضد مواطنيها الذين ارتكبوا جرائم الكترونية في هذه الدول .

وأشارت المادة 15 من القانون 04/09 إلى أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

2 . نقل الإجراءات

يقصد بنقل الإجراءات قيام إحدى الدول باتخاذ الإجراءات الجنائية بشأن جريمة في إقليم دولة أخرى ولمصلحة هذه الدولة بناء على اتفاقية، وذلك إذا توفرت شروط معينة أهمها:[1]

- ✓ . أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها.
- ✓ . أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب منها عن ذات الجريمة.
- ✓ . أن يكون الإجراء المطلوب اتخاذه يؤدي إلى الوصول إلى الحقيقة كان تكون أدلة الجريمة موجودة بالدولة المطلوب منها.

3. المساعدة القضائية الدولية

تعتبر المساعدة القضائية كل إجراء قضائي من شانه تسهيل ممارسة الاختصاص القضائي في دولة أخرى بصد جريمة من الجرائم ومعظم الاتفاقيات الدولية الخاصة بمكافحة الإرهاب تتضمن نصوصا تقضي بضرورة اللجوء إلى المساعدة القضائية بين الدول المتعاقدة من اجل تحقيق العالية والسرعة في إجراءات ملاحقة وعقاب جرائم الإرهاب، وهذا الالتزام تبرره ضرورة المصلحة المشتركة لجميع الدول المتعاقدة في مواجهة الأعمال الإرهابية.[2] ومن صور المساعدة القضائية تبادل المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن اتهامات وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما أن هناك مطهر أخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة، من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي للفرد المحال إليها.

وعليه من اجل مواجهة الإرهاب الالكتروني بفاعليه مثمرة، ينبغي الاعتماد على المعايير الأساسية التالية:

- ✓ . إتباع قواعد ومبادئ القانون الدولي

[1]. رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، المرجع السابق ص189

[2]رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، مرجع نفسه، ص191

- ✓ . الإدانة العالية والاعتراف بعدم شرعية الإرهاب بجميع مظاهرة وأيضا الإرهاب الالكتروني
- ✓ التعاون الدولي وتبادل المعلومات بين الدول حول الظواهر الإرهابية
- ✓ . حتمية مسؤولية الارهابين السيبرانيين الذين ارتكبوا الجريمة الإرهابية
- ✓ . فعالية إجراءات مكافحة الإرهاب السيبراني.[1]

وتبقى مشكلة الاختصاص القضائي في جرائم الإرهاب له بالغ الأهمية، وذلك في حالة رفض تسليم مرتكبي الجرائم الإرهابية من قبل الدولة المطلوب إليها التسليم ، إذ يتعين عليها هنا القيام بمحاكمة الفاعل عما ارتكبه من جرائم، وتأخذ الاتفاقيات الدولية بمبدأ إما أن تسلم وإما أن تحاكم وهذا المبدأ يقتضي تأسيس اختصاص محاكم الدولة بالنظر في الجرائم الإرهابية وذلك عندما تمتنع الدولة عن تسليم مرتكبي هذه الجرائم حتى لا يفلت المتهم من العقوبة، وفي هذا الشأن تلعب المنظمات الدولية دورا هاما من خلال إصدار توصيات تلزم الدول باللجوء إلى المساعدة القضائية المتبادلة لقمع الجرائم الإرهابية والتوصية بإزالة العقبات القانونية التي قد توجد في التشريعات الوطنية تحول دون تسليم أو محاكمة مرتكبي جرائم الإرهاب، فالاختصاص القضائي العالمي يشكل اليوم أساسا مناسبا للتصدي للإرهاب عموما والإرهاب الالكتروني خصوصا ويشكل صورة مثلى للتعاون بين الدول على صعيد التعاون القضائي فيما بينها[2].

المطلب الثاني: المواجهة الإجرائية لمكافحة الإرهاب الالكتروني في التشريع الجزائري

إن أداة الجريمة في الإرهاب الالكتروني تتمثل في شبكة الانترنت مما يثير الكثير من الإشكالات ، كصعوبة اكتشافها وإثباتها وغياب الدليل المادي الذي يدين مرتكبيها ، ونتيجة لغياب إستراتيجية فعالة لمحاربتها والتقليل منها، سارعت التشريعات إلى وضع قوانين صارمة لهذا النوع من الجرائم ، والمشرع الجزائري بدوره عمد على إرساء ترسانة قانونية محاولة منه توفير الحماية القانونية ضد هذا النوع من الجرائم من خلال تعديل قانون العقوبات لجعله يتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال إلى جانب تعديل قانون الإجراءات الجزائية بالأمر رقم 22/06 ، وكذا إصدار قانون رقم 04/09 الذي دعم به النصوص الواردة في قانون الإجراءات الجزائية ، وهذا كله من اجل الإحاطة الفعالة لقمه هذه الجريمة.

الفرع الأول: الإجراءات العامة لمتابعة جريمة الإرهاب الالكتروني

وضع المشرع إجراءات استثنائية للمتابعة في جريمة الإرهاب الالكتروني ،يتم العمل بها أمام جهات التحقيق الأولي على غرار الإجراءات العادية للمتابعة الجزائية وفقا للمبادئ العامة، وقد نظمها المشرع الجزائري في قانون الإجراءات الجزائية من خلال التعديل الواقع بموجب القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 ، المعدل والمتمم ، والذي تضمن كيفية

[1]. ناصر العلي، الجهود الدولية في مكافحة الإرهاب الالكتروني، المرجع السابق، ص42

[2]. رمزي حوحو، التعاون الدولي لمكافحة جرائم الإرهاب، المرجع السابق،ص191.

تطبيق بعض الإجراءات البحث والتحري التقليدية على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب ، إضافة إلى إدراجه لبعض الإجراءات الخاصة كاعتراض المراسلات وتسجيل الأصوات والتقاط الصور والمراقبة الالكترونية وعزز المشرع الجزائري المنظومة القانونية بإصداره الأمر رقم 04/09 المؤرخ في 2009/8/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، إذ ابرز من خلاله المشرع الجزائري اتجاهه نحو تسمية الجرائم المستحدثة بتسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1].

1. الإجراءات المادية:

تتمثل الإجراءات المادية في المعاينة التقنية من جهة والتفتيش في بيئة الكترونية وكذا ضبط الدليل الرقمي، وسوف نبينها فيما يلي:

أ. المعاينة التقنية

المقصود بالمعاينة التقنية المكان الذي ارتكبت فيه الجريمة ،الوعاء الأساسي الذي يحتوي على اخطر الأدلة الجنائية التي يخلفها الجاني وراءه عقب تنفيذ الجريمة ، حيث ينتقل ضباط الشرطة القضائية إلى ذلك المكان للمعاينة واثبات الآثار المادية للجريمة والمحافظة عليها واثبات حالة الأماكن والأشخاص وكل ما يفيد كشف الحقيقة ، وقد نصت المادة 42منق.ا.ج.ج على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو مخول لجهاز الضبطية القضائية سواء في الحالة العادية أو حالات التلبس[2]وحتى تحقق المعاينة ثمارها وتفي بأغراضها المشهودة نجد أن التشريعات قررت جزاءات جنائية على كل من يقوم بإجراء أي تغير على حالة الأماكن التي فيها الجريمة أو ينزع أي شيء منها[3] أو يحدث تعديلا في مكان وقوع الجريمة قبل قيام سلطة التحقيق أو الاستدلالات بإجراء المعاينة الأولى، حسب نص المادة 43 من ق. ا.ج.ج .

وإذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فان جريمة الإرهاب الالكتروني تتم فيها المعاينة على مستويين:

- ✓ . المسرح التقليدي وهو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة من أمثلة ذلك أشرطة الحاسب والكابلات الخاصة به وشاشة العرض ومفاتيح التشغيل ....

[1]. عز الدين عثماني إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات والنظم السياسية، العدد الرابع جانفي2018.

[2]. عبد الله ماجد العكايلة، الوجيز في الضبطية القضائية، طبعة 1، دار الثقافة للنشر والتوزيع، عمان 2010 ص 65.

[3]. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في الكمبيوتر والانترنت، طبعة1، دار الفكر الجامعي الإسكندرية 2006، ص160.

وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس والملموس، وفي هذه الحالة تتميز المعاينة بالسهولة باعتبار أنها تتم على عناصر ملموسة محلا للجريمة أو تخلفت عنها.

- ✓ . أما المسرح الافتراضي يقع عادة داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخلة وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها وكذلك الجرائم التي تتم بطريق الانترنت مثل الإرهاب الالكتروني.

وتتميز المعاينة في العالم الافتراضي بالصعوبة نظرا لعدة أسباب نذكر منها[1]:

- ✓ . ندرة الآثار المادية التي تختلف عن الجرائم التي تقع على أدوات المعلومات
- ✓ . الإعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة زمنية قصيرة[2]

وحتى يمكن لضباط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه أن ينتقل إلى العالم الافتراضي لمعاينة من مكتبه أو اللجوء إلى مقهى الانترنت ا والى الخبراء وغيرها من الأماكن التي تساعده في إظهار الحقيقة.

أما عن إجراءات المعاينة التقنية فلا بد على ضابط الشرطة القضائية إتباع بعض القواعد والإرشادات الفنية عند معاينة مسرح الجريمة منها:

- ✓ . عند العثور على حاسبات إليه أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها، وتدوين الحالة التي هي عليها
- ✓ . يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها.
- ✓ . عند العثور على دعائم التخزين (اسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها، والمكان الذي وجدت فيه.
- ✓ . يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة بلاستيكية أو ورقية كما ينبغي حمايتها من الكسر أو تأثير العوامل الجوية، وإبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وإرسالها إلى المخبر لإجراء الخبرة.

[1]. ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة ماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، السنة الجامعية 2016/2015.

[2]. نظرا لكون الجريمة المعلوماتية صعبة الإثبات واكتشاف من قام بها خاصة في مقاهي الانترنت لتوافد عدد كبير جدا من الأشخاص على مسرح الجريمة.

ب . التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق وذك لمساسه بالحريات التي تكفلها الدساتير عادة، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما يضمن ضمانات الحرية الفردية أو حرمة المسكن فالتفتيش ما هو إلا وسيلة للإثبات المادي لأنه إجراء يستهدف الوصول إلى أدلة مادية، ويخضع تفتيش الحاسب الآلي إلى ضوابط منها ما هو موضوعي ومنها ما هو شكلي.

فالمقصود بالشروط الشكلية تلك الإجراءات التي اوجب المشرع مراعاتها عند إجراء عملية التفتيش، من اجل ضمان صحة ودقة النتائج التي يصل إليها القائم بالتفتيش وإحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية ذلك أن الشكلية في الإجراءات الجنائية تعد ضمانة لعدم تعسف الجهات القائمة بالتفتيش

وحدد المشرع الجزائري أوقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا وقد نص على ذلك في قانون الإجراءات الجزائية (لا يجوز البدء في التفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساء .....)[1]

والمشرع الجزائري أجاز من خلال نص المادة2/47 منق.ا.ج.ج على إجراء التفتيش في أي وقت من أوقات النهار أو الليل في جرائم خطيرة محددة من بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات بشرط إذن مسبق من وكيل الجمهورية المختص، كما اشترط أن يتم التفتيش المنازل في حضور المتهم ، وفي حالة ما تعذر عليه الحضور وقت الإجراء كان على ضابط الشرطة القضائية أن يكلفه بتعين ممثل له وإذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوبه شاهدين من غير الموظفين الخاضعين له وهذا طبقا لأحكام المادتين 47 و47 من ق .ا.ج.ج لكن المشرع بموجب القانون رقم 22/06أضاف فقرة على المادة 45 تتضمن استثناء الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من الأحكام المنصوص عليها في المادة 45 مفادها أن ضابط الشرطة القضائية غير ملزم بحضور المشتبه فيه ولا رضاه أثناء التفتيش أو حتى حضور من يمثله عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما أضافت المادة 47 مكرر من نفس القانون إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوس في مكان أخر يمكن أن يجري التفتيش بعد الموافقة

[1]. انظر المادة 47 من الأمر رقم 155/66 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

المسبقة لوكيل الجمهورية أو قاضي التحقيق طبقا لأحكام المادة 45 ، وان مخالفة الإجراءات الواجب إتباعها في المادتين 45 و47 يترتب عليها البطلان[1].

وبما أن التفتيش عمل من أعمال التحقيق فينبغي تحرير محضر به يثبت ما تم من إجراءات أو ما أسفر عنه التفتيش من أدلة، فيكون المحضر مكتوب باللغة الرسمية، يحمل تاريخ تحريره وتوقيع محرره ويتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.

أما عن الشروط الموضوعية للتفتيش، فيقصد بها الشروط اللازمة لإجراء تفتيش صحيح ويمكن أن نذكر الأساسية منها وهي:

- ✓ . **سبب التفتيش:** حتى يكون التفتيش صحيحا لابد أن تكون هناك جريمة قد وقعت وهي جريمة معلوماتية وهو ما أكدته المادة 5 من القانون 04/09.
- ✓ **محل التفتيش:** يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره ، فقد يكون إما مسكنا أو شخصا أو سيارة ...مع مراعاة الإجراءات القانونية المقررة ، و بالنسبة لهذا النوع من الجرائم فمحل التفتيش هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الانترنت على العالم ، والشبكة التي تشمل في مكوناتها الخادم[2] والمزود الآلي[3] وغيرها، وفي إطار جريمة الإرهاب الالكتروني يقع التفتيش على موضوعين اثنين هما : تفتيش المكونات الحاسب الآلي (المادية والمعنوية) و تفتيش الشبكات المعلوماتية المتصلة بالحاسوب.
- ✓ **السلطة المختصة بالقيام بالتفتيش:** حرص المشرع على إسنادها لجهة قضائية تكفل الحقوق والحريات تتمثل في قاضي التحقيق أو النيابة العامة.فهي التي لها الحق فيمنح الإذن بالتفتيش ولابد أن يكون مكتوب
- ✓ **. الغاية من التفتيش:** لابد أن يكون التفتيش بقصد ضبط أشياء تتعلق بالجريمة أو تفيد في كشف الحقيقة والكشف عن أشياء تتعلق بالجريمة أو تفيد في أظهار الحقيقة طبقا للنص المادة 44 من ق.ا.ج.ج ويعتبر باطلا التفتيش الذي يجري لأغراض أخرى.

ج. ضبط الأدلة:

ضبط الأدلة الالكترونية هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عن مرتكبيها وهو يرد إلا على الأشياء المادية وبالتالي لا صعوبة في ضبط أدلة الجريمة الواقعة على المكونات المادية لكمبيوتر وإنما تكمن الصعوبة في ضبط

[1]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، مرجع نفسه ص215.

[2]. الخادم: هو الجهاز الرئيسي أو المسئول في الشبكة وباقي الأجهزة المتصلة بالشبكة هي عبارة عن عملاء لأنها تطلب في خدمات معينه منه.

[3]. المزود الآلي: هو المزود الذي يوفر لعملائه إمكانية الوصول إلى الانترنت.

الوسائل الفنية المستحدثة في إتلاف البرامج مثل الفيروس وكذا المكونات المعنوية للحاسوب، والمشرع الجزائري تدخل بموجب ال قانون04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حيث قرر آليات خاصة بها:

- ✓ . نسخ المعطيات محل البحث على دعامة تخزين قابلة للحجز (وسائط تخزين البيانات والمعطيات والبرمجيات) مع الحفاظ على سلامة المعطيات في المنظومة المعلوماتية
- ✓ . الحجز عن طريق منع الوصول إلى المعلومات، ويتم عادة عن طريق الترميز أو بتقيد الدخول إلى تلك المنظومة أو عن طريق أية وسلة الكترونية.
- ✓ . الحجز على المكونات المادية للحاسوب وملحقاته والمعدات المستعملة في الشبكة كجهاز المودم

كما أن قانون الإجراءات الجزائية نص على انه لا يجوز ضبط الأدلة إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة العامة، غير انه طبقا لقانون الإجراءات الجزائية المعدل والمتمم في الفصل الرابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور نصت المادة 65 مكرر فقرة 3 على انه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة ، أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نقس إجراءات الجريمة العادية[1].

2: الإجراءات الشخصية

وهي إجراءات تتعلق بالشخص في حد ذاته وتشمل الخبرة والاستجواب شهادة شاهد الكتروني .

أ. الخبرة

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية أو العلمية والتي لا تتوفر لدى رجال القضاء من اجل الكشف عن الدليل أو قرينة تفيد معرفة الحقيقة بشأن وقوع الجريمة ونسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية[2]

ونظرا لان جريمة الإرهاب الالكتروني لها خصوصيتها، فان الخبير ألمعلوماتي لابد أن توافر لديهم المقدرة الفنية والإمكانيات العلمية والفنية في المسالة موضوع الخبرة، ولا يكفي في ذلك حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العلمية، لأنها هي التي تحقق الكفاءة الفنية من اجل كشف الغموض عن الجريمة وتجميع أدلتها والتحفظ عليها، ومساعدة المحقق في إيجاد جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

ويخضع الخبير إلى إجراءات قانونية هي:

[1]. بشير حماني، خصوصية التحقيق في الجريمة الالكترونية، مذكرة تخرج مقدمة لنيل شهادة الماستر بعنوان، جامعة محمد بوضياف، المسيلة 2019/2018 ،ص20

[2]- احمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري الجزء الثاني، الطبعة 5، ديوان المطبوعات الجامعية الجزائر،ص259.

- ✓ . اختياره من طرف جدول الخبراء حسب المادة147 من ق.ا.ج.ج
- ✓ . على الخبير أداء اليمين القانونية حسب المادة 145 من ق.ا.ج.ج

ومن أهم الوسائل المادية والأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:عناوين IP، والبريد الالكتروني وبرامج المحادثة

- ✓ . برتوكول الانترنت (IP) يعتمد عليه الخبير من خلال إتباع المسار ألتراسلي للبروتوكول للبحث عن رقم الجهاز المستعمل في الجريمة وثم تحديد موقعه ومنه معرفة الجاني
- ✓ . البر وكسي (PROXY) الذي يعمل كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cashe Memory

. برامج التتبع : يقوم هذا البرنامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه ، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IPالذي تمت من خلاله عمل ية الاختراق ، واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق ، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى ، ومن الأمثلة على هذا البرنامج . نظام كشف الاختراق ويرمز له اختصارا IDS. و برنامج الدمج وفك الدمج (pkzip)، وكذلك أدوت تدقيق ومراجعة العمليات الحاسوبية (Auditing Tools) و . الذكاء الصناعي أدوات فحص ومراقبة الشبكات .....الخ.

ب . الاستجواب:

الاستجواب هو مساءلة المتهم ومناقشته عن الوقائع المنسوبة إليه ارتكابها ومجابهته بالأدلة وسماع ما لدية من دفوع للتهمة المنسوبة إليه، واستجواب المتهم في الجرائم المعلوماتية تحكمه نفس القواعد العامة للاستجواب في الجرائم التقليدية، لا بد أن تكون السلطة المختصة التي تتولى الاستجواب مؤهلة للتحقيق في جريمة الإرهاب الالكتروني حتى يمكنه الاستيعاب والتعامل مع مفرداتها وقد أحاط المشرع الاستجواب بعدة ضمانات لضمان حقوق المتهم.[1]

ومن الإجراءات المستحدثة لمواجهة جريمة الإرهاب الالكتروني في التشريع الجزائري تمديد التوقيف تحت النظر الممنوح لضباط الشرطة القضائية مرة واحدة طبقا لإحكام المادة 51 فقرة 5 من الأمر 02/15 المؤرخ في 23 جويلية 2015 مع العلم أن

[1]. خلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية،مداخلة مقدمة في الملتقى حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة 16-17 نوفمبر 2015 ص.ص 2-3

هذا الإجراء البوليس يقوم به الضباط ضد كل شخص تتوافر دلائل قوية على ارتكابه الجريمة وذلك بوضع شخص في مركز الشرطة أو الدرك لمدة يحددها المشرع كلما دعته الضرورة لذلك على انه لا يجوز أن تتجاوز مدة التوقيف للنظر 24 ساعة ماعدا بعض الجرائم الخطيرة التي خصها المشرع باستثناءات من ضمنها جريمة الإرهاب الالكتروني باعتبار أنها من الجرائم الماسة بالمعالجة الآلية للمعطيات [1].

كما أجاز المشرع استعمال القوة لإحضار الأشخاص وهذا ما أقرته المادة 65فقرة1من القانون رقم 22/06

ج سماع الشهود

الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي لديه خبرة جوهرية لازمة للدخول إلى نظام المعالجة الآلية للمعطيات[2]وينحصر الشاهد ألمعلوماتي في عدة طوائف وفئات وهم:

- ✓ . مشغلو الحاسب الآلي أي الشخص المسئول عن تشغيل الجهاز والمعدات المتصلة به، ولا بد أن يكون لديه خبرة كبيرة في استخدام الحاسب الآلي ومكوناته عن طريق استخدام هذه البيانات وكيفية إدخال البيانات ثم استخراجها ومعالجتها كما يجبان تكون له خبرة واسعة في الكتابة السريعة عن طريق لوحة مفاتيح الحاسب الآلي.
- ✓ . خبراء البرمجة وهم الأشخاص المتخصصون في كتابة أوامر البرامج وهم فئتين مخططو برامج التطبيقات ومخططو برامج النظم[3]

وقد أطلق عليهم المشرع الجزائري مقدمي الخدمات وعرفهم القانون 04/09 على أنهم:

. أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات.

. وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال أو لمستعمليها.

الفرع الثاني: الإجراءات الخاصة في جريمة الإرهاب الالكتروني

في ظل تفاقم الاعتداءات على معطيات الحاسب الآلي خاصة مع ضعف الحماية الفنية استدعى ذلك تدخلا تشريعيا حيث استدرك المشرع الجزائري الفراغ القانوني من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها وتضمن هذا القانون 19 مادة في ستة فصول.

[1]. سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، جامعة الإخوة متنوري، قسنطينة، مجلة العلوم الإنسانية عدد52، المجلد ب، ديسمبر 2019 ص52.

[2]. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2003، ص339.

[3]. خلف فاروق ، الآليات القانونية لمكافحة الجريمة المعلوماتية ،المرجع السابق ص4 .

1: الإجراءات الخاصة بحماية معطيات الحاسب الآلي:

تمثل المعطيات أهم العناصر المعنوية التي يتشكل منها نظام المعالجة الآلية للمعطيات، لذلك كانت أحد العناصر المستهدفة في الجريمة المعلوماتية، هذا ما دفع بالمشرع الجزائري إلى محاولة توفير الحماية الجنائية لها.

أ. التحفظ المعجل على البيانات المخزنة:

هذا الإجراء يعد أداة تحقيق مستحدثة ويقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته وتحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية، ويتضح أن التحفظ العاجل هو إجراء أولي تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها[1].

ب . الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك:

الأصل أن البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية، غير انه يسمح لرجال الضبط القضائي بان يأمر الأشخاص بتسليم ما تحت أيديهم من موضوعات يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات.[2]

2: السماح بالمراقبة الاتصالات الالكترونية:

يقصد بمراقبة الاتصالات الالكترونية أثناء بثها وليس الحصول على الاتصالات الالكترونية المخزنة حيث يقوم المراقب باستخدام التقنية الالكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء كان شخص أو مكان أو شيئا حسب طبيعته ، وعليه فان المراقبة الالكترونية هي وسيلة حديثة تخص فقط الجريمة المعلوماتية دون غيرها ، وأيضا هي من وسائل جمع البيانات والمعلومات عن المشتبه فيه،[3]وقد عرفت فقرة 03من قانون 04/09 مراقبة الاتصالات الالكترونية حيث تشمل الاتصالات السلكية واللاسلكية والخلوية كالفاكس والبريد الالكتروني ومواقع الدردشة ، وهذا الإجراء ليس بالجديد فقد تعرض له المشرع الجزائري من خلال تعديل ق .ا.ج.ج بموجب القانون 22/06 ومن خلال نصوص المواد من 65مكرر5إلى 65 مكرر10 أجاز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور ، إذ تنص أحكام هذه المواد على انه في حالة ضرورة التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات ،يجوز لوكيل الجمهورية أو قاضي التحقيق حسب الحالة أن يأذن لضباط أو أعوان الشرطة القضائية باعتراض

[1]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، مرجع سابق ص230.

[2]. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية،المرجع نفسه، ص230.

[3]. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الكمبيوتر والانترنت في مرحلة جمع الاستدلالات دون ذكر طبعة، دار الفكر الجامعي، الإسكندرية 2013 ،ص204.

المراسلات بواسطة وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية من اجل تسجيل المكالمات والتقاط الصور، على أن تتم هذه الإجراءات في سرية تامة لما فيها من مساس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا ، غير أن المشرع كفلها بكل الضمانات والضوابط الأساسية.

ولقد نص المشرع الجزائري من خلال المادة 4 من قانون 04/09 على الحالات التي بتوافرها يمكن اللجوء إلى المراقبة الالكترونية المنصوص عليها في المادة3 المذكورة أعلاه وتشمل هذه الحالات التالية:

- ✓ . الوقاية من الأفعال الإرهابية أو التخريبية أو الماسة بأمن الدولة.
- ✓ في حالة توفر معلومات كافية بوجود تهديدات ضد منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .
- ✓ مقتضيات التحريات والتحقيقات القضائية ذلك، عندما يكون من الصعب الوصول إلى نتيجة دون اللجوء إلى المراقبة الالكترونية .
- ✓ إذا ما تعلق الأمر بتنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1]

وحتى يكون إجراء مراقبة الاتصالات الالكترونية صحيحا لابد أن يخضع إلى مجموعة من الإجراءات التي تحكمه، منها ما نص عليه ق.ا.ج.ج المعنون ب اعتراض المراسلات والتقاط الصور وأخرى منصوص عليها في قانون04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، فهناك ضوابط وردت في ق.ا.ج.ج،التي نصت عليها المادة 65مكرر1 وما بعدها وفي حالة عدم احترمها يترتب بطلان الإجراء وتتمثل هذه الضوابط في:

- ✓ . صدور إذن من السلطة المختصة ويكون مكتوب صادر من قاضي التحقيق أو وكيل الجمهوري[2].
- ✓ لا بد أن يتضمن الإذن كل العناصر التي تسمح للضباط بالتعرف على الاتصالات المطلوب التقاطها[3].
- ✓ لابد من يكون نوع الجريمة إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- ✓ . مدة الإجراء هي 4 أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق.
- ✓ لابد من تحرير محضر بالمعطيات التي تمت عليها العملية وان يتضمن المحضر ساعة بداية ونهاية تلك العملية وتاريخها

أما الضوابط التي وردت في القانون 04/09، فقد نصت عليها المادة 04 من هذا القانون على الحالات التي تسمح اللجوء إلى المراقبة الالكترونية، والتي سبق وان تعرضنا لها،أما عن شروط المراقبة الالكترونية فهي كالأتي: [4]

[1]. المادة 4 من القانون 04/09 المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2]. أحسن بوسقيعة، التحقيق القضائي، طبعة 10، دار هومة للنشر . الجزائر2009، ص124.

[3]. انظر المادة 65مكرر7 تعديل ق.ا.ج.ج 2006.

[4]. ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية المرجع السابق.

- ✓ . صدور الإذن من النائب العام لدى مجلس قضاء الجزائر العاصمة[1].
- ✓ يباشر عملية المراقبة ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه.
- ✓ تكون مدة الإذن 6 أشهر قابلة للتجديد[2].

3: الحماية التقنية للأنظمة من الاعتداءات الالكترونية:

هناك العديد من الأساليب والبرمجيات لحماية المعلومات والأجهزة الالكترونية يتم اتخاذها كالإجراءات وقائية لتكون المعلومات والبيانات في مأمن من العبث والانتهاك وذلك بالاعتماد على مجموعة من الوسائل نذكر منها:

أ . برامج الحماية:

هي تلك البرامج التي تحقق الأمن عن طريق تصفية وحجب المواقع الممنوعة والخطيرة ويتضمن إدارة الوقت لتحديد زمن ومدة اتصال بالمواقع ، وهناك برامج حماية خاصة للأطفال تقوم بتحديد البرامج التي يستخدمها وتمنعهم من إرسال معلومات شخصية أثناء المحادثة وكمثال عن برامج الحماية ، **جدار النار:** حيث قامت شركات . خدمات المعلومات والبرامج ، وبطاقات الائتمان الكبيرة بتطوير أنظمة حماية نذكر منها جدار النارfaire Wall softwareكواحد من الاستراتيجيات المتبعة لمنع عمليات الدخول غير الشرعية من الانترنت ويعتبر جدار النار بمثابة ممر الكتروني يراقب الدخول على الشبكة والخروج منها ، وتؤكد الإحصائيات انه ما يزيد عن ثلث مواقع الوات على الانترانت محمي ببعض أشكال جدار النار[3].

ب . الحماية من الفيروسات:

تتم بوضع برنامج اكتشاف في الحواسيب، للقيام بالفحص الدوري والسريع للبرامج المخزنة والمعلومات المتداولة بين مختلف الأجهزة المتصلة فيما بينها وعند اكتشاف فيروس ما يتم التنبيه لوجوده للتمكن من محاصرته ومنعه من التكاثر وإبطال نشاطه التدميري.

ج . اكتشاف التطفل وسوء الاستخدام:اكتشاف التطفل وسوء الاستخدام يهدف لاكتشاف النشاط الضار في بدايته ، ويمكن أن يتحقق ذلك عن طريق مراقبة هذه الأنشطة فيها ، وان تم اكتشاف مبكر ربما في الإمكان إجهاض المحاولة قبل حدوث الضرر، ولكن هذا المبدأ ليس عمليا لأنه لا يمنع كل الهجمات فيصير الاكتشاف هو الأسلوب العلمي.[4]

[1]. انظر المادة 4 فقرة 03 من قانون 04/09، المرجع السابق.

[2]. انظر المادة 13 من قانون 04/09.المرجع نفسه.

[3]. قندوشي ربيعة، الإعلان الالكتروني، دون ذكر الطبعة، دار هومة للنشر والتوزيع،الجزائر،2012، ص114.

[4]. ذياب البدانية، الأمن وحرب المعلومات، المرجع السابق، ص390.

خلاصة الفصل الثاني

تم التطرق في هذا الفصل إلى إستراتيجية مكافحة جريمة الإرهاب الالكتروني من خلال المبحث الأول تحت عنوان: الحماية الموضوعية ضد الإرهاب الالكتروني، تم فيه استعراض جهود المنظمات الدولية والوطنية لمكافحة الظاهرة، والتعرف على الإطار المؤسساتي الدولي والوطني المكلف بذلك أما المبحث الثاني فكان بعنوان الحماية الإجرائية ضد الإرهاب الالكتروني، تناولنا فيه آليات التعاون الدولي لمكافحة جريمة الإرهاب الالكتروني كما تم التطرق إلى المواجهة الإجرائية لمكافحة الإرهاب الالكتروني في التشريع الجزائري.

الخاتمة

الخاتمة

إن التطورات الهائلة التي عرفتها التكنولوجيات الحديثة للإعلام والاتصال، ورغم ما وفرته من تسهيلات في أمور حياتنا اليومية، إلا أنها في المقابل فتحت الباب على مصراعيه لتطور أدوات وسائل تنفيذ الجرائم الإرهابية وجعلها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة الدولية.

ومن خلال دراستنا لموضوع جريمة الإرهاب الالكتروني توصلنا إلى مجموعة من الاستنتاجات والتوصيات هي:

أولا: الاستنتاجات

1. مصطلح الإرهاب الالكتروني يمكن آن يطلق على إحدى الصور المستحدثة للإرهاب الذي تقوم به التنظيمات الإرهابية والذي يستهدف تحقيق أهداف الإرهاب التقليدي وذلك باستخدامك تكنولوجيا المعلومات

2. يتميز الإرهاب الالكتروني بكونه من الجرائم غير العنيفة التي ترتكب من خلال حاسب ألي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، كما انه جريمة إرهابية متعدية للدود وغير خاضعة لنطاق إقليمي محدد ومن الصعب اكتشافها وإثباتها نظرا لسرعة إخفاء الدليل الرقمي وسهولة إتلافه، كما يكون مرتكبها عادة من ذوي الاختصاص في مجال تقنية المعلومات، إضافة إلى خطورتها البالغة وإضرارها الكبيرة.

3. بالنظر لخطورة الإرهاب الالكتروني وأضراره البالغة فان مواجهته تتطلب وضع استراتيجية خاصة للتعاون بين الدول في ظل مراعاة عدد من المعايير التي تعتمد في مواجهة أنماط الإرهاب الالكتروني المختلفة.

4. تتوزع الجهود الدولية في مكافحة الإرهاب الالكتروني إلى ثلاث أنماط هي تجريمه في التشريعات الوطنية، والتعاون فيما بينها في مواجهته، وتفعيل دور منظمة الأمم المتحدة في ذلك، وتتمثل أبرز أوجه التعاون فيما بينها في التعاون التشريعي الدولي والتعاون الأمني الدولي والتعاون القضائي الدولي.

5. يتحقق التعاون التشريعي الدولي في مواجهة الإرهاب الالكتروني من خلال التعاون فيما بينها في إصدار طائفتين من التشريعات: الأولى تشريعات متعلقة بالجرائم الالكترونية بقواعدها الموضوعية والإجرائية وتشريعات تنظيم الخدمات الالكترونية والسلامة المعلوماتية والطائفة الثانية تشريعات مكافحة الإرهاب.

6. لقد وضع المجتمع الدولي صكوكا قانونية عالمية لمكافحة الإرهاب تحت رعاية الأمم المتحدة ووكالاتها إلا انه لا توجد حتى ألان اتفاقية شاملة للأمم المتحدة بشأن الإرهاب عامة والإرهاب الالكتروني خاصة.

7 . يلعب الانتربول ومكتب الشرطة الأوربية الأوروبول و مكتب الشرطة الإفريقية الافريبول ووحدة التعاون القضائي وفرق التحقيق المشتركة دورا كبيرا في تجسيد أهداف التعاون الأمني الدولي على صعيد مكافحة الإرهاب الالكتروني في العالم.

8. يلعب التعاون القضائي الدولي دورا بارزا في مكافحة الجرائم ومن بينها الإرهاب الالكتروني، ويتخذ هذا التعاون عدة أشكال مثل تبادل الخبرات والمعلومات الفضائية والمساعدة القضائية والإنابة القضائية أو مصادرة الأموال الناتجة من الجريمة المنظمة أو تسليم المجرمين، والاعتراف بالأحكام الجنائية أو نقل الإجراءات الجنائية وغيرها ذلك.

9. تعد الولاية القضائية العالمية ذات أهمية خاصة لردع الإرهاب الالكتروني حيث من الصعب للغاية تطبيق الولاية القضائية الإقليمية على الإرهاب الالكتروني نظرا لطبيعة الانترنت وخصائص الإرهاب الالكتروني العابر للحدود الوطنية لذلك يعد الاختصاص القضائي الإقليمي غير ملائم لمواجهة الإرهاب الالكتروني.

ثانيا التوصيات

1. نوصي بإعطاء جرائم التقنية حقها من الأهمية في المؤسسات التشريع الوطنية والدولية على حد سواء مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، وباعتبار أن جرائم الانترنت ذات بعد دولي تتطلب الانخراط في الاتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

2. عقد دورات مكثفة للعاملين في حقل التحري والتحقيق والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب المرتبطة بها والنظر في تضمين مناهج التحقيق الجنائي في كليات ومعاهد تدريب الشرطة موضوعات عن جرائم الانترنت.

3. التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الانترنت لا تحدها حدود وطنية أو قومية.

4. سرعة تماشي عملية التشريع مع المعطيات الواقعية، والإسراع في إصدار القوانين التنظيمية من خلال محاولة وضع مدونة قواعد السلوك في المجال المعلوماتية تتناسب والتطورات التي يعرفها الإجرام ألمعلوماتي

5. ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق العمل على تبادل المعلومات بين الأجهزة الأمنية المعنية بمواجهة الإرهاب الالكتروني وإنشاء خلايا مشتركة تعمل على رصد تهديدات الإرهاب الالكتروني وتبادل المعلومات بشأنها.

6. وأخيرا في رأينا أن أحسن حماية هي الحماية الوقائية لذا نوصي بضرورة نشر الوعي الرقمي بين مستخدمي الانترنت عن طريق لفت انتباههم إلى خطورة الإرهاب من خلال مختلف ورش العمل التعريفية والإعلامية وضرورة الانخراط في مواجهته.

قائمة المراجع والمصادر

أولا . **المراجع العامة**

أ . المعاجم والقواميس

1. ابن محمد بن مكرم الإفريقي المصري، لسان العرب، د.ط، مجلد الأول، دار صادر،بيروت، بلا سنة طبع.

2 . الشيخ محمد بن أبي بكر عبد القادر الرازي .، مختار الصحاح .، دار الرسالة،الكويت،سنة 1983.

3 . انطوان نعمة وآخرون ، معجم المنجد في اللغة المعاصرة، طبعة 2، دار المشرق ، بيروت ،2001.

ب . الكتب

1. أحسن بوسقيعة، التحقيق القضائي، طبعة 10، دار هومة للنشر . الجزائر، سنة 2009 .

2 . احمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، الطبعة 5، ديوان المطبوعات الجامعية، الجزائر، دون سنة طبع.

3. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية د.ط، دار الخلد ونية، الجزائر،سنة2017م/1438هـ.

4. خلفي عبد الرحمان، محاضرات في القانون الجنائي، د.ط، دار الهدى، عين مليلة،الجزائر،2012.

5. رشيدة بوكر،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت لبنان ط1سنة2012.

6. روابح فريد، محاضرات في قانون الإجراءات الجزائية،كلية الحقوق والعلوم السياسية، جامعة لمين دباغين، سطيف، د.س،ط.

7. زين العابدين عواد كاظم الكردي، جريمة الإرهاب ألمعلوماتي، د.ط،بيروت، منشورات الحلبي الحقوقية، سنة 2018

8. ضرغام جابر عطوشألمواش، جريمة التجسس ألمعلوماتي دراسة مقارنة الطبعة الأولى، المركز العربي للنشر والتوزيع،مكتبة دار السلام القانونية السعودية، سنة 2017 .

9. طه زكي صافي، القواعد الجزائية العامة فقها واجتهادا،د.ط، المؤسسة الحديثة للكتاب،طرابلس، لبنان، سنة1997 .

10. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط1، دار النهضة العربية د.ط سنة2001.

11. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في الكمبيوتر والانترنت، طبعة1، دار الفكر الجامعي الإسكندرية سنة 2006 .

12. عبد الله ماجد العكايلة، الوجيز في الضبطية القضائية، طبعة 1، دار الثقافة للنشر والتوزيع، عمان 2010.

13. علي عدنان الفيل، الإجرام الالكتروني،الطبعة 1، مكتبة زين الحقوقي والأدبية، لبنان، سنة2011.

14. علي جابر، جرائم الانترنت،د.ط،مكتبة زين الحقوقية،لبنان، سنة2018.

15. علي عسيري، الإرهاب والانترنت، ط1، مكتبة جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2006.

16. عمر خوري، شرح قانون العقوبات القسم العام، كلية الحقوق، جامعةالجزائر1، السنة الجامعية 2011/2010.

17. عفيفي كامل عفيفي . جرائم الكمبيوتر . الطبعة 2، دار الثقافة للطباعة والنشر والتوزيع . القاهرة مصر. سنة 2012 .

18 . قندوشي ربيعة، الإعلام الالكتروني، دون ذكر الطبعة، دار هومة للنشر والتوزيع،الجزائر ، 2012 .

19 . محمد حماد مرهج إلهيتي، الجريمة المعلوماتية، دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني،د.ط، دار الكتب القانونية،الإمارات، سنة 2014.

20 .محمد أمين بشري، التحقيق في الجرائم المستحدثة، ط 4، مركز الدارسات والبحوث المملكة العربية السعودية،والبحوث جامعة نيل العربية للعلوم الأمنية رياض، سنة 2004 .

21 . محمد علي سويلم، جرائم الإرهاب الالكتروني (دراسة مقارنة)، د.ط، دار المصرية للنشر والتوزيع،القاهرة، سنة 2018

22. منصوري رحماني، الوجيز في قانون الجنائي العام، دار العلوم لنشر والتوزيع، عنابة، سنة 200

23. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الكمبيوتر والانترنت في مرحلة جمع الاستدلالات، د.ط، دار الفكر الجامعي، الإسكندرية، سنة 2013

24 . نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع،الأردن، سنة 2008

25 . هشام محمد، جرائم الإرهاب، ط1، المركز العربي للإصدارات القانونية، مصر سنة2016

ثانيا: الأطروحات والمذكرات .

1 . ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة لنيل شهادة ماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، السنة الجامعية 2016/2015 .

2. إسراء طارق جواد كاظم الجابري،جريمة الإرهاب الالكتروني،دراسة مقارنة رسالة لنيل درجة الماستر في القانون العام، كلية الحقوق، جامعة النهرين،2012 .

3. أدهم باسم نمر بغدادي، وسائل البحث والتحري عن الجرائم الالكترونية، مذكرة لنيل درجة ماجستير في القانون العام كلية الدراسات العليا جامعة النجاح الوطنية نابلس، فلسطين 2018 .

4. أسامة مهمل، الإجرام السيبراني، مذكرة لنيل شهادة الماستر الأكاديمي، فرع القانون الجنائي، قسم الحقوق، كلية العلوم السياسية والقانونية جامعة محمد بوضياف المسيلة 2018/2017 .

5. بشان نسرين وبلعباسي منال، خصوصية الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد بشير الابراهيمي برج بوعريريج، السنة الجامعية 2020-2019.

6. بشير حماني، خصوصية التحقيق في الجريمة الالكترونية، مذكرة تخرج مقدمة لنيل شهادة الماستر، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، السنة الجامعية 2019/2018 .

7. ليلة مرزوق، جرائم المساس بأنظمة المعالجة الآلية للمعطيات على ضوء الاتفاقيات الدولية والتشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة العربي بن مهيدي، كلية الحقوق والعلوم السياسية، السنة الجامعية 2017/2016

8. شاشوة ياسمينة، الإرهاب الالكتروني بين مخاطرة واليات ومكافحته مذكرة لنيل شهادة الماستر في الحقوق، القانون الجنائي، جامعة أكلي محند اولحاج كلية الحقوق والعلوم السياسية سنة 2019 /2020.

9. شنيني عقبة، الجريمة الإرهابية في التشريع الجزائري، مذكرة مكملة نيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة محمد خيضرة،بسكرة 2014/2013 .

10. عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقا يد تلمسان سنة 2012 .

11. على بوعمرة، جريمة الإرهاب الالكتروني، مذكرة لنيل شهادة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة العربي تبسي، تبسة، السنة الجامعية 2020-2021.

12. غلاف كريمة وجرلالزوهرة . جريمة الإرهاب الالكتروني . مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية جامعة عبد الرحمان ميرة، بجاية، السنة الجامعية 2019/2018 .

ثالثا: المجلات والمقالات

1 . اوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني،مركز البيان للدارسات والتخطيط أغسطس، د.ب 2016

2. احمد رفعت وصالح بكر الطيار،الإرهاب الدولي، مركز الدراسات العربي الأوروبي، سنة1988

3بيتر غرابوسكي، جرائم الحاسب الآلي الإبعاد العالمية، ط1، مركز البحوث والدارسات الأمنية القيادة العامة ابوظبي 2006 .

4. بوعنادة فاطمة الزهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول 2013 .

5. جعفر حسن جاسم الطائي، الإرهاب ألمعلوماتي وأليات الحد منه، مجلة العلوم القانونية والسياسية، عدد خاص بمؤتمر الكلية، كلية القانون والعلوم السياسية جامعة ديالي، العراق ،2016.

6 . حسين عبد علي عيسى ولاله محمد تقي محمد أمين، التعاون الدولي في مواجهة جريمة الإرهاب الالكتروني، دراسات قانونية وسياسية، مجلة علمية محكمة، السنة السادسة ال عدد1،د.س.ط

7. خلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية،مداخلة مقدمة في الملتقى حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة 16-17 نوفمبر 2015

8. صباح كزيز، أمال كزيز،الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم1، العدد8، سنة 2008.

9. سعيدة بوزنون، مكافحة الجريمة الالكترونية في التشريع الجزائري، جامعة الإخوة منثوري،قسنطينة، مجلة العلوم الإنسانية عدد52، المجلد ب، ديسمبر 2019 .

10. مرين يوسف، إرهاب الانترنت عندما تتحول التقنية إلى وسيلة للإجرام، مجلة الدراسات القانونية والسياسية، المجلد الرابع،العدد2، 2018.

11. معمري خديجة وخلفاوي خليفة، الإشكالات القانونية لجريمة الإرهاب الالكتروني، مجلة القانون، المجتمع والسلطة المجلد 11 العدد1 السنة2022

12. مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الالكتروني، مجلة جامعة الناصر، العدد الخامس، يناير 2015 .

13. ناصر العلي، الجهود الدولية في مكافحة الإرهاب الالكتروني، مجلة الباحث للدراسات الأكاديمية،المجلد 08 ال عدد01،سنة2021

14. يوسف كوران، جريمة الإرهاب والمسؤولية المترتب عنها في القانون الجنائي الداخلي والدولي، منشورات كردستان للدراسات الاستراتيجية العراق، السلمانية 2008.

رابعا: النصوص القانونية

أ . النصوص القانونية الوطنية

1. الأمر 66-156 المؤرخ في 1966/06/8 ، المتضمن قانون العقوبات الجزائري الصادر في الجريد الرسمية الجزائرية بتاريخ 1966/6/11 العدد49، المعدل والمتمم.

2. القانون رقم 04-15 المؤرخ في 2004/11/10، جريدة الرسمية عدد71، الصادر في 2004/11/10 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 8يونيو 1996المتضمن قانون العقوبات الجزائري المعدل والمتمم .

3 . القانون رقم 04-14 المؤرخ في2004/11/10،المعدل والمتمم للأمر رقم 155/66 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية، عدد17 الصادر 2004/11/10

4 .القانون رقم 04-25 المؤرخ في 2004/11/10 المعدل والمتمم لأمر 66-156 المتضمن قانون العقوبات الجزائري الصادر في الجريدة الرسمية بتاريخ 2004/11/11 العدد71 بتاريخ 10 نوفمبر2004

5 القانون .02/16 المؤرخ في 19يوميو2016، المتضمن قانون العقوبات الجزائري المعدل والمتمم ج ر، العدد 37 الصادرة بتاريخ 22 يونيو 2016

6. قانون رقم 09-04 المؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جريدة رسمية، عدد 47، الصادر في 2009/02/16

7. القانون رقم 06/15 المؤرخ في 15 فبراير2015 يعدل ويتمم القانون رقم 01/05 المؤرخ في 6 فبراير سنة 2005 والمتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها المعدل والمتمم

8 القرار الرئاسي 216-15 المؤرخ في أكتوبر 2015، والقاضي بإنشاء هيئة خاصة بالمراقبة الوقائية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة

ب . الاتفاقيات الدولية

1. الاتفاقية العربية لمكافحة الإرهاب المؤرخة في 22 ابريل 1998، بالقاهرة، جمهورية مصر العربية صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 98-413 المؤرخ في 7ديسمبر1998 .

2. . الاتفاقية المتعلقة بالجريمة الالكترونية، بودابست مجلس أوربا، مجموعة المعاهدات الأوربية، رقم 185، صادرة بتاريخ 2001/11/23 .

3 . اتفاقية بودابست

4 . اتفاقية الامم المتحدة

خامسا: مواقع الانترنت

1. بن بادة عبد الحليم، بوحاده محمد سعد، جريمة التجسس الالكتروني، نمط جديد من التهديدات السيبرانية الماسة بأمن الدول تاريخ النشر في 3 يوليو2020، متوفر على الموقع:httpsm//www.elmizane.com

2 . محمدمحمد الألفي مكافحة جرائم الإرهاب عبر الانترنت، المؤتمر الدولي لمكافحة علمية للإرهاب، بمؤسسة الأهرام المصرية، نشر يوم 05-04-2007، القاهرة، متوفر على الرابط:

.http://www. Maghress.Com/hespress/655تم الاطلاع عليه بتاريخ 2023/5/2

3. منيرة غلوش، دراسة عن مواجهة استخدام الارهابين لشبكة الانترنت، دون تاريخ نشر، تاريخ الاطلاع 2003/05/02 على الساعة 11صباحا، متوفر على الرابط:

http://gomhuriaonline.com/main.asp?v-articl-id-:204832

4. عبد المجيد حلاوة، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب ألمعلوماتي، الدورة التدريبية، مكافحة جرائم الإرهاب ألمعلوماتي، في فترة 9-13 /2006/04، متوفر على الرابط:http://jlps.univsul.edu.iq

4. عبد المجيد حلاوة، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب ألمعلوماتي، الدورة التدريبية، مكافحة جرائم الإرهاب ألمعلوماتي، في فترة 9-13 /2006/04، متوفر على الرابط:http://jlps.univsul.edu.iq

5. رائد عدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية حول توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، متوفر على الرابط:https://www.iasj.net

6 . وفاء لطفي حسين عبد الواحد، الإرهاب الالكتروني والأمن القومي في ظل جائحة كورونا كوفيد19، كلية العلوم الاقتصاد والإدارة، جامعة 6 أكتوبر، متوفر على الرابط: http://dspace.univ-bouira.dz

الفهرس

فهرس المحتويات